VeszLife Magánklinika

Korlátolt Felelősségű Társaság

ADATVÉDELMI ÉS ADATKEZELÉSI SZABÁLYZAT

Tartalom

Az adatkezelő szervezet megnevezése:	**VeszLife Magánklinika Korlátolt Felelősségű Társaság (továbbiakban: Társaság)**
A szervezet székhelye:	8200 Veszprém, Szófia u. 2/1.
A szabályzat tartalmáért felelős személy:	Dr. Bertalan Rita Ágnes és Dr. Szita István, ügyvezetők
A szabályzat hatályba lépésének dátuma:	2021. augusztus 1.
Az adatvédelmi tisztviselő neve:	Hornyák Edina
Az adatvédelmi tisztviselő elérhetőségei:	info@szofiaklinika.hu

A Társaság Veszprém egyik legjobban felszerelt és legnagyobb szaktudással bíró Magánklinikáját üzemelteti 2021. őszétől. A Szófia Magánklinika járóbeteg szakellátást végez az orvoslás számos szakterületén. A 2021-ben átadott új, önálló épületében a modern gyógyítás iránt elkötelezett, elhivatott, nemzetközileg is elismert szakemberek dolgoznak a betegek biztonságos gyógyulásáért.

1. A szabályzat célja, hatálya, alapelvek, alapfogalmak

1.1. Bevezető rendelkezések

1. A Társaság jelen szabályzatban (a továbbiakban: Szabályzat) határozza meg a természetes személyek személyes adatainak kezelésével és védelmével kapcsolatos irányelveket, valamint az adatvédelmi tevékenység ellátásában résztvevők feladatait és együttműködésük kereteit.

2. A Szabályzat hatálya alá tartozó személyek kötelesek a tevékenységük során a Társaság kezelésében lévő személyes adatokat a mindenkori jogszabályi rendelkezéseknek megfelelően, így különösen a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016/679/EU európai parlamenti és tanácsi rendelet (a továbbiakban: GDPR) rendelkezései, valamint a Társaságra irányadó egyéb jogszabályok rendelkezései szerint kezelni. A Társaság a személyes adatok kezelésével járó tevékenysége során érvényre juttatja a GDPR alapelveit, így különösen:
   a/ jogszerűség, tisztességes eljárás és átláthatóság elve: a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni;
   b/ célhoz kötöttség elve: a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történik, és azokat a Társaság nem kezeli ezekkel a célokkal össze nem egyeztethető módon;
   c/ adattakarékosság elve: a kezelt személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk;

d/ pontosság elve: a kezelt 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;

e/ korlátozott tárolhatóság elve: a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé;

f/ integritás és bizalmas jelleg: 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;

g/ beépített adatvédelem elve: olyan megfelelő technikai és szervezési intézkedések végrehajtása, amelyek már az adatkezeléssel járó folyamatok tervezésétől (az adatkezelés módjának meghatározásától) kezdődően az adatkezelés megszüntetéséig terjedő időszakban azt célozzák, hogy az adatvédelmi elvek hatékony megvalósítása, illetve a GDPR-ban foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépüljenek az adatkezelés folyamatába;

h/ alapértelmezett adatvédelem elve: olyan technikai és szervezési intézkedések végrehajtása, amelyek biztosítják, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek, továbbá, hogy a gyűjtött személyes adatok mennyisége, kezelésük mértéke, tárolásuk időtartama és hozzáférhetőségük is csak az adatkezelési cél szempontjából szükséges mértékre korlátozódjon. Különösen azt kell biztosítani, hogy a személyes adatok alapértelmezés szerint természetes személy beavatkozása nélkül arra illetéktelen személyek számára ne válhassanak hozzáférhetővé.

1.2. A Szabályzat célja

3. Jelen Szabályzat célja, hogy biztosítsa a Társaság tevékenysége során a személyes adatok védelméhez fűződő jog érvényesülését, továbbá, hogy a Társaság által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes és különleges adatok kezelése során irányadó adatvédelmi és adatbiztonsági szabályokat.

4. A Szabályzat célja továbbá, hogy meghatározza azokat a szervezési és technikai intézkedéseket, amelyek kialakításával a Társaság gondoskodik a személyes adatok kezelése során a személyes adatok biztonságáról. Erre tekintettel a Szabályzat a Társaság által folytatott adatkezelési tevékenységek során figyelembe veendő és követendő elveket, rendelkezéseket tartalmaz. Ezeket az előírásokat minden egyes adatkezelési folyamat, tevékenység során, annak teljes tartama alatt figyelembe kell venni.

5. A Szabályzat további célja, hogy meghatározza a Társaság egyes feladatai során vezetett, személyes adatokat tartalmazó nyilvántartások vezetésének és működtetésének jogszerű rendjét, valamint biztosítsa a személyes adatok védelme elveinek és az adatbiztonság követelményeinek érvényesülését.

1.3. A szabályzat személyi hatálya

6. Jelen Szabályzat személyi hatálya kiterjed a Társaság munkavállalóira, továbbá azon természetes személyekre (a továbbiakban: érintett), akik személyes adatait a jelen Szabályzat hatálya alá tartozó adatkezelések tartalmazzák, továbbá azon érintettekre, akik jogait vagy jogos érdekeit az adatkezelés érinti. A Társaság megbízásából személyes adatok kezelését vagy feldolgozását végzők esetén az erre a jogviszonyra a Társaság által kötött szerződésben a GDPR 28. cikkének megfelelően rendelkezni kell arról, hogy a Társaság által megbízott adatfeldolgozó a feladata ellátása során hogyan juttatja érvényre jelen Szabályzat rendelkezéseit.

1.4. A szabályzat tárgyi hatálya

7. A Szabályzat tárgyi hatálya a Társaság mindazon adatkezeléseire kiterjed – függetlenül attól, hogy az adatkezelés elektronikusan vagy papíralapon történik –, amelyek

    a/ az egészségügyi ellátás nyújtásához kapcsolódó adatkezelést valósítanak meg;
    b/ az egészségügyi ellátáson kívüli ügyfélkapcsolati jellegű adatkezelést valósítanak meg (a Társasággal kapcsolatba lépni szándékozó, kapcsolatban álló vagy kapcsolatban állt személyek, beleértve ezek meghatalmazottait, képviselőit is);
    c/ foglalkoztatási jogviszonyhoz kapcsolódó adatkezelést valósítanak meg (a Társasággal munkaviszonyban vagy egyéb foglalkoztatási jogviszonyban (együtt: foglalkoztatási jogviszony) álló, állt, vagy foglalkoztatási jogviszonyba lépni szándékozó személyek);
    d/ a Társasággal szerződéses kapcsolatban álló társaságok képviselőinek, kapcsolattartóinak az adataira vonatkoznak.

1.5. Dokumentálási kötelezettség

8. A Társaság felelős a személyes adatok kezelésére vonatkozó alapelvek [GDPR 5. cikk (1) bek.] betartásáért. A Társaságnak képesnek kell lennie a személyes adatok kezelésére vonatkozó alapelvek betartásának igazolására [GDPR 5. cikk (2) bek. – elszámoltathatóság elve]. A megfelelőség igazolása különösen az adatkezeléshez kapcsolódó döntéseket megalapozó körülmények és a döntések (pl. az adatkezelés feltételeit meghatározó döntéselőkészítő iratok), az érintetteknek szóló adatkezelési tájékoztatók, az érintettől származó nyilatkozatok (pl. hozzájáruló nyilatkozatok, az adatkezelési tájékoztató megismerését igazoló dokumentumok), továbbá a személyes adatokat tartalmazó (elektronikus vagy papír alapú) dokumentumok szervezeten belüli vagy azon kívüli mozgásának megfelelő dokumentálásával történik. A Társaság – a GDPR 30. cikkének megfelelően – nyilvántartást vezet az általa végzett adatkezelésekről.

9. A megfelelőség igazolása adatvédelmi incidens esetén különösen az incidenssel érintettek körének, az incidenssel érintett személyes adatok körének, az incidens kezelése során tett intézkedéseket megalapozó körülmények és a döntések dokumentálásával történik. A Társaság – a GDPR 33. cikkének megfelelően – nyilvántartást vezet a bekövetkezett incidensekkel kapcsolatos tényekről és intézkedésekről.

2. Alapfogalmak

10. Jelen Szabályzat alkalmazása során a GDPR 4. cikkében meghatározott fogalmakon kívül az alábbi fogalmakat kell alkalmazni:

a/ adatbiztonság: a személyes adatok jogosulatlan kezelése, így különösen jogosulatlan megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni szervezési, technikai megoldások, valamint eljárási szabályok összessége; az adatkezelés azon állapota, amelyben az adatok sérülésének, illetéktelen felhasználásának, megsemmisülésének kockázati tényezőit – és ezáltal a fenyegetettséget – a szervezési, műszaki megoldások és intézkedések a minimálisra csökkentik,

b/ Adatkezelési Tevékenységek Nyilvántartása: jelen szabályzatban meghatározott adattartalmú, folyamatosan karbantartott nyilvántartás;

c/ adatvédelmi felügyeleti hatóság: a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság),

d/ adatvédelmi hatásvizsgálat: olyan vizsgálat, amelyet a Társaság kijelölt munkavállalója köteles elvégezni, amennyiben valamely tervezett adatkezelés – figyelemmel annak jellegére, hatókörére, körülményeire és céljaira, ideértve különösen az új technológiák alkalmazásának esetét – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, és amelynek célja annak megállapítása, hogy a tervezett adatkezelés a személyes adatok védelmét hogyan érinti. Az adatvédelmi hatásvizsgálat egy olyan eljárás, amelynek során az adatkezelő a tervezett adatkezelési műveletet vagy műveleteket áttekinti, megvizsgálja az adatkezelés érintettekre gyakorolt esetleges hatását, felméri annak kockázatait, a kockázatok kezelésének módját, és mindezt megfelelően dokumentálja,

e/ adatvédelmi incidens jellege: személyes adatok megsemmisülése, személyes adatok jogosulatlan megsemmisítése, személyes adatok rendelkezésre állásának sérülése, személyes adatok integritásának sérülése, személyes adatok elvesztése, személyes adatok jogosulatlan megváltoztatása, személyes adatok jogosulatlan közlése vagy jogellenes továbbítása, személyes adatokhoz történő jogosulatlan hozzáférés, személyes adatok bizalmasságának sérülése (pl. titoksértés) stb.

f/ adatvédelmi tisztviselő: a Társaság szervezetében működő, a GDPR 39. cikkében meghatározott feladatokat a Társaság jelen szabályzatában foglaltak szerint ellátó, a Társasággal foglalkoztatási jogviszonyban álló természetes személy,

g/ álnevesítés (pszeudonimizálás): a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni,

h/ anonimizálás: a nyilvántartási rendszerben tárolt személyes adatok közül a személyazonosításra alkalmas adatok eltávolítása olyan, visszafordíthatatlan módon, hogy a nyilvántartási rendszerben megmaradó adatok a továbbiakban semmilyen körülmények között nem teszik lehetővé egy természetes személy azonosítását,

i/ dolgozói személyes adat: a Társasággal foglalkoztatási jogviszonyban álló személyek adata,

j/ érdekmérlegelési teszt: jogos érdeken alapuló adatkezelés tervezett bevezetése esetén annak írásbeli dokumentálása, hogy az adatkezelő számba vette az

adatkezelést megalapozó érdekeket, érveket, valamint az érintettek személyes adatok védelméhez fűződő – a tervezett adatkezelés ellen ható – jogait és érdekeit, és ezen érdekek és érvek összevetésével megalapozza az adatkezelés bevezetését vagy a bevezetés elutasítását,

k/ titkosítás: az adatok olyan átalakítása, melynek során az adat értelmezhetetlenné válik a megfelelő kulcs ismerete nélkül,

l/ törlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása a továbbiakban már nem lehetséges. A törlés célja megvalósítható anonimizálással

m/ munkaköri alkalmassági vizsgálat: annak megállapítása, hogy egy meghatározott munkakörben és munkahelyen végzett tevékenység által okozott megterhelés a vizsgált személy számára milyen igénybevételt jelent és annak képes-e megfelelni;

n/ szakmai alkalmassági vizsgálat: a szakma elsajátításának megkezdését megelőző, illetőleg a képzés és az átképzés időszakában az alkalmasság véleményezése érdekében végzett orvosi vizsgálat;

o/ személyi higiénés alkalmassági vizsgálat: annak megállapítása, hogy a járványügyi szempontból kiemelt munkaterületen munkát végző személy fertőző megbetegedése mások egészségét nem veszélyezteti, illetve meghatározott esetekben kórokozó hordozása mások egészségét nem veszélyezteti;

p/ munkát végző személy: aki nem szervezett munkavégzés keretében járványügyi szempontból kiemelt munkaterületen tevékenységet folytat;

q/ ügyvezető: a Társaság által az adatkezelési feladatok ellátásával megbízott ügyvezető

3. A szabályzathoz kapcsolódó jogszabályok, belső szabályzatok

GDPR	Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [az Infotv-nek a GDPR hatálya alá eső adatkezelésekre alkalmazandó szabályai – lsd. Infotv. 2. § (2) és (4) bekezdése]
Eüak.	1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről, és a végrehajtására kiadott jogszabályok
Eütv.	1997. évi CLIV. törvény az egészségügyről, és a végrehajtására kiadott jogszabályok
Ebtv.	1997. évi LXXXIII. törvény kötelező egészségbiztosítás ellátásairól, és a végrehajtására kiadott jogszabályok
Mt.	2012. évi I. törvény a Munka Törvénykönyvéről
	a munkaköri, szakmai, illetve személyi higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről szóló 33/1998. (VI. 24.) NM rendelet

	a foglalkozás-egészségügyi szolgálatról szóló 89/1995. (VII. 14.) Korm. rendelet

4. Az adatvédelmi tevékenység szervezete és irányítása

4.1. Az adatvédelmi tevékenység ellátásában résztvevők

11. Az adatvédelmi tevékenység irányításában és ellátásában a Társaság által megbízottak, illetve foglalkoztatási jogviszonyban állók feladatkörükön belül – az alábbiak szerint vesznek részt.

12. Az ügyvezető felelős azért, hogy a Társaság – mint adatkezelő, illetve adatfeldolgozó – működése az adatvédelmi szabályoknak megfeleljen. Ennek érdekében:
    a/ gondoskodik az adatvédelmi tevékenység irányításában és ellátásában résztvevők kijelöléséről, feladataik, az adatvédelmi tárgyú ügyekkel kapcsolatos döntési jogkörök meghatározásáról, az egyes adatkezelési döntési szintek kialakításáról;
    b/ biztosítja az adatvédelmi tevékenység irányításához és ellátásához, valamint az érintett jogai gyakorlásához szükséges személyi és tárgyi feltételeket;
    c/ felelős az adat- és titokvédelmi, valamint biztonsági és információbiztonsági szabályzatok kiadásáért és betartatásáért;
    d/ gondoskodik arról, hogy az adatvédelmi tevékenység során esetleg előforduló, feltárt hiányosságok megszűntetéséről, szükség szerint a felelősségre vonásról;
    e/ megbízza a Társaság adatvédelmi tisztviselőjét, és az adatvédelmi tisztviselő nevét és elérhetőségét bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak;
    f/ biztosítja a Társaság adatvédelmi tisztviselője feladatainak ellátásához szükséges személyi és tárgyi feltételeket,
    g/ biztosítja, hogy az adatvédelmi tisztviselő véleményét kikérjék a Társaság adatvédelmi tárgyú vagy adatvédelmi vonatkozású belső szabályzatainak előkészítése során,
    h/ az adatvédelmi tisztviselő szükség szerinti közreműködésével ellátja az érintetti jogok gyakorlásával kapcsolatos panaszok, beadványok megválaszolását.

13. Az informatikai feladatot ellátó a Társaság Informatikai biztonsági szabályzatában meghatározott feladatkörében:
    a/ ellátja az informatikai biztonsági biztonsággal kapcsolatos feladatokat
    b/ ellátja az informatikai fejlesztéseknél és beszerzéseknél a beépített adatvédelem kontrolljai meglétének biztosításával, az adatminőség biztosításával, az informatikai biztonság kockázatarányos szintjét biztosító jogosultsági és naplózási rendszer kialakításának megfelelőségével, a biztonságos szoftverfejlesztés alapelveinek érvényesítésével kapcsolatos feladatokat,
    c/ az informatikai rendszerek üzemeltetése területén ellátja a személyes adatok kezelésével kapcsolatos technikai védelem megvalósítását, ellátja – az Informatikai biztonsági szabályzatban meghatározott – hatáskörébe tartozó információbiztonsági feladatokat, valamint rendelkezésre állási kontrollok biztosítását, a tárolt és továbbított személyes adatok bizalmasságának védelmét, az incidensfelderítési és -kezelési tevékenység támogatását,

d/ gondoskodik az információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról.

4.2. Az adatvédelmi tisztviselő

14. Az adatvédelmi tisztviselőt az ügyvezető nevezi ki.

15. Az adatvédelmi tisztviselő független, függetlensége biztosítása érdekében szakmai feladatai ellátása során utasítást nem fogadhat el, szakmai feladatai ellátásával összefüggésben – ha foglalkoztatási jogviszonyban áll - nem bocsátható el. Jelen Szabályzatban foglalt tevékenysége ellátása során autonóm, szakmai ügyekben kizárólag az ügyvezetőnek tartozik felelősséggel.

16. a Társaság elősegíti az adatvédelmi tisztviselő megfelelő szakmai feladatellátását, ennek érdekében a Társaság biztosítja különösen az adatvédelmi tisztviselő feladatai végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáférést, valamint a szakértői szintű ismereteinek fenntartásaihoz szükséges forrást, valamint az informatikai és a biztonsági szakterület együttműködése révén az adatvédelmi tisztviselő bevonását:
    a/ a megfelelő technikai-eljárási intézkedésekhez szükséges források meghatározása során annak érdekében, hogy teljesüljenek az adatvédelem alapelvei a technikai vívmányok alkalmazása (beépített adatvédelem) és az adatvédelem-barát megoldások (alapértelmezett adatvédelem) révén;
    b/ a felügyeleti hatósággal történő együttműködés során, amellyel az adatvédelmi tisztviselő tartja a kapcsolatot.

17. Az adatvédelmi tisztviselő véleményét – a jelen szabályzat rendelkezései szerint – ki kell kérni az adatkezelést érintő döntések, szerződések és belső szabályzatok tervezetéről.

18. Az adatvédelmi tisztviselőt tisztsége fennállása alatt és annak megszűnését követően titoktartási kötelezettség terheli a tevékenysége során tudomására jutott minden olyan információ tekintetében, amely nem minősül közérdekű vagy közérdekből nyilvános adatnak.

19. A Társaságnál nem lehet adatvédelmi tisztviselő az a természetes személy, aki a Társaságnál az adatkezelési tevékenység céljainak, kereteinek, eszközeinek meghatározásáról dönt, különösen az ügyvezető.

20. Az adatvédelmi tisztviselő az adatvédelmi tisztviselői feladatokon kívül az ügyvezető döntése alapján más munkakörhöz kötődő feladatokat is elláthat, amennyiben azok nem eredményeznek összeférhetetlenséget.

21. Az adatvédelmi tisztviselő nevét és elérhetőségeit a Társaság honlapján, székhelyén, telephelyén a nyilvánosság részére mindenkor elérhetővé kell tenni. A Társaság továbbá közli az adatvédelmi tisztviselő nevét és elérhetőségét a Nemzeti Adatvédelmi és Információszabadság Hatósággal.

22. Az adatvédelmi tisztviselő feladatai:
    a/ közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;

b/ ellenőrzi a GDPR, az Infotv. és az adatkezelésre vonatkozó más jogszabályok, valamint a jelen szabályzat, továbbá a Társaság egyéb belső szabályzatai rendelkezéseinek a megtartását, belső adatvédelmi ellenőrzési eljárást folytat le;
c/ kivizsgálja a neki címzett panaszokat, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;
d/ az informatikai szakterülettel együttműködve elkészíti az adatvédelmi és adatbiztonsági szabályzatot;
e/ gondoskodik az adatvédelmi ismeretek oktatásáról;
f/ a személyes adatok kezelésére vonatkozó előírásokról tájékoztatást nyújt, tanácsot ad;
g/ személyes adatot is kezelő új informatikai rendszer bevezetése során közreműködik a beépített adatvédelem alapelve érvényesülésének érdekében, vagy ha szükséges, az adatvédelmi hatásvizsgálat lefolytatásában;
h/ az adatvédelmi incidenskezeléssel kapcsolatban ellátja a jelen szabályzat szerinti feladatokat;
i/ kapcsolatot tart és együttműködik a Hatósággal;

5. Adatkezelés bevezetésével, módosításával és megszüntetésével kapcsolatos feladatok

5.1. Adatkezelés bevezetésével kapcsolatos feladatok

23. Jogszabályban elrendelt vagy jogszabály rendelkezése miatt szükséges, vagy a Társaság döntése alapján létrehozandó nyilvántartási rendszer (a továbbiakban együtt: adatkezelés) bevezetése esetén, amennyiben az természetes személyek adatainak kezelésével (beleértve meglévő nyilvántartási rendszer adatainak új célú felhasználásával, új célú adatkezelés bevezetésével, nyilvántartási rendszerbe adatok felvételével, adatok tárolásával, harmadik személynek továbbításával stb.) jár, az adatkezelés bevezetése során a [döntéselőkészítés rendjére vonatkozó belső szabályokat] e fejezet rendelkezéseit figyelembe véve kell alkalmazni.

24. Adatkezelés bevezetése az ügyvezető döntése alapján történik. Az adatvédelmi tisztviselő véleményét az adatkezelés bevezetését megelőzően ki kell kérni.

25. Az adatkezelőket szükség esetén be kell vonni az adatkezelés feltételeinek kidolgozási folyamatába.

26. Az új adatkezelés szakmai megfelelőségéért az ügyvezető, ezen belül az adatvédelmi megfelelőségéért az adatvédelmi tisztviselő, az informatikai, információbiztonsági megfelelőségért pedig az informatikai feladatokat ellátó a felelős.

5.2. Az adatvédelmi hatásvizsgálat elvégzésének módszertana

27. Ha az új adatkezelés - különösen új technológiákat alkalmazó típusa - valószínűsíthetően magas kockázattal jár a természetes személyek jogaira nézve az adatkezelést megelőzően adatvédelmi hatásvizsgálatot kell végezni. Olyan, egymással hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló kockázatokkal járnak, egyetlen adatvédelmi hatásvizsgálat (továbbiakban: hatásvizsgálat) keretei között is értékelhetők.

28. A hatásvizsgálat elvégzésének szükségességéről az ügyvezető – minden új adatkezelés bevezetését megelőzően - kikéri az adatvédelmi tisztviselő véleményét.

29. A hatásvizsgálat elvégzését a tervezett adatkezelésért felelős koordinálja az adatvédelmi tisztviselő elvi iránymutatásai alapján. A hatásvizsgálat megállapításait írásban kell rögzíteni. Az elkészült hatásvizsgálati dokumentációt az adatvédelmi tisztviselőnek kell megküldeni, amely azt 8 munkanapon belül szakmai szempontból véleményezi. Ha az ügyvezető úgy ítéli meg, hogy az új adatkezelés semmiképpen nem jár magas kockázattal a természetes személyek jogaira, úgy ezt meg kell indokolni. A bevezetendő adatkezelés kizárólag a hatásvizsgálat elvégzését követően kezdhető meg.

30. Adatvédelmi hatásvizsgálatot a GDPR 35. cikk (3) bekezdésében, illetve a Nemzeti Adatvédelmi és Információszabadság Hatóság által közzétett jegyzékben (https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf) szereplő adatkezelések, adatkezelési műveletek esetén mindenképpen el kell végezni.

31. Az előző pontban említett jegyzéken kívül minden olyan bevezetésre kerülő – különösen az új technológiákat alkalmazó – adatkezelés esetén is hatásvizsgálatot kell végezni, mely adatkezelés az ügyfélre tekintettel jelentős joghatással bír/az ügyfelet (jogait) jelentős mértékben érinti.

32. A hatásvizsgálat módszertanát minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani. A hatásvizsgálat elvégzésére alkalmazó szoftver megtalálható a Nemzeti Adatvédelmi és Információszabadság Hatóság honlapján (https://naih.hu/adatvedelmi-hatasvizsgalati-szoftver.html).

33. A hatásvizsgálat első részében összefoglalóan le kell írni a tervezett adatkezelést, különösen:
    a/ az adatkezelő és a tervezett közös adatkezelő vagy adatfeldolgozó megjelölését;
    b/ az adatkezelés jogalapját, célját (az adatkezeléstől várt előnyöket, az adatkezelés szükségességét), terjedelmét (időben és a kezelt adatok volumenében);
    c/ az adatkezeléssel érintettek körét, a kezelendő adatok körét, az adatok megőrzésének tervezett idejét,
    d/ azon adatkezelők megjelölését, akiknek az adatot továbbítani tervezik, és különösen, ha harmadik országba vagy nemzetközi szervezet felé tervezik az adattovábbítást;
    e/ az adatkezelésre vonatkozó követelmények (jogszabályi követelmények vagy magatartási kódexből, szabványból eredő követelmények);
    f/ az adatkezelés folyamatának a leírását.

34. A hatásvizsgálat második részében ki kell fejteni és meg kell indokolni
    a/ az adatkezelés szükségességének és arányosságának garanciáit,
    b/ az érintett jogait biztosító garanciák érvényesülését.

35. A hatásvizsgálat harmadik részében azonosítani és értékelni kell az adatkezelés potenciális kockázatait, és a kockázatok enyhítésére tervezett, elfogadott intézkedéseket, megoldásokat.

36. A hatásvizsgálat negyedik része tartalmazza a tervezett adatkezelés értékelését:
    a/ a meghatározott szempontok értékelését a tekintetben, hogy azok egyenként megfelelőek, további intézkedésekkel megfelelőek lehetnek, illetve nem megfelelőek;

b/ a tervezett kiegészítő intézkedések végrehajtásának ütemtervét;
c/ annak egyértelmű rögzítését, hogy a tervezett adatkezelés valószínűsíthetően magas kockázattal jár-e a természetes személyek jogaira nézve, és ennek alapján az adatkezelés megkezdhető-e, illetve szükség van-e az adatvédelmi felügyeleti hatósággal való konzultációra.

37. A hatásvizsgálat megállapításait az adatkezelési tevékenységbe vissza kell csatolni és ennek megfelelően kell kialakítani az adatkezelést.

38. A hatásvizsgálatot legalább évente dokumentáltan felül kell vizsgálni, szükség esetén újra el kell végezni.

5.3. Adatkezelés megszüntetésével kapcsolatos feladatok

39. Amennyiben a kezelt adatokra a továbbiakban nincs szükség (az adatkezelési cél megvalósult vagy a kezelt adatokra vonatkozó megőrzési idő letelt), vagy jogszabályi változások miatt, vagy az adatvédelmi felügyeleti hatóság vagy bíróság döntése értelmében az adatok kezelését meg kell szüntetni.

5.4. Az érdekmérlegelési teszt elvégzésének módszertana

40. Amennyiben a Társaság valamely adatkezelésének a Társaság vagy harmadik személy jogos érdeke a jogalapja [GDPR 6. cikk (1) bekezdés f) pont], érdekmérlegelési tesztet kell elvégezni és azt dokumentálni. Jogos érdek az a törvényes, kellően pontosan megfogalmazott, valós és fennálló, illetve elérhető előny, amelyet az adatkezelő származtat – vagy a harmadik személy származtathat – az adatkezelésből.

41. Az érdekmérlegelési tesztet az adatvédelmi tisztviselő végzi el. Az érdekmérlegelési tesztet írásban kell elvégezni. A jogos érdeken alapuló adatkezelés kizárólag az érdekmérlegelési teszt elvégzését és az adatvédelmi tisztviselő véleményének beszerzését követően kezdhető meg.

42. Az érdekmérlegelési teszt módszertanát, a megválaszolandó kérdéseket minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani, az alábbi kérdések köre csak orientáló, a tervezett adatkezelés szempontjából releváns egyéb kérdésekkel bővíthető. Abból kell kiindulni, hogy bármilyen adatkezelés beavatkozás az érintett magánszférájába, és e beavatkozás jogosságát, szükségességét és arányosságát kell bizonyítani a mérlegelés során.

43. Az érdekmérlegelési teszt részei:
a/ a tervezett adatkezelés leírása és az annak keretében kezelni tervezett személyes adatok (körének vagy típusának) meghatározása,
b/ az adatkezelő vagy azon harmadik fél jogos érdekének azonosítása, akinek az adatkezelés érdekében áll (Miért szükséges az adatkezelés?),
c/ az érintett érdekeinek, jogainak azonosítása (Arányban van-e az adatkezelés az érintett magánszférájának korlátozásával?),
d/ az adatkezelő (vagy harmadik fél) és az érintettek érdekeinek összevetése,
e/ a személyes adatok védelme biztosítékainak leírása,
f/ az érdekmérlegelési teszt eredménye.

6. Az érintetti jogok gyakorlásának elősegítése

6.1. Az adatkezelési tevékenység nyilvánossága

44. A Társaság a honlapján egy olyan, „Adatvédelem” nevű oldalt tart fenn, amely bármely érintett számára közvetlenül elérhető. Az „Adatvédelem” oldalon közzé kell tenni:
    a/ a Társaság jelen szabályzatát;
    b/ a Társaság általános – a Klinika szolgáltatásait igénybe vevők részére készült - adatkezelési tájékoztatóját;
    c/ a Társaság egyes adatkezelési tevékenységeihez kapcsolódó esetleges (különös) adatkezelési tájékoztatókat, ide nem értve a munkavállalók, egyéb jogviszonyban foglalkoztatottak adatainak kezelésére vonatkozó tájékoztatókat;
    d/ közös adatkezelés esetén a közös adatkezelésben résztvevők közötti megállapodás lényegét, ha azt a különös adatkezelési tájékoztatók nem tartalmazzák;
    e/ tájékoztatást arról, hogy az érintett kihez fordulhat az adatkezelést érintő kérdéseivel, panaszaival (az adatkezelő és az adatvédelmi tisztviselő elérhetősége, az adatvédelmi felügyeleti hatóság elérhetősége);

45. A Társaság honlapjának olyan aloldalain, amelyek személyes adatok kezelésével járó egyes tevékenységekről tájékoztatnak (pl. egyes ellátási formák igénybevételének feltételeit tartalmazzák), el kell helyezni legalább az adott tevékenységhez kapcsolódó
    a/ adatkezelési tájékoztatóra mutató hivatkozást;
    b/ egyéb releváns dokumentumokat (pl. betegtájékoztatókat, formanyomtatványokat).

6.2. A gyermekek tájékoztatáshoz való jogának biztosítása

46. A Társaság ügyvezetése gondoskodik arról, hogy a Társaság által kezelt vagy a Társasággal más módon kapcsolatba kerülő gyermekek az adataik kezelésével kapcsolatos tájékoztatást a gyermek számára világos és elérhető módon megkapják. A tájékoztatás az alábbi módokon történhet:
    a/ a gyermek törvényes képviselője útján: a gyermeket érintő adatkezelésről a gyermekkel kapcsolatba lépő munkavállaló tájékoztatja a gyermek törvényes képviselőjét,
    b/ a gyermek vagy a törvényes képviselő kifejezett kérésére a gyermekkel kapcsolatba lépő munkavállaló – a fentieken túlmenően – biztosítja a gyermek részére a rövid, szóbeli tájékoztatást is az adatai kezelésével kapcsolatban;
    c/ amennyiben a gyermek életkora és érettsége lehetővé teszi, a gyermekkel kapcsolatba lépő munkavállaló írásban közvetlenül a gyermeket is tájékoztatja az adatkezelésről.

6.3. Korlátozottan cselekvőképes és cselekvőképtelen (gondokság alatt álló) személyek tájékoztatáshoz való jogának biztosítása

47. A Társaság ügyvezetése gondoskodik arról, hogy az általuk ellátott korlátozottan cselekvőképes vagy cselekvőképtelen nagykorú személyek törvényes képviselői, illetve – állapotától függően – a korlátozottan cselekvőképes személy is megfelelő tájékoztatást kapjon a személyes adatok kezeléséről. A törvényes képviselőt írásban nyilatkoztatni kell, hogy a tájékoztatást közli a gondnoksága alatt álló érintettel.

6.4. Gyermekek és gondokság alatt álló személyek személyes adatainak kezelése hozzájáruló nyilatkozat alapján

48. A Társaság ügyvezetője gondoskodik arról, hogy a Társasággal a tevékenysége alapján kapcsolatba kerülő gyermekek, illetve gondnokság alatt álló személyek tekintetében – amennyiben az adatkezelés hozzájáruláson alapul – a személyes adatok kezeléséhez való hozzájárulást törvényes képviselőjük adja meg.

49. A hozzájáruló nyilatkozatnak tartalmaznia kell a törvényes képviselőnek arra vonatkozó nyilatkozatát, hogy jogosult az érintett helyett a jognyilatkozat megtételére.

50. Amennyiben az érintett törvényes képviselői (pl.: szülői felügyelet gyakorlására jogosult szülők) eltérő nyilatkozatot tesznek az adatkezeléshez való hozzájárulásról, úgy az adatkezeléshez való hozzájárulást meg nem adottnak kell tekinteni.

6.5. Hozzátartozók tájékoztatása

51. A Társaság ügyvezetése gondoskodik arról, hogy a Társasággal tevékenysége alapján kapcsolatba kerülő személyek hozzátartozóit az adatvédelmi szabályoknak megfelelően tájékoztassák, amelyben – az érintett személy képességeit is figyelembe véve – magát az érintettet is bevonhatja.

52. A hozzátartozók adatainak kezelését önálló adatkezelési tevékenységként kell feltüntetni az adatkezelési tevékenységek között, és az adatkezelési tájékoztatóban ki kell térni a hozzátartozók adatainak kezelésére.

7. Az érintettől származó kérelmek, panaszok megválaszolásának rendje

7.1. Az adatvédelmi bejelentések típusai

53. Az érintettől a következő, személyes adatai Társaság általi kezelését érintő beadványok érkezhetnek:
    a/ bejelentheti a Társaság által nyilvántartott adatok megváltozását;
    b/ tájékoztatást kérhet személyes adatai [milyen személyes adato(ka)t, milyen célból, milyen jogalapon, milyen forrásból szerezve, meddig kezeli a Társaság, alkalmaz-e automatizált döntéshozatalt és/vagy profilalkotást az adatkezelés során, és a személyes adatokat kinek, milyen jogalapon továbbítja)] – hozzáféréshez való jog (GDPR 15. cikk);
    c/ kérheti pontatlanul nyilvántartott személyes adatai helyesbítését, illetve vitathatja a nyilvántartott személyes adatok pontosságát – helyesbítéshez való jog (GDPR 16. cikk);
    d/ kérheti nyilvántartott személyes adatai törlését – törléshez való jog (GDPR 17. cikk);
    e/ kérheti személyes adatai kezelésének korlátozását (a pontatlan adat helyesbítéséig terjedő időre; a jogellenesen kezelt személyes adatok törlése helyett; jogszerűen kezelt, de szükségtelenné vált adatok törlése helyett az érintett kérésére az érintett jogi igényének előterjesztéséhez, érvényesítéséhez vagy védelméhez; jogos érdeken alapuló adatkezelés elleni tiltakozás elbírálásáig) – az adatkezelés korlátozásához való jog (GDPR 18. cikk);

f/ kérheti, hogy a rá vonatkozó, általa a Társaság rendelkezésére bocsátott és elektronikus adatbázisban, a hozzájárulása, a személyes adatok különleges kategóriái esetén a kifejezett hozzájárulása, vagy a vele kötött szerződés teljesítéséhez szükséges jogalapon automatizált módon kezelt adatait tagolt, széles körben használt, géppel olvasható formátumban megkapja – adathordozhatósághoz való jog (GDPR 20. cikk);

g/ tiltakozhat személyes adatai kezelése ellen, ha az adatkezelés jogalapja az adatkezelő vagy harmadik személy jogos érdeke, illetve közérdekű feladat vagy közfeladat ellátása, beleértve mindkét esetben a profilalkotást is – tiltakozási jog gyakorlása (GDPR 21. cikk);

h/ automatizált döntéshozatal alkalmazása esetén az adatkezelő részéről emberi beavatkozást kérhet, közölheti álláspontját [GDPR 22. cikk (3) bek.];

i/ kifogást nyújthat be az automatizált döntéshozatal alkalmazásával meghozott döntéssel szemben [GDPR 22. cikk (3) bek.];

j/ panaszt nyújthat be a személyes adatok kezelését, illetve a GDPR szerinti jogai gyakorlását érintően [GDPR 77. cikk, 38. cikk (4) bek.];

k/ az elhunyt érintett életében tett meghatalmazottjaként vagy közeli hozzátartozójaként gyakorolni kívánja az érintett egyes jogait [Infotv. 25. §].

7.2. Az adatvédelmi beadványok elintézése

54. Az adatvédelmi tisztviselő bármely esetben – az érintett beadványának kivizsgálása, illetve saját ellenőrzése eredményeként, továbbá az adatvédelmi felügyeleti hatóság vagy bíróság döntése végrehajtásaként – kezdeményezheti személyes adat helyesbítését, törlését vagy az adatkezelés korlátozását (zárolást).

55. A Társasághoz érkező személyes adatok kezelésére vonatkozó beadványokat a Társaság – a GDPR 12. cikkében írt határidők figyelembevételével – köteles intézni, az alábbi kiegészítésekkel és eltérésekkel:

a/ a beadvány érkezése dátumát és időpontját pontosan rögzíteni kell;

b/ a panasz kivizsgálását az adatvédelmi tisztviselő végzi. A panasz kivizsgálása során a Társaság foglalkoztatottjai kötelesek az adatvédelmi tisztviselővel együttműködni.

c/ az érintettnek saját adatairól szóbeli tájékoztatás csak egyértelmű azonosítás után lehetséges. Amennyiben a beadványozó nem azonosítható vagy kétség merül fel a beadványozó személyazonosságát illetően, meg kell megkísérelni a beadványozó személyének azonosítását, beleértve a személyes megjelenés igénylését.

d/ amennyiben a beadvány a GDPR hatálya alá tartozó beadványnak minősül, a beadványozót a beadvány érkezését követő 8 napon belül értesíteni kell a beadvány érkezéséről, a megválaszolására nyitva álló határidőről, illetve arról, hol kaphat további felvilágosítást a beadványáról. Nem kell ilyen értesítést küldeni a beadványozónak, ha a beadványban kért intézkedést ezen időn belül teljesítik;

e/ amennyiben a beadványt előreláthatóan nem lehet a GDPR 12. cikk (3) bekezdése szerinti határidőben megválaszolni, a beadványozót legkésőbb a beadvány érkezését követő 21. napon elküldött levélben vagy elektronikus üzenetben tájékoztatni kell a határidő meghosszabbításának szükségességéről, okairól és az új határidőről;

f/ amennyiben a beadványt – a beadványozó kérelme ellenére – nem lehet, vagy nem célszerű elektronikus úton megválaszolni (a kért dokumentumokat nem lehet vagy nem célszerű ilyen úton elküldeni), fel kell venni a kapcsolatot a beadványozóval annak érdekében, hogy kölcsönösen elfogadható megoldást találjanak. Különösen indokolt a beadványozóval a kapcsolatfelvétel, ha a beadványozó egészségügyi adat

megküldését kéri nem biztonságos elektronikus úton. A kapcsolatfelvételre olyan időben kell sort keríteni, hogy a beadványt akkor is meg lehessen válaszolni a határidő betartásával, ha a beadványozó ragaszkodik a nem biztonságos elektronikus úthoz.

g/ Elektronikus úton egészségügyi adat csak a beadványozó kifejezett kérésére és csak oly módon küldhető, ha előzőleg a beadványozó figyelmét felhívták a kockázatokra, és a beadványozó ezek után megerősíti a szándékát, egyúttal tudomásul véve a Társaság felelősségkizáró nyilatkozatát, továbbá az adatok bizalmassága, integritása és rendelkezésre állása biztosítható (pl. jelszavas védelemmel ellátott file, ahol a jelszót külön csatornán küldik el).

56. Az adatvédelmi beadványokról olyan ügyiratnyilvántartást kell vezetni, amely segítségével bármikor egyértelműen azonosíthatók a beadványok, nyomon követhetők a beadványok elintézése során tett intézkedések.

8. Az adatbiztonsági intézkedések (technikai és szervezési intézkedések) meghatározása és végrehajtása

57. Az adatbiztonsági szabályok kialakítása során különös gondot kell fordítani a beépített és az alapértelmezett adatvédelem elveinek (GDPR 25. cikk) betartására, valamint arra, hogy a Társaság által alkalmazott adatbiztonsági intézkedések megfeleljenek a GDPR 32. cikkében írt követelményeknek.

58. Az adatbiztonsági szabályok tervezetének kialakításába – a véleményezésre vonatkozó egyéb szabályokat nem érintve – az adatvédelmi tisztviselőt be kell vonni.

59. Az adatbiztonság elveinek egy adatkezelés bevezetésének (lsd. 23. pont) vagy személyes

60. Az adatbiztonsági intézkedések mindennapi működésben történő betartására a Társaság minden foglalkoztatottja, valamint a Társaság informatikai rendszereihez hozzáférő személy köteles.

9. A közös adatkezelői és az adatfeldolgozói szerződések megkötésének és végrehajtása ellenőrzésének szabályai

9.1. Közös adatkezelés

61. Közös adatkezelésnek minősül, ha az adatkezelés céljait és eszközeit a Társaság egy vagy több másik adatkezelővel közösen határozza meg (GDPR 26. cikk).

62. A közös adatkezelésről szóló megállapodásban meg kell határozni különösen

a/ az adatkezelés célját, a kezelendő adatok körét, az adatkezelés időtartamát, az alkalmazandó adatbiztonsági intézkedéseket, az adatkezelés egyéb feltételeit,

b/ azt, hogy a közös adatkezelésben érintett egyes adatkezelők

ba/ mely adatkezelési műveleteket (pl. hozzájáruló nyilatkozatok felvétele, adatok tárolása, adatok felhasználása stb.) végzik,

bb/ az érintett tájékoztatását hogyan végzik (pl. melyik adatkezelő készíti el az adatkezelési tájékoztatót és bocsátja az érintettek rendelkezésére stb.),

bc/ az érintett jogai gyakorlását hogyan biztosítják (pl. személyes felvilágosítás nyújtása stb.),

bd/ az esetleges jogellenes adatkezelés következményeit milyen arányban viselik;

c/ az adatvédelmi incidens észlelése esetén követendő eljárást, különösen azt, hogy

ca/ az adatvédelmi incidens tudomásra jutása esetén a másik adatkezelő adatvédelmi tisztviselőjét (adatvédelmi tisztviselő hiányában a kijelölt kapcsolattartót) haladéktalanul kötelesek értesíteni az adatvédelmi rendellenességről vagy incidensről,

cb/ egymással kötelesek együttműködni az adatvédelmi rendellenesség vagy incidens okának kiderítésében és következményeinek felszámolásában,

cc/ az egyes adatkezelőket mely adatvédelmi incidensek tekintetében terheli a bejelentési kötelezettség;

d/ kijelölnek-e kapcsolattartót az érintettek számára, és ha igen, a kapcsolattartó személyét és elérhetőségét naprakészen kell tartani,

e/ a megállapodásról az érintett rendelkezésére bocsátandó összefoglalót, aminek – a GDPR 13-14. cikkeiben írtakon túl – tartalmaznia kell az adatkezelők által végzett adatkezelési műveleteket, és azt, hogy az érintett hogyan gyakorolhatja jogait a közös adatkezelés tekintetében.

63. A közös adatkezelés szükségességét az adatvédelmi tisztviselő vizsgálja meg.

64. Amennyiben döntés születik a közös adatkezelés bevezetéséről, az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselő előkészíti a közös adatkezelésről szóló megállapodás tervezetét (benne a közös adatkezelőknek az érintettek számára kijelölendő kapcsolattartójának kijelölésével kapcsolatos döntést, valamint a közös adatkezelésre vonatkozó megállapodásnak az érintettek rendelkezésére bocsátható lényegi elemeit) és azt megküldi a Társaság ügyvezetőjének.

9.2. Adatfeldolgozói szerződések

65. Amennyiben harmadik országbeli adatfeldolgozó igénybevétele merül fel, először abban a kérdésben kell dönteni, hogy a harmadik országbeli adatfeldolgozó képes-e a GDPR-nak megfelelő adatbiztonsági követelmények teljesítésére. Amennyiben a harmadik országbeli adatfeldolgozó nem képes a GDPR által elvárt adatbiztonsági követelmények érvényesítésére, illetve nem tud a GDPR szerinti garanciákat nyújtani a személyes adatok kezelésére, az adatfeldolgozóval nem köthető szerződés.

66. Adatfeldolgozó igénybevétele esetén az adatfeldolgozóval kötendő szerződésnek tartalmaznia kell a GDPR 28. cikk (1)-(4) bekezdésében foglalt tartalmi elemeket.

67. Az adatfeldolgozóval kötendő szerződésben

a/ a kellő részletességgel meg kell határozni az adatfeldolgozó, vagy az adatfeldolgozó által igénybe veendő további adatfeldolgozó (al-adatfeldolgozó) által betartandó adatbiztonsági szabályokat, amelyek nem lehetnek kevésbé szigorúak, mint a Társaság által alkalmazott adatbiztonsági intézkedések, és az adatfeldolgozónak az adatbiztonsági intézkedések végrehajtásával kapcsolatos feladatait;

b/ rögzíteni kell az adatfeldolgozónak az érintettől származó kérelmek, panaszok megválaszolásában való közreműködésének eljárásrendjét;

c/ rögzíteni kell az adatfeldolgozó kötelezettségeit adatvédelmi incidens észlelése esetén, így különösen

ca/ az adatvédelmi incidens tudomásra jutása esetén a Társaság adatvédelmi tisztviselőjét haladéktalanul köteles értesíteni az adatvédelmi incidensről,

cb/ köteles együttműködni a Társaság adatvédelmi tisztviselőjével az adatvédelmi incidens okának feltárásban és következményeinek felszámolásában,

cc/ köteles együttműködni az adatvédelmi incidens bejelentésének teljesítésében,

d/ rögzíteni kell az adatfeldolgozó kötelezettségét az adatvédelmi hatásvizsgálat elvégzésében, illetve a hatásvizsgálatban azonosított kockázatok alakulásának figyelemmel kísérésében, az adatkezeléssel járó kockázatok változásának jelzésében, illetve az adatvédelmi hatásvizsgálatok utóellenőrzésben.

68. Az adatfeldolgozó igénybevételének szükségességét az adatkezelési tisztviselő az adatkezelés bevezetéséről való döntés előkészítése részeként vizsgálja meg. Ezt a szabályt kell alkalmazni akkor is, ha az adatfeldolgozó igénybevételéről az adatkezelés folyamán születik döntés.

69. Az adatbiztonsági intézkedések technikai megfelelőségének megítélése az informatikai feladatokat ellátó szakember hatáskörébe tartozik.

70. Amennyiben döntés születik az adatfeldolgozó igénybevételéről, az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselő előkészíti az adatfeldolgozóval kötendő szerződés tervezetét.

71. A Társaság, maga is adatfeldolgozónak minősülhet, így például a vele szerződést kötő munkáltatóknál foglalkoztatott természetes személyek személyes adatai vonatkozásában, ezért a partner munkáltatók mindegyikével adatfeldolgozói megállapodást köt.

10. Az Adatkezelési Tevékenységek Nyilvántartása

72. Az adatvédelmi tisztviselő vezeti az adatkezelési tevékenységek nyilvántartását (Adatkezelési Tevékenységek Nyilvántartása). Az Adatkezelési Tevékenységek Nyilvántartása valamennyi, a Társaság általi adatkezelés esetén tartalmazza:
    a/ az adatkezelés célját,
    b/ az adatkezelés jogalapját,
    c/ az érintettek körét,
    d/ az érintettekre vonatkozó személyes adatok kategóriáit,
    e/ az adatok kezelésének időtartamát vagy az adattörlés ideje megállapításának szempontjait;
    f/ a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló, valamint nemzetközi szervezethez történő adattovábbításokat és azok garanciáinak leírását is,
    g/ az adatfeldolgozó nevét és címét, a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét,
    h/ az adatkezelő, valamint közös adatkezelés esetén a közös adatkezelők megnevezését és elérhetőségét,
    i/ az adatvédelmi tisztviselő nevét és elérhetőségét,
    j/ ha lehetséges, az adatbiztonsági intézkedések általános leírását,

73. Az Adatkezelési Tevékenységek Nyilvántartásának célja a Társaság, mint adatkezelő adatkezelési tevékenysége átláthatóságának biztosítása, és ezzel az esetleges felesleges, párhuzamos adatkezelések elkerülése.

74. A Társaság adatvédelmi tisztviselője az Adatkezelési Tevékenységek Nyilvántartásába való betekintést – a Hatóság képviselőin kívül – a Társaság ügyvezetése és adatkezelést végző foglalkoztatottjai, továbbá a közös adatkezelést érintő rész tekintetében a közös adatkezelő részére biztosítja.

75. Az Adatkezelési Tevékenységek Nyilvántartásába bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezelésért felelős 5 munkanapon belül köteles bejelenteni az adatvédelmi tisztviselőnek, aki ennek megfelelően módosítja az Adatkezelési Tevékenységek Nyilvántartásának adatait.

11. Az adatvédelmi incidensek kezelése

11.1. Az adatvédelmi incidens minősítése

76. Adatvédelmi incidens csak akkor következik be, ha az adatbiztonsági intézkedések – akár vétlen, akár szándékos – megsértésének következtében bekövetkezik a személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés:
    a/ súlyos incidens: olyan incidens (pl. adatvesztés, adatsérülés), mely valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve (pl.: a jogosulatlan hozzáféréssel érintett adatok esete; az olyan adatsérülés, adatvesztés, amelynél az adatok naplózott állományból nem állíthatóak helyre). Magas kockázatúnak minősül az az eset, amely fizikai, vagyoni vagy nem vagyoni károkat okozhat az érintetteknek, pl. az érintetteknek a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, pénzügyi veszteséget, jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését eredményezheti;
    b/ enyhe incidens: minden incidens, amely nem tartozik az a) pont alá (pl. átmeneti szolgáltatásleállás, - kiesés a Társaság munkavállalói által használt olyan belső rendszerekben, amely nem jár adatsérüléssel vagy adatvesztéssel).

77. Az adatvédelmi incidensre vonatkozó szabályokat kell alkalmazni a Társaság tulajdonát képező adathordozón, mobiltelefonon, laptopon, egyéb számítástechnikai eszközön tárolt adatokra, továbbá a Társaság alkalmazottainak olyan saját tulajdonú eszközein (adathordozó, mobiltelefon, laptop, egyéb számítástechnikai eszköz) tárolt adatokra, amely eszközöket munkavégzéshez, munkaköri feladatok ellátásához, hivatalos célból használhat. Az adatvédelmi incidensre vonatkozó szabályokat a Társaság birtokában lévő papíralapú adathordozón lévő adatokra is alkalmazni kell.

78. Az elektronikus információs rendszereket érintő (biztonsági vagy egyéb) események adatvédelmi incidensnek is minősülnek, amennyiben személyes adatokra nézve következik be. A jelen Szabályzat adatvédelmi incidens kezelésére vonatkozó rendelkezéseinek alkalmazása nem mentesít az elektronikus információs rendszereket érintő (biztonsági vagy egyéb) események kezelésére (bejelentésére, kivizsgálására stb.) vonatkozó szabályok betartása alól, azaz az elektronikus információs rendszereket érintő (biztonsági vagy egyéb) események kezelésére vonatkozó szabályokat jelen Szabályzat előírásaival párhuzamosan alkalmazni kell.

11.2. Az adatvédelmi incidens bejelentése

79. Az a munkavállaló, aki a Társaság által kezelt vagy feldolgozott személyes adatokkal kapcsolatban, vagy a Társaság szerződéses partnere által kezelt vagy feldolgozott személyes adataival kapcsolatban adatvédelmi incidenst vagy annak gyanúját észleli, köteles azt haladéktalanul bejelenteni az adatvédelmi tisztviselőnek

80. Az adatvédelmi incidensről szóló bejelentésben ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az adatvédelmi incidenssel érintett személyes adatok kategóriáit és hozzávetőleges számát, továbbá a bejelentő nevét és elérhetőségét.

81. A közös adatkezelésről szóló szerződésben [GDPR 26. cikk], illetve az adatfeldolgozóval kötendő szerződésben [GDPR 28. cikk] egyértelműen rendelkezni kell a másik adatkezelő, illetve az adatfeldolgozó azon kötelezettségéről, hogy az adatvédelmi incidensről a Társaságot köteles haladéktalanul, de legkésőbb az észlelést követő 24 órán belül értesíteni. A szerződésnek tartalmaznia kell továbbá a közös adatkezelő, illetve az adatfeldolgozó kötelezettségeit adatvédelmi incidens bejelentésében és kivizsgálásában.

11.3. Incidensprotokoll általában

82. Az informatikai feladatokat ellátó bevonásával a riasztásokban szereplő sérülékenység elhárításakor a következők szerint kell eljárni:
    a/ figyelembe kell venni a különböző informatikai biztonsági szabályozásokban a sérülékenységek elhárítására vonatkozó rendelkezéseket;
    b/ amennyiben a riasztás személyes adatot tartalmazó alkalmazás sérülékenységével kapcsolatban keletkezett, az adatvédelmi tisztviselőt haladéktalanul tájékoztatni kell;
    c/ amennyiben a Társaság rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt azzal az eszközzel azonnal el kell kezdeni;
    d/ ha a Társaság nem rendelkezik automatizált módszerrel az adott sérülékenység elhárítására, akkor azt manuális módon kell azonnal elkezdeni;
    e/ amennyiben a sérülékenység elhárítása belső erőforrásból nem kivitelezhető, akkor külső szakértőket kell bevonni az elhárítás folyamatába.

83. A papíralapon kezelt iratokkal kapcsolatban a jelen Szabályzat személyi hatálya alá tartozó személyek kötelesek a személyes adatokat tartalmazó iratokat a munkavégzés befejezését követően, ahol ennek feltételei biztosítottak, zárható szekrényben, zárral ellátott fiókban tárolni. Ahol a tárolás előbb nevesített feltételei nem adottak, az irodahelyiség ajtajának kulcsra zárásával kell a személyes adatok védelmét biztosítani abban az esetben, ha az irodahelyiségben senki sem tartózkodik. A Szabályzat személyi hatálya alá tartozó személyek kötelesek a Társaság egyéb belső szabályzatai, így különösen az iratkezelés rendjéről, illetve a biztonsági előírásokról szóló mindenkor hatályos belső szabályzatnak megfelelően eljárni.

11.4. Az adatvédelmi incidens kivizsgálása

84. Adatvédelmi incidens (papíralapú és nem papíralapú adatokra vonatkozóak egyaránt) felmerülése esetén a Társaság adatvédelmi tisztviselője megvizsgálja, és kategorizálja a

bekövetkezett incidenst, és meghatározza az esetleges elhárítás érdekében szükséges további intézkedéseket.

85. Az adatvédelmi incidensről az adatvédelmi tisztviselő haladéktalanul értesíti az ügyvezető.

86. A bejelentés előzetes megvizsgálása során az alábbi szempontokat kell figyelembe venni:
    a/ a bejelentés személyes adatot érint-e,
    b/ amennyiben a bejelentés személyes adatot érint, megállapítható-e a személyes adatok köre,
    c/ megállapítható-e az incidensben érintett személyek köre,
    d/ a hatályos jogszabályok és belső szabályok alapján megállapítható-e, hogy személyes adat jogellenes kezelése vagy feldolgozása (beleértve a törlést/megsemmisítést is) történt,
    e/ az incidens valószínűsíthetően magas kockázattal jár-e az érintettek jogaira és szabadságaira nézve,
    f/ melyek az adatvédelmi incidensből eredő, valószínűsíthető következmények,
    g/ a Társaság által alkalmazott technikai és szervezési védelmi intézkedések az incidensben érintett személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik-e az adatokat.

11.5. Az érintett tájékoztatása a súlyos adatvédelmi incidensről

87. Súlyos adatvédelmi incidens esetén a Társaság – az érintettel kapcsolatban rendelkezésére álló elérhetőségeken, ennek hiányában vagy alkalmazásuk lehetetlensége esetén (GDPR 34. cikk) a Társaság honlapján közzétett közlemény útján – indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

88. Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább az alábbi információkat és intézkedéseket:
    a/ az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
    b/ az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
    c/ az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

89. Az érintettet nem kell tájékoztatni, amennyiben az incidens nem jár magas kockázattal, és a következő feltételek bármelyike teljesül:
    a/ a Társaság megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;
    b/ a Társaság az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az említett magas kockázat a továbbiakban valószínűsíthetően nem áll fenn;
    c/ a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

90. A Társaság ügyvezetőjének döntése alapján a Társaság az érintetteket a Társaság honlapján vagy országos lefedettségű sajtótermékben közzétett hirdetmény útján is értesítheti.

11.6. Az adatvédelmi incidens bejelentése a Hatóságnak

91. Az adatvédelmi incidensről szóló bejelentést a Hatóság mindenkori kapcsolati pontjára kell eljuttatni.

92. A bejelentés összeállításának és beadásának felelőse az adatvédelmi tisztviselő. Az adatvédelmi incidensről szóló bejelentéshez szükséges információkat az adatvédelmi tisztviselő rendelkezésére kell bocsátani.

93. Az adatvédelmi incidensről szóló 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 eredő, valószínűsíthető következményeket;
    d/ ismertetni kell a Társaság által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

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

11.7. Az adatvédelmi incidensek nyilvántartása

95. Az adatvédelmi incidensekről az adatvédelmi tisztviselő elektronikus nyilvántartást vezet.

96. A nyilvántartásban rögzíteni kell:
    a/ az incidensben érintett személyes adatok körét és számát,
    b/ az adatvédelmi incidenssel érintettek körét és számát,
    c/ az adatvédelmi incidens észlelésének és tudomásszerzésének időpontját,
    d/ az adatvédelmi incidens körülményeit, hatásait,
    e/ az adatvédelmi incidens elhárítására megtett intézkedéseket,
    f/ az adatvédelmi incidenssel kapcsolatban adott tájékoztatások adatait.

97. A Társaság az adatvédelmi incidens kivizsgálásával kapcsolatos papíralapú és elektronikus dokumentumokat 10 évig köteles megőrizni. Az adatvédelmi incidensek vizsgálata során keletkezett, iktatott dokumentumokat az adatvédelmi tisztviselő az incidens vizsgálatának lezárásától számított 10 évig őrzi meg, illetéktelenek számára hozzá nem férhető, zárt helyen.

12. Harmadik országba irányuló adattovábbítás különös szabályai

98. Amennyiben személyes adatnak harmadik országba történő továbbításának szükségessége merül fel, az adatkezelő köteles az adatvédelmi tisztviselő véleményét kérni az adattovábbítás megengedhetőségéről, illetve az adattovábbítás lehetséges módjáról.

13. Adatvédelmi audit

99. Az adatvédelmi audit célja, hogy az adatvédelmi tisztviselő meggyőződjön arról, hogy a Társaság az adatvédelemmel kapcsolatos jogszabályoknak és belső szabályzatoknak megfelelően kezelik-e az adatokat.

100. Az adatvédelmi tisztviselő éves ellenőrzési tervet készít. Az éves ellenőrzési tervnek az ellenőrzés várható időpontját, továbbá az ellenőrzés tárgykörét kell tartalmaznia. Az éves ellenőrzési tervet legkésőbb adott év február 28. napjáig kell elkészíteni és a Társaság ügyvezetője részére bemutatni.

101. Az éves ellenőrzési tervet az ügyvezető hagyja jóvá.

102. Az ellenőrzés során az adatvédelmi tisztviselő a Társaság irodahelységeibe beléphet, az – ellenőrzés tárgyával összefüggésben kezelt – irataiba betekinthet, a munkatársaktól tájékoztatást kérhet adott üggyel kapcsolatos adatkezelésről.

103. Az adatvédelmi tisztviselő az ellenőrzés megtörténtéről jegyzőkönyvet készít. A jegyzőkönyv az ellenőrzés lefolytatásának tényét, annak időpontját és időtartamát, továbbá a tevékenység során rögzített tényeket, megállapításokat, információkat tartalmazza.

14. A Társaság tevékenysége alapján történő adatkezelések

14.1. Munkaviszonnyal és tagsági jogviszonnyal kapcsolatos adatkezelések

14.1.1. Munkaügyi, személyzeti nyilvántartás

A munkavállalóktól csak olyan adatok kérhetők és tarthatók nyilván, illetve olyan munkaköri alkalmassági vizsgálatok (ideértve a munka alkalmassági orvosi vizsgálatot is) elvégzését lehet kérni, amelyet munkaviszonyra vonatkozó szabály ír elő, és amelyek munkaviszony létesítéséhez, fenntartásához és megszüntetéséhez szükségesek és a munkavállaló személyiségi jogait nem sértik.

A Társaság jogszabályi kötelezettség, (GDPR 6. cikk (1) bekezdése c) pont) jogcímén munkaviszony létesítése, fenntartása vagy megszűnése céljából kezeli a munkavállaló alábbi adatait:

1. név,
2. születési név,
3. születési helye, ideje,
4. anyja neve,
5. lakcíme,
6. állampolgársága,
7. adóazonosító jele,
8. TAJ száma,
9. nyugdíjas törzsszám (nyugdíjas munkavállaló esetén),
10. telefonszám,
11. e-mail cím,
12. személyazonosító igazolvány száma,
13. lakcímkártya száma,
14. bankszámlaszáma (ha a fizetés bankszámlára való átutalással történik),
16. munkába lépésének kezdő és befejező időpontja, valamint napi munkakezdésének és munkavégzésének időpontja,

17. munkaköre,
18. iskolai végzettségét, szakképzettségét igazoló okmány másolata,
19. önéletrajz,
20. a munkabérrel, a bérfizetéssel, és egyéb juttatásokkal kapcsolatos adatok,
21. a munkavállaló munkabéréből jogerős határozat vagy jogszabály, illetve írásbeli hozzájárulása alapján levonandó tartozás, illetve ennek jogosultságát igazoló okirat,
22. az előző munkaviszony megszűnésének módja, az erre vonatkozó iratok,
23. erkölcsi bizonyítvány (ha a munkakörhöz szükséges),
24. a munkaköri alkalmassági vizsgálatokra vonatkozó iratok,
25. önkéntes nyugdíj - és egészségpénztári tagság esetén a pénztár megnevezése, azonosító száma és a munkavállaló tagsági száma,
26. külföldi munkavállaló esetén útlevélszám; munkavállalási jogosultságot igazoló dokumentumának megnevezése és száma,
27. munkavállalót ért baleset jegyzőkönyvében rögzített adatok
28. saját személygépkocsi hivatali célra történő használata esetén a gépjármű törzskönyv másolata
29. ha a munkakör ellátásához jogosítvány szükséges, a jogosítvány száma és másolata.

Betegségre és szakszervezeti tagságra vonatkozó adatokat a Társaság csak a Munka Törvénykönyvében meghatározott jog, vagy kötelezettség teljesítése céljából kezel. A személyes adatok tárolásának időtartama a munkaviszony megszűnését követő 50 év. Az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a Munka Törvénykönyvén, a társadalombiztosítási-, adó- és nyugdíjjogszabályokon alapul.

A munkáltató a munkaszerződés megkötésével egyidejűleg az Adatkezelési Tájékoztató átadásával tájékoztatja a munkavállalót személyes adatainak kezeléséről és a személyhez fűződő jogairól.

14.1.2. Alkalmassági vizsgálatokkal - ideértve a munkaköri alkalmassági orvosi vizsgálatot is - kapcsolatos adatkezelés

A munkavállalóval csak olyan alkalmassági vizsgálat végeztethető el, amelyet jogszabály vagy munkaviszonyra vonatkozó szabály ír elő, vagy amely munkaviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges. A vizsgálat előtt a munkavállalókat részletesen tájékoztatni kell többek között arról, hogy az alkalmassági vizsgálat milyen készség, képesség felmérésére irányul, a vizsgálat milyen eszközzel, módszerrel történik, és miért kell. Amennyiben jogszabály írja elő a vizsgálat elvégzését, akkor tájékoztatni kell a munkavállalókat a jogszabály címéről és számáról, valamint a pontos jogszabályhelyről is.

A kezelhető személyes adatok köre: a munkaköri, valamint az egészségügyi alkalmasság ténye, és az ehhez szükséges alkalmassági feltételek teljesítése.

Az adatkezelés jogalapja: jogi (a Munka törvénykönyve, a munkaköri, szakmai, illetve személyi higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről szóló 33/1998. (VI. 24.) NM rendeletben előírt) kötelezettség teljesítése (GDPR 6. cikk (1) bek. c) pont), valamint a személyes adatok különleges kategóriáira vonatkozóan a foglalkoztatást szabályozó jogi előírásokból fakadó kötelezettség teljesítése (GDPR 9. cikk (2) bek. b) pont.

A személyes adatok kezelésének célja: munkaviszony létesítése, fenntartása, munkakör betöltése.

A személyes adatok kezelésének időtartama: a munkaviszony megszűnését követő 3 év.

14.1.3. Felvételre jelentkező személyek adatainak kezelése

A kezelhető személyes adatok köre: a természetes személy neve, születési helye, ideje, anyja neve, lakcíme, képesítési adatok, az erre vonatkozó bizonyítvány-másolatok, fénykép, telefonszám, e-mail cím, önéletrajz, a benyújtott pályázat, a jelentkezőről készített munkáltatói értékelés (feljegyzés).

A személyes adatok kezelésének célja: jelentkezés, pályázat elbírálása, a kiválasztott személlyel munkaszerződés megkötése.

Az érintettet az elutasító döntés meghozatalát követő 15 napon belül tájékoztatni kell arról, ha a munkáltató nem őt választotta az adott állásra.

Az adatkezelés jogalapja: az érintett hozzájárulása (GDPR 6. cikk (1) bek a) pont).

A személyes adatok tárolásának időtartama: az érintett hozzájárulása hiányában a jelentkezés, pályázat elbírálását követő 15 nap. A ki nem választott jelentkezők személyes adatait a 16. napon törölni kell. Törölni kell annak a jelentkezőnek az adatait is, aki jelentkezését, pályázatát visszavonta.

A munkáltató csak az érintett kifejezett, egyértelmű és önkéntes hozzájárulása alapján őrizheti meg a fenti határidőn túl a pályázatokat, feltéve, ha azok megőrzésére a jogszabályokkal összhangban álló adatkezelési célja elérése érdekében szükség van. E hozzájárulást a felvételi eljárás lezárását követően – a 15 napos határidő leteltéig - kell kérni a jelentkezőktől. Ebben az esetben személyes adatok tárolásának időtartama: 5 év.

14.1.4. Munkára alkalmas állapot vizsgálata

Az adatkezelés célja: A Társaság a munkavállalója munkavégzésének helyén a munkavállaló csak biztonságos munkavégzésre alkalmas állapotban, a munkavédelemmel kapcsolatos utasítások és előírások betartásával tartózkodhat és végezhet munkát. A munkavállaló köteles a munkatársaival együttműködni, és munkáját úgy végezni, hogy az mások, vagy saját testi épségét ne veszélyeztesse.

A Társaság által kezelt intézmények teljes területén tilos a munkavállalóknak alkoholos befolyásoltság, vagy egyéb tudatmódosító szer hatása alatt tartózkodniuk. Mivel ezen tudatmódosító szerek hatása alatt a munkaképesség nem biztosítható, a Munka törvénykönyvéről szóló 2012.évi I. tv, valamint a munkavédelemről szóló 1993.évi XCIII. tv. alapján a munkáltató köteles meggyőződni róla, hogy a munkavállalók betartják-e az alkoholfogyasztás tilalmával kapcsolatos szabályokat. A munkáltató ellenőrzési gyakorlata nem járhat az emberi méltóság megsértésével, így a vizsgálat csak a Társaság munkavédelmi utasításával összhangban megvalósítható. A munkavállaló alkoholszondás ellenőrzésével kapcsolatosan jegyzőkönyvet kell felvenni.

A kezelt adatok köre: Munkavállaló neve, anyja neve, születési helye, ideje, beosztása, ellenőrzés eredménye

Az adatkezelés jogalapja: A munkavédelemről szóló 1993.évi XCIII. tv 60. § valamint a munka törvénykönyvéről szóló 2012.évi I. tv 52. §-a, tehát jogi kötelezettség teljesítése (GDPR 6. cikk

(1) bek. c) pont), valamint a személyes adatok különleges kategóriáira vonatkozóan a foglalkoztatást szabályozó jogi előírásokból fakadó kötelezettség teljesítése (GDPR 9. cikk (2) bek. b) pont.

Az adatkezelés időtartama: Az ellenőrzés tényéből származtatott jogok és kötelességek által megalapozott igények érvényesítési lehetőségeiből fakadó határidő.

14.1.5. Megváltozott munkaképességű munkavállalók adatainak kezelése

A megváltozott munkaképességű munkavállalókra adatkezelési szempontból azonos szabályok vonatkoznak, mint a Társaság saját alkalmazottjaira, rájuk vonatkozóan azonban bővebb a kezelt adatok köre. A Társaság törvényi előírás alapján kezeli a megváltozott munkaképességű munkavállalók egészségi állapotára vonatkozó adatokat.

Kezelt adatok köre: a munkaviszony létesítésére vonatkozó adatokon kívül a munkavállaló fogyatékosságát igazoló, szükséges orvosi dokumentumok.

Az adatkezelés jogalapja: jogi kötelezettség teljesítése (GDPR 6. cikk (1) bek. c) pont), valamint a személyes adatok különleges kategóriáira vonatkozóan a foglalkoztatást szabályozó jogi előírásokból fakadó kötelezettség teljesítése (GDPR 9. cikk (2) bek. b) pont.

14.1.6. E-mail fiók használatának ellenőrzésével kapcsolatos adatkezelés

Ha a Társaság e-mail fiókot bocsát a munkavállaló rendelkezésére – ezen e-mail címet és fiókot a munkavállaló kizárólag munkaköri feladatai céljára használhatja, annak érdekében, hogy a munkavállalók ezen keresztül tartsák egymással a kapcsolatot, vagy a munkáltató képviseletében levelezzenek az ügyfelekkel, más személyekkel, szervezetekkel.

A munkavállaló az e-mail fiókot személyes célra nem használhatja, a fiókban személyes leveleket nem tárolhat.

A munkáltató jogosult az e-mail fiók teljes tartalmát és használatát rendszeresen – 3 havonta - ellenőrizni, ennek során az adatkezelés jogalapja a munkáltató jogos érdeke. Az ellenőrzés célja az e-mail fiók használatára vonatkozó munkáltatói rendelkezés betartásának ellenőrzése, továbbá a munkavállalói kötelezettségek (Mt. 8.§, 52. §) ellenőrzése.

Az ellenőrzésre és adatkezelésre a munkáltató vezetője, vagy a munkáltatói jogok gyakorlója jogosult.

Amennyiben az ellenőrzés körülményei nem zárják ki ennek lehetőségét, biztosítani kell, hogy a munkavállaló jelen lehessen az ellenőrzés során.

Az ellenőrzés előtt tájékoztatni kell a munkavállalót arról, hogy milyen munkáltatói érdek miatt kerül sor az ellenőrzésre, munkáltató részéről ki végezheti az ellenőrzést, - milyen szabályok szerint kerülhet sor ellenőrzésre (fokozatosság elvének betartása) és mi az eljárás menete, - milyen jogai és jogorvoslati lehetőségei vannak az e-mail fiók ellenőrzésével együtt járó adatkezeléssel kapcsolatban.

Az ellenőrzés során a fokozatosság elvét kell alkalmazni, így elsődlegesen az email címéből és tárgyából kell megállapítani, hogy az a munkavállaló munkaköri feladatával kapcsolatos, és nem személyes célú. Nem személyes célú e-mailek tartalmát a munkáltató korlátozás nélkül vizsgálhatja.

Ha jelen szabályzat rendelkezéseivel ellentétben az állapítható meg, hogy a munkavállaló az e-mail fiókot személyes célra használta, fel kell szólítani a munkavállalót, hogy a személyes adatokat haladéktalanul törölje. A munkavállaló távolléte, vagy együttműködésének hiánya esetén a személyes adatokat az ellenőrzéskor a munkáltató törli. Az e-mail fiók jelen szabályzattal ellentétes használata miatt a munkáltató a munkavállalóval szemben munkajogi jogkövetkezményeket alkalmazhat.

A munkavállaló az e-mail fiók ellenőrzésével együtt járó adatkezeléssel kapcsolatban e szabályzatnak az érintett jogairól szóló fejezetében írt jogokkal élhet.

A kezelt adatok köre: Munkavállaló neve, e-mail címe, ellenőrzés eredménye

Az adatkezelés jogalapja: A munka törvénykönyvéről szóló 2012. évi I. tv 8. §., 52. §, tehát jogi kötelezettség teljesítése (GDPR 6. cikk (1) bek. c) pont)

Az adatkezelés időtartama: Az ellenőrzés tényéből származtatott jogok és kötelességek által megalapozott igények érvényesítési lehetőségeiből fakadó határidő.

14.1.7. Számítógép, laptop, tablet ellenőrzésével kapcsolatos adatkezelés

A Társaság által a munkavállaló részére munkavégzés céljára rendelkezésre bocsátott számítógépet, laptopot, tabletet a munkavállaló kizárólag munkaköri feladata ellátására használhatja, ezek magáncélú használatát a Társaság megtiltja, ezen eszközökön a munkavállaló semmilyen személyes adatot, levelezését nem kezelheti és nem tárolhatja. A munkáltató ezen eszközökön tárolt adatokat ellenőrizheti. Ezen eszközök munkáltató általi ellenőrzésére és jogkövetkezményire egyebekben az előbbi 14.1.6. pont rendelkezései irányadók.

14.1.8. A munkahelyi internethasználat ellenőrzésével kapcsolatos adatkezelés

A munkavállaló csak a munkaköri feladatával kapcsolatos honlapokat tekintheti meg, a személyes célú munkahelyi internethasználatot a munkáltató megtiltja.

A munkaköri feladatként a Társaság nevében elvégzett internetes regisztrációk jogosultja a Társaság, a regisztráció során a társaságra utaló azonosítót, jelszót kell alkalmazni. Amennyiben a személyes adatok megadása is szükséges a regisztrációhoz, a munkaviszony megszűnésekor azok törlését köteles kezdeményezni a Társaság.

A munkavállaló munkahelyi internethasználatát a munkáltató ellenőrízheti, amelyre és jogkövetkezményire az 14.1.6. pont rendelkezései irányadók.

14.1.9. Céges mobiltelefon használatának ellenőrzésével kapcsolatos adatkezelés

A munkáltató engedélyezi a céges mobiltelefon magáncélú használatát egyedileg meghatározott értékhatárig, a mobiltelefon a továbbiakban csak munkavégzéssel összefüggő célokra használható, és a munkáltató valamennyi kimenő hívás hívószámát és adatait, továbbá a mobiltelefonon tárolt adatokat ellenőrizheti.

A munkavállaló köteles bejelenteni a munkáltatónak, ha a céges mobiltelefont magáncélra használta. Ezesetben az ellenőrzés akként folytatható le, hogy a munkáltató hívásrészletezőt kér a telefonszolgáltatótól és felhívja a munkavállalót arra, hogy a dokumentumon a magáncélú hívások esetében a hívott számokat tegye felismerhetetlenné. A munkáltató előírhatja, hogy a magáncélú hívások költségeit a munkavállaló viselje.

Egyebekben az ellenőrzésre és jogkövetkezményire az 14.1.6. pont rendelkezései irányadóak.

14.1.10. A munkabalesetek és a foglalkozási megbetegedések nyilvántartásával kapcsolatos adatkezelés

Az adatkezelés célja: A Társaságra vonatkozó munkavédelmi szabályok betartása

A kezelt adatok köre: Sérült, beteg munkavállaló neve, anyja neve, születési helye, ideje, TAJ száma, beosztása, munkabaleset, foglalkozási betegség leírása

Az adatkezelés jogalapja: jogi kötelezettség teljesítése (GDPR 6. cikk (1) bek. c) pont), valamint a személyes adatok különleges kategóriáira vonatkozóan a munkáltató feladatait meghatározó jogi előírásokból fakadó kötelezettség teljesítése (GDPR 9. cikk (2) bek. b) pont.

Az adatkezelés időtartama: a baleset, foglalkozási betegség következményeinek megszűnését követő 5 év

14.1.11. A Társaság tagjainak (üzletrész-tulajdonosainak) nyilvántartása

A Társaság tagjainak cégjegyzékben szereplő adatai nyilvánosak, azokhoz adatvédelmi intézkedések nem köthetők. Azok az adatok azonban, amelyek a cégjegyzéknek nem részei, ugyanolyan védelmet kell, hogy élvezzenek, mint bármely más természetes személy adatai.

Ezek az adatok a következők:

- születési név,
- születési hely,
- adóazonosító jele,
- TAJ száma,
- telefonszám,
- e-mail cím,
- személyi igazolvány száma,
- lakcímkártya száma,
- bankszámlaszáma (ha bármely pénzbeli juttatás bankszámlára való átutalással történik),
- törzsbetét mértéke.

Az adatkezelés jogalapja: a tagnak a Társasággal kötött szerződésének teljesítéséhez szükséges az adatkezelés: azaz a GDPR 6. cikk (1) bekezdés b) pontja.

Adatok tárolásának időtartama: A személyes adatok tárolásának időtartama a tagsági viszony megszűnését követő 5 év.

14.2. A Társaság által nyújtott egészségügyi szolgáltatások adatkezelése

A Társaság által alkalmazott rendszer az egészségügyi szolgáltatás nyújtása körében az alábbi adatokat kezeli:

- a beteg személyazonosító adatai (családi és utónév, leánykori név, nem, születési hely és idő, anya leánykori családi és utóneve, lakóhely, tartózkodási hely, társadalombiztosítási azonosító jel (TAJ szám), telefonszám, e-mail cím);

- biztosító által finanszírozott ellátás esetén a biztosító/biztosítás adatai;
- egészségpénztár által finanszírozott ellátás esetén az egészségpénztár adatai;
- cselekvőképes beteg esetén az értesítendő személy neve, lakcíme, elérhetősége;
- kiskorú, illetve a cselekvőképességet részlegesen vagy teljesen korlátozó gondnokság alatt álló beteg esetében a törvényes képviselő neve, lakcíme, elérhetősége;
- a kórelőzmény, a kórtörténet;
- a vizsgálati eredmény;
- a diagnózist és a gyógykezelési tervet megalapozó vizsgálati eredmények, a vizsgálatok elvégzésének időpontja;
- az ellátást indokló betegség megnevezése, a kialakulásának alapjául szolgáló betegség, a kísérőbetegségek és szövődmények;
- egyéb, az ellátást közvetlenül nem indokoló betegség, illetve a kockázati tényezők megnevezése;
- az elvégzett beavatkozások ideje és azok eredménye;
- a gyógyszeres és egyéb terápia, annak eredménye;
- a beteg gyógyszer-túlérzékenységére vonatkozó adatok;
- a betegnek, illetőleg tájékoztatásra jogosult más személynek nyújtott tájékoztatás tartalma;
- a beteg önrendelkezéshez való joga alapján szükséges a beteg beleegyezése az egészségügyi ellátáshoz, ezen belegyező nyilatkozat;
- a beteg az Eü.tv-ben foglalt feltételekkel visszautasíthatja az egészségügyi ellátást, ezen visszautasítás ténye, valamint időpontja;

Az adatkezelés célja:

- az egészség megőrzésének, javításának, fenntartásának előmozdítása;
- a Társaság eredményes gyógykezelési tevékenységének elősegítése, ideértve a szakfelügyeleti tevékenységet is;
- az érintett egészségi állapotának nyomon követése;
- a betegjogok érvényesítése;
- egészségügyi szolgáltatások nyújtása;
- az adatkezelő és az ügyfél között létrejött szolgáltatási szerződés teljesítése, végrehajtása, a szerződés alapján vállalt szolgáltatás nyújtása;
- a szerződéssel kapcsolatos kötelezettségek és jogosultságok igazolása;
- a szerződéssel kapcsolatosan esetlegesen felmerülő követelések érvényesítése, behajtása és értékesítése;
- kapcsolattartás;
- az igénybe vett szolgáltatások nyomon követése;

Az adatkezelés jogalapja az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény rendelkezései, valamint az érintett önkéntes hozzájárulása.

Az adatszolgáltatás elmaradásának lehetséges következményei: az egészségügyi szolgáltatás nyújtásának elmaradása.

Az adatkezelés időtartama: Az egészségügyi dokumentációt az adatfelvételtől számított legalább 30 évig, a zárójelentést legalább 50 évig kell megőrizni. Ettől eltérően a képalkotó

diagnosztikai eljárással készült felvételt annak készítésétől számított 10 évig, a felvételről készített leletet a felvétel készítésétől számított 30 évig kell megőrizni.

A számviteli törvény az üzleti évről készített beszámolót, az üzleti jelentést, valamint az azokat alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá a naplófőkönyvet, vagy más, a törvény követelményeinek megfelelő nyilvántartást olvasható formában legalább 8 évig köteles megőrizni.

A fentebb nem érintett adatokat az érintett törlési kérelmének beérkezését követő 60 napon belül kell törölni.

14.2.1. A beteg (érintett) adatainak felvétele

A társaságnál a betegellátás az előjegyzési rendszeren (MyHealzz) keresztül történik. Az előjegyzés során a Healzz elnevezésű programban kerülnek rögzítésre a beteg személyes, és a vizsgálat elvégzéséhez szükséges egészségügyi adatai.

14.2.1.1. A MyHealzz rendszerben (ügyfélportálon) történő időpontfoglaláshoz kapcsolódó adatkezelés

Az ügyfélportál használatához szükséges minimálisan szükséges adatok: jelszó, vezeték- és keresztnév, születési idő, e-mail cím, telefonszám, regisztráció időpontja;

Az ügyfélportál használata során a felhasználó által opcionálisan megadható adtok: egyéb egészségügyi adatok, illetve ilyen adatokat tartalmazó dokumentumok, kép- és/vagy hangfelvételek.

Az érintettek köre: az ügyfélportálon regisztrált valamennyi érintett.

Az adatgyűjtés célja: szolgáltató az ügyfélportál teljes körű használata, pl. szolgáltatás nyújtására irányuló szerződés létrehozása, tartalmának meghatározása, módosítása, teljesítésének figyelemmel kísérése, az abból származó díjak számlázása, valamint az azzal kapcsolatos követelések érvényesítése, regisztráció céljából kezeli a Felhasználók személyes adatait.

Az adatkezelés időtartama, az adatok törlésének határideje: A regisztráció törlésével azonnal. Kivéve a számviteli bizonylatok esetében. A számvitelről szóló 2000. évi C. törvény 169. § (2) bekezdése alapján a könyvviteli elszámolást közvetlenül és közvetetten alátámasztó számviteli bizonylatot (ideértve a főkönyvi számlákat, az analitikus, illetve részletező nyilvántartásokat is), legalább 8 évig kell olvasható formában, a könyvelési feljegyzések hivatkozása alapján visszakereshető módon megőrizni.

Az adatok megismerésére jogosult lehetséges adatkezelők személye: A személyes adatokat az adatkezelő Társaság munkatársai kezelhetik, a fenti alapelvek tiszteletben tartásával.

Az érintettek adatkezeléssel kapcsolatos jogainak ismertetése: A következő adatok módosítását lehet elvégezni a weboldalakon: Jelszó, vezeték- és keresztnév, e-mail cím, telefonszám, felhasználó neve. A személyes adatok törlését, vagy módosítását az érintett kezdeményezheti: postai úton a 1015 Budapest, Ostrom utca 16. Fsz. 5. címen, e-mail útján az info@healzz2.hu e-mail címen.

14.2.1.2. Időpontfoglalás egyéb módon

Az előjegyzés (időpontfoglalás) történhet telefonon vagy e-mailen keresztül is.

A már előjegyzett betegek részére a Társaság figyelmeztető sms-t küld a közelgő vizitről. A Társasága az sms küldő szolgáltatás nyújtóját (MyHealzz) adatfeldolgozónak tekinti a betegek telefonszáma és a vizsgálataik (vizitjeik) időpontja, mint kezelt adatok körében.

14.2.1.3. Telefonos hangfelvétel készítése

A Társaság a központi számára érkező telefonhívásokat rögzíti. A hangfelvétel alapján rögzített hang és hangfelvétel személyes adat. Az emberi hang a személyiség megnyilvánulása, amely alapján azonosítható, és amelyből következtetések vonhatóak le rá nézve. A hang rögzítése által szükségszerűen adatkezelés valósul meg.

A fogyasztóvédelemről szóló 1997. évi CLV. törvény (Fgytv.) 17/B. § (3) bekezdése értelmében a telefonos eléréssel működtetett ügyfélszolgálat, illetve a rendelés időpontjának előzetes lefoglalására biztosított telefonos elérés esetében biztosítani kell a fogyasztó által kezdeményezett hívás sikeres felépülésének időpontjától számított öt perc várakozási időn belüli hívásfogadást és az érdemi ügyintézés megkezdését, kivéve, ha az a tevékenységi körén kívül eső elháríthatatlan ok miatt nem lehetséges, feltéve, hogy a vállalkozás úgy járt el, ahogy az az adott helyzetben általában elvárható. A vállalkozás köteles a panasszal kapcsolatos élőhangos ügyintézés választását a fogyasztó beazonosítása nélküli módon - reklám továbbítása nélkül - a telefonos eléréssel működtetett ügyfélszolgálat menüsorrendjének első helyére tenni. Az ügyfélszolgálathoz beérkező valamennyi telefonon tett szóbeli panaszt, valamint az ügyfélszolgálat és a fogyasztó közötti telefonos kommunikációt hangfelvétellel rögzíteni kell.

A hangfelvételt egyedi azonosítószámmal kell ellátni és öt évig meg kell őrizni.

Az adatkezelés célja: időpontfoglalás rendelésre, rendelésekkel kapcsolatos ügyintézés, esetlegesen panasz.

Az adatkezelés jogalapja: közérdekű feladat ellátása (Rendelet 6. cikk (1) bek. e) pont)

Az adattárolás határideje: az adatrögzítéstől számított 5 év. A szolgáltató kizárólag a jogszabály által előírt ideig kezelheti a hangfelvételt. Ezt követően a rögzített adatállományt – beleértve minden biztonsági másolatot – törölni kell.

Az adatkezelés módja: elektronikusan.

Az érintett bejelentő kérésére, az erre irányuló kéréséről történő tudomásszerzéstől számított 30 napon belül díjmentesen biztosítani kell a Társaság ügyfélszolgálatán a hangfelvétel meghallgatását, valamint hangfelvételenként egy alkalommal a hangfelvételről másolatot kell biztosítani.

Amennyiben az érintett kéri, a hangfelvételről készült másolatot elektronikus úton kell rendelkezésére bocsátani. A Társaság ebben az esetben a hangfelvétel kiadását az érintett azonosításán túl egyéb feltételhez nem kötheti.

A hangfelvételt az eljáró hatóságokon kívül (rendőrség, ügyészség, bíróság, fogyasztóvédelmi hatóság, stb.) a Társaság érintett területen dolgozói és a Társaság ügyvezetése ismerheti meg.

14.2.2. A gyógykezelés céljából történő adatkezelés

Az egészségügyi dokumentáció vezetése a kezelőorvos kötelezettsége. A rendszerhez a szakdolgozó és a recepciós feladatokat ellátó dolgozó is hozzáférhet. A dokumentáció vezetése a Társaság által bevezetett MyHealzz elnevezésű rendszer betegnyilvántartó és receptíró moduljában történik.

A beteg az ellátás befejezését követően az egészségügyi dokumentáció (vizsgálati lelet, ambuláns lap, zárójelentés, számla) egy példányát átveszi. Az ellátást követően a beteg, vagy közeli hozzátartozója, vagy meghatalmazottja - kérésre - a beteg dokumentációjába a jelen szabályzatban rögzített módon betekintést nyerhet, valamint azokról másolatot kaphat.

A gyermekek vonatkozásában végzett személyes adatok kezelése akkor jogszerű, ha a gyermek a 16. életévét betöltötte. A 16. életévét be nem töltött gyermek esetén, a gyermekek személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló (törvényes képviselő) adta meg, illetve engedélyezte.

Az ellátás során az Adatkezelő rögzíti a kezelést igénybe vevő személy (érintett) személyes-, illetve a kezelés szakszerű lefolytatása céljából szükséges egészségügyi adatait. Az érintett vagy törvényes képviselője az egészségügyi és a személyazonosító adatokat az Adatkezelővel, mint egészségügyi szolgáltatóval kötött szerződés teljesítése érdekében adja meg az Adatkezelő részére.

Az egészségügyi adatok felvétele a gyógykezelés része. A kezelést végző orvos dönti el, hogy a szakmai szabályoknak megfelelően - a kötelezően felveendő adatokon kívül - mely egészségügyi adat felvétele szükséges.

Az érintett gyógykezelésével kapcsolatos tevékenységet végző egyéb személy a kezelést végző orvos utasításának megfelelően, illetve a feladatai ellátásához szükséges mértékben vehet fel egészségügyi adatot.

Az adatkezelő az orvosi titkot köteles megtartani.

Mentesül a titoktartási kötelezettség alól, ha
a) az egészségügyi és személyazonosító adat továbbítására az érintett, illetve törvényes képviselője írásban hozzájárult, az abban foglalt korlátozásokon belül, valamint
b) az egészségügyi és személyazonosító adat továbbítása törvény előírásai szerint kötelező.

A Társaság által működtetett intézményben az egészségügyi és személyazonosító adatok továbbíthatók, illetve összekapcsolhatók, amennyiben az az érintett egészségügyi állapotának érdekében szükséges, kivéve, ha ezt az érintett írásban tett nyilatkozatában megtiltja. A különböző forrásból származó egészségügyi és személyazonosító adatokat csak addig az időpontig és olyan mértékig lehet összekapcsolni, ameddig az a megelőzés, a gyógykezelés érdekében feltétlenül szükséges.

Sürgős szükség esetén a kezelést végző orvos által ismert, a gyógykezeléssel összefüggésbe hozható minden egészségügyi és személyazonosító adat továbbítható.

A kezelést végző orvos az általa megállapított, az érintettre vonatkozó egészségügyi adatokról az érintettet közvetlenül tájékoztatja.

Az egészségügyi és a személyazonosító adatoknak az érintett részéről történő szolgáltatása - az egészségügyi ellátás igénybevételéhez kötelezően előírt személyazonosító adatok kivételével - önkéntes.

Abban az esetben, ha az érintett önként fordul az egészségügyi szolgáltatóhoz, a gyógykezeléssel összefüggő egészségügyi és személyazonosító adatainak kezelésére szolgáló hozzájárulását - ellenkező nyilatkozat hiányában - megadottnak kell tekinteni, és erről az érintettet (törvényes képviselőjét) tájékoztatni kell.

Sürgős szükség, valamint az érintett belátási képességének hiánya esetén az önkéntességet vélelmezni kell.

A gyógykezelés során a kezelést végző orvoson és az egyéb betegellátó személyeken kívül csak az lehet jelen, akinek jelenlétéhez az érintett hozzájárul, kivéve ha erről jogszabály máshogy rendelkezik.

Az érintett hozzájárulása nélkül is jelen lehet, aki az érintettet az adott betegség miatt korábban gyógykezelte, akinek erre az intézményvezető vagy az adatvédelmi tisztviselő szakmai-tudományos célból engedélyt adott, kivéve, ha ez ellen az érintett kifejezetten tiltakozott.

14.2.3. Gyógykezelés során jelen lévő személyek

A betegnek joga van ahhoz, hogy vizsgálata és gyógykezelése során csak azok a személyek legyenek jelen, akiknek részvétele az ellátásban szükséges, illetve azok, akiknek jelenlétéhez a beteg hozzájárult, kivéve, ha törvény másként nem rendelkezik. Az érintett hozzájárulása nélkül jelen lehet az érintett emberi jogainak és méltóságának tiszteletben tartásával:

- más személy, ha a gyógykezelés rendje több beteg egyidejű ellátását igényli,
- a rendőrség hivatásos állományú tagja, amennyiben a gyógykezelésre fogvatartott személy esetében kerül sor,
- a büntetés-végrehajtási szervezet szolgálati jogviszonyban álló tagja, amennyiben a gyógykezelésre olyan személy esetében kerül sor, aki a büntetés-végrehajtási intézetben szabadságelvonással járó büntetését tölti, és a gyógykezelést végző betegellátó biztonsága, illetve szökés megakadályozása céljából erre szükség van,
- ha bűnüldözési érdekből a beteg személyi biztonsága ezt indokolttá teszi, és a beteg nyilatkozattételre képtelen állapotban van.

Fent meghatározottakon felül jelen lehet az,

- aki a beteget az adott betegség miatt már kezelte,
- akinek az egészségügyi szolgáltató vezetője szakmai ok miatt engedélyt adott. A gyógykezelt személy kifejezett tiltakozásának ebben az esetben helyt kell adni.

Az egészségügyi szakember-képzés céljából az érintett (törvényes képviselője) hozzájárulásával lehet jelen a gyógykezelés során orvos, orvostanhallgató, egészségügyi szakdolgozó, egészségügyi főiskola, egészségügyi szakiskola vagy egészségügyi szakközépiskola hallgatója, valamint tanulója. A hozzájárulást a gyógykezelt személy szóban is megteheti a kezelést végző orvosnak.

14.2.4. Tájékozódási, tájékoztatási jog és kötelezettség, a beteg joga a tájékoztatáshoz

A betegellátás megkezdése előtt a beteget tájékoztatni kell a szolgáltató adatvédelmi rendjéről. A beteg tájékoztatása az adatvédelemről a kezelést végző orvos kötelessége. A beteg dokumentációjához csatolni kell a beteg esetleges korlátozó nyilatkozatát is.

A gyógykezelt személy gyógykezelésével kapcsolatos tájékoztatást a beteg kezelését végző orvos adja meg. A beteg gyógykezelésének ápolási vonatkozásairól az őt ellátó egészségügyi szakdolgozó is felvilágosítást adhat. Szakdolgozó, illetve más dolgozó a beteg gyógykezeléséről tájékoztatást nem adhat, kivéve, ha a beteg kezelését végző orvos erre az adott beteg esetében felhatalmazta. A tájékoztatás személyesen történik.

A kezelést végző orvos az általa megállapított, az érintettre vonatkozó egészségügyi adatokról az érintettet közvetlenül tájékoztatja. A pszichiátriai beteg esetében kivételesen korlátozható a betegnek az egészségügyi dokumentáció megismeréséhez való joga, ha alapos okkal feltételezhető, hogy a beteg gyógyulását nagymértékben veszélyeztetné, vagy más személy személyiségi jogait sértené az egészségügyi dokumentáció megismerése. A korlátozás elrendelésére kizárólag az orvos jogosult. A korlátozás elrendeléséről a betegjogi képviselőt és a beteg törvényes vagy meghatalmazott képviselőjét haladéktalanul értesíteni kell.

A beteg jogosult:

- a rá vonatkozó egészségügyi adatokat megismerni;
- az egészségügyi dokumentációba betekinteni;
- az egészségügyi dokumentációról kivonatot/másolatot készíteni, saját költségére ilyet kapni;
- egészségügyi adatairól indokolt célra - saját költségére - összefoglaló vagy kivonatos írásos véleményt kapni;
- adatainak kezeléséről tájékoztatást kapni;
- a jogszabály által előírt esetekben zárójelentést kapni.

A beteg ellátásának időtartama alatt az általa írásban felhatalmazott személy, az ellátás befejezését követően az általa teljes bizonyító erejű magánokiratban felhatalmazott személy jogosult a másolat kiadásának kérésére, illetve átvételére.

Az érintett halála esetén - ha korábban másként nem rendelkezett - törvényes képviselője, közeli hozzátartozója, valamint örököse jogosult a halál okával összefüggő vagy összefüggésbe hozható, továbbá a halál bekövetkezését megelőző gyógykezelésével kapcsolatos egészségügyi adatokat megismerni, az orvosi dokumentációba betekinteni, valamint azokról másolatot kapni. A jogosultságot a kérelmező okirattal köteles igazolni.

A másolat(ok) kiadása kizárólag eredeti, teljes bizonyító erejű magánokiratban foglalt kérelem alapján történhet. A kérelem eredeti példányát az ügyirathoz (kórlaphoz) csatoltan kell őrizni.

Az egészségügyi dokumentáció kiadása esetén a kért dokumentumokat a rendszerben rögzítettek szerint kell kiadni. A dokumentumok kiadásáért az adatvédelmi tisztviselő felel. A kiadás tényét a dokumentációban, és külön nyilvántartásban rögzíteni kell. A kiadást megelőzően az átvevő személyazonosságát, vagy meghatalmazását igazolni köteles. Az igazolás tényét az átvevő személyi adatainak és személyi igazolvány számának rögzítése mellett fel kell vezetni. Amennyiben más, felhatalmazott személy kéri ki a dokumentációt, akkor a felhatalmazás dokumentumát is csatolni kell a betegdokumentációhoz.

Az egészségügyi dokumentáció kiadása kizárólag az ügyvezető engedélyével történhet az alábbi esetekben:

a. Rendőrhatóság, vagy más hatósági szerv megkeresése;
b. Ügyvédi megkeresés;
c. Az egészségügyi ellátással összefüggő kártérítési igénnyel kapcsolatos megkeresés.

14.2.5. Az orvosi titok védelme

A Társaságot, mint szolgáltatót, valamint a vele munkaviszonyban, vagy munkavégzésre irányuló egyéb jogviszonyban álló más személyt a beteg egészségi állapotával kapcsolatos adat, továbbá a munkavégzéssel kapcsolatosan tudomására jutott egyéb adat vonatkozásában időbeli korlátozás nélkül titoktartási kötelezettség terheli. A titoktartási kötelezettség független attól,

hogy az adatokat milyen módon ismerte meg. A titoktartási kötelezettség tehát nemcsak a kezelést végző orvost, illetve a szakdolgozókat köti, hanem a szolgáltató minden dolgozóját. A szolgáltatót – az igazságügyi orvos szakértő kivételével - a titoktartási kötelezettség azzal a betegellátóval szemben is köti, aki a beteg gyógykezelésében nem működött közre, kivéve, ha az adatok a gyógykezelt személy további gyógykezelése érdekében szükségesek. A titoktartási kötelezettség alól írásban felmentést adhat a beteg, vagy törvényen alapuló adatszolgáltatási kötelezettség, továbbá a jelen adatvédelmi tájékoztatóban rögzített személyek részére történő adattovábbítás, az általuk kezelt adatok erejéig.

14.2.6. Közegészségügyi, járványügyi célból történő adatkezelés

A betegellátó haladéktalanul továbbítja az egészségügyi államigazgatási szervnek az egészségügyi és személyazonosító adatot, ha fertőző betegséget észlel, vagy annak gyanúja merül fel. Az egészségügyi államigazgatási szerv közegészségügyi vagy járványügyi közérdekre hivatkozva kérheti az érintett személyazonosító adatait.

14.2.7. Az egészségügyi és személyes adatok tárolásának módja, az adatkezelés biztonsága

A Társaság számítástechnikai rendszerei és más adatmegőrzési helyei a székhelyén és adatfeldolgozóinál találhatók meg. A Társaság a személyes adatok kezeléséhez a szolgáltatás nyújtása során alkalmazott informatikai eszközöket úgy választja meg és üzemelteti, hogy a kezelt adat:

- az arra feljogosítottak számára hozzáférhető (rendelkezésre állás);
- hitelessége és hitelesítése biztosított (adatkezelés hitelessége);
- változatlansága igazolható (adatintegritás);
- a jogosulatlan hozzáférés ellen védett (adat bizalmassága) legyen.

A Társaság az adatokat megfelelő intézkedésekkel védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés, sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

A Társaság a technika mindenkori fejlettségére tekintettel olyan műszaki, szervezési és szervezeti intézkedésekkel gondoskodik az adatkezelés biztonságának védelméről, amely az adatkezeléssel kapcsolatban jelentkező kockázatoknak megfelelő védelmi szintet nyújt. A Társaság Informatikai Biztonsági Szabályzatát jelen szabályzat melléklete tartalmazza.

A Társaság az adatkezelés során megőrzi

- a titkosságot: megvédi az információt, hogy csak az férhessen hozzá, aki erre jogosult;
- a sértetlenséget: megvédi az információnak és a feldolgozás módszerének a pontosságát és teljességét;
- a rendelkezésre állást: gondoskodik arról, hogy amikor a jogosult használónak szüksége van rá, valóban hozzá tudjon férni a kívánt információhoz, és rendelkezésre álljanak az ezzel kapcsolatos eszközök.

Az adatokat keletkezésükkor, megfelelő minőségű (elsősorban információ technológiai) adathordozóra kell rögzíteni. Az adatok olvashatóságáért és pontosságáért az azokat felvevő, illetve rögzítő (leíró) személy felel.

A Társaságnál felvett és tárolt egészségügyi dokumentációt - a képalkotó diagnosztikai eljárással készült felvételek, az arról készített leletek kivételével - az adatfelvételtől számított

legalább 30 évig, a zárójelentést legalább 50 évig kell megőrizni. A kötelező nyilvántartási időt követően gyógykezelés vagy tudományos kutatás érdekében - amennyiben indokolt - az adatok továbbra is nyilvántarthatók. Ha a további nyilvántartás nem indokolt a nyilvántartást meg kell semmisíteni. A képalkotó diagnosztikai eljárással készült felvételt az annak készítésétől számított 10 évig, a felvételről készített leletet a felvétel készítésétől számított 30 évig kell megőrizni.

Az egészségügyi dokumentációt a társaság szakorvosa, valamint a közreműködői által a Társaság által alkalmazott információs (MyHealzz) rendszerben kell kezelni és tárolni. Amennyiben az adatok fizikailag is kinyomtatásra kerülnek, úgy azokat rendezett, visszakereshető formában, zárható körülmények között kell tárolni. A dokumentumokat a véletlen megsemmisüléstől, illetve szándékos károkozástól óvni kell, illetve ezen események megelőzésére a lehetőségek korlátait figyelembe véve mindent el kell követni a megsemmisült, vagy eltűnt dokumentumok reprodukálhatóságát – a lehetőségek figyelembevételével - biztosítani kell. A rendszernek biztosítania kell az adatok visszakereshetőségét.

14.2.8. Az egészségügyi adatok kezelésére jogosultak köre

A beteg személyi és egészségügyi adataihoz, dokumentációjához az alábbi személyek férhetnek hozzá:

- a kezelőorvos;
- az ellátásért felelős, abban résztvevő egészségügyi szakszemélyzet;
- az ellátáshoz közvetlenül kapcsolódó egészségügyi szakszemélyzet (recepciós munkatárs)
- az adatfeldolgozást végző Informatikai munkatárs az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény előírásainak figyelembevételével;
- az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvényben meghatározott szervezetek, személyek;
- a Társaság adatfeldolgozói, az általuk végzett adatfeldolgozáshoz igazodó mértékben.

14.2.9. Az adatkezelési rendszer környezetének védelme

A fizikailag kinyomtatott, manuálisan kezelt betegdokumentációt (zárójelentések, leletek, ambuláns- és járóbetegellátási dokumentációk), a Társaság irodájában, irattárában el kell zárni. A tárolók zárhatóságát és a rendszeres zárás ellenőrzését biztosítani kell.

A dokumentációs anyag tárolási helyein a tűzvédelmi előírások és óvórendszabályok betartása kötelező.

A megsérült, elveszett adatok visszaállítását és annak mértékét - a lehetőségek felmérésével, indoklásával és mérlegelésével - az ügyvezetővel egyeztetve az adatvédelmi tisztviselő adatvédelmi tisztviselő rendeli el írásban.

Amennyiben a visszaállítás - reális módon - nem valósítható meg, arról az adatvédelmi tisztviselő írásos feljegyzést készít, melyet az ügyviteli rendszerben „Adatvédelem” iktatási jelzéssel archiválnak.

A visszaállításról - amennyiben az méltányos és megoldható -, a mulasztásért felelős köteles gondoskodni. A méltányosság és a személyes felelősség eldöntése az adatvédelmi tisztviselő hatáskörébe tartozik.

14.2.10. Az adatkezelő azonosítása, az adatkezelési rendszerbe történő belépés, illetve kilépés esetén

A Társaság által kezelt elektronikus rendszerben tárolt adatok védelméért a Társaság adatvédelmi tisztviselője felelős.

Az elektronikus adatkezelési rendszerhez való hozzáférés kizárólag a bejelentkezési eljárás sikeres végrehajtása után lehetséges. Ennek során az adatkezelő - a kezelőorvos - a rendszerbe elkülönített azonosítójával lép be az adatkezelési rendszerbe és ezt követően felviszi az általa kezelt beteg személyes adatait, valamint a szakmai szabályok szerint az egészségügyi adatokat.

Az ellátás végeztével a felhasználó kilép a rendszerből, ezáltal a további adathozzáférés nem lehetséges.

14.2.11. Az adatkezelők jogosultságának nyilvántartása, felelősség az adatok pontosságáért

Az adatkezelők jogosultságait az adatkezelési rendszer rögzíti és tartja nyilván.

Az adatkezelési rendszer tulajdonságából kifolyólag minden felhasználó csak a jogosultsági rendszeren keresztül férhet hozzá bármilyen adathoz.

Betegdokumentációról kért másolatok nyilvántartásáért az adatvédelmi tisztviselő a felelős.

Az adatok pontosságáért az adatokat származtató és rögzítő munkatárs a felelős.

Az adatok bevitelekor az egészségügyi dokumentáció vezetésére vonatkozó szakmai előírások és protokollok rendelkezéseit maradéktalan be kell tartani.

14.2.12. Laboratóriumi, szövettani vizsgálatok eredményeinek továbbítása

A Társaság, mint egészségügyi szolgáltató egyes vizsgálatok elvégzésére laboratóriumi feladatokat végző szervezet (adatfeldolgozó) segítségét veszi igénybe. A laboratórium az elvégzett vizsgálatok eredményét a Társaság e-mail címére jelszóval védett file-ként küldi meg.

Az e-mailes leletküldési üzenet és annak bármely csatolt anyaga bizalmas, bizalmas egészségügyi adatokat tartalmaz. A Társaság nem vállal felelősséget az üzenet teljes és pontos – címzett(ek)hez történő – eljuttatásáért, valamint semmilyen késésért, kapcsolat megszakadásból eredő hibáért, vagy az információ felhasználásából vagy annak megbízhatatlanságából eredő kárért, saját számítástechnikai rendszerén kívül; illetve a lelet fogadásához és megnyitásához szükséges hardver-, szoftverkörnyezet és informatikai ismeret hiányáért sem.

14.2.13. Az egészségügyi szolgáltatás során alkalmazott adatkezelés jogalapja

Az adatkezelés jogalapja általános egészségügyi ellátás esetében: az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény rendelkezései, azaz kötelező adatkezelés (GDPR 6. cikk (1) bek. c) pont). Tekintettel arra, hogy a személyes adatok különleges kategóriájának (egészségügyi adatok) kezelése történik, ezért a GDPR 9. cikke alapján is szükséges jogalap meghatározása, ellenkező esetben a minősített adatok kezelése tilos. A GDPR 9. cikk (2) bekezdésének a) pontja – az érintett kifejezett hozzájárulása - alapján történik az adatkezelés, foglalkozásegészségügyi-szolgáltatás esetében pedig GDPR 9. cikk (2) bekezdésének b) pontja alapján mivel az az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó

jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges.

Az adatszolgáltatás elmaradásának lehetséges következményei: az egészségügyi szolgáltatás nyújtásának elmaradása.

Az adatkezelés időtartama: Az egészségügyi dokumentációt az adatfelvételtől számított legalább 30 évig, a zárójelentést legalább 50 évig kell megőrizni. Ettől eltérően a képalkotó diagnosztikai eljárással készült felvételt annak készítésétől számított 10 évig, a felvételről készített leletet a felvétel készítésétől számított 30 évig kell megőrizni.

14.2.14. Az EESZT rendszer használata

Az egészségügyi ágazat számára létrehozott Elektronikus Egészségügyi Szolgáltatási Teret (EESZT) szakmai felhasználók érhetik el, és ők is csak a végzettségüknek és szerepkörükhöz rendelt jogosultságaiknak megfelelő tartalommal. A belépéshez egyedi azonosító szükséges. Az EESZT szolgáltatásait a rendszerhez csatlakozó saját, intézményi informatikai rendszerükön keresztül használhatják.

Az e-egészségügyi szolgáltatások biztosítják a magyar egészségügyi ellátók számára, hogy a betegadatok egységes elérésével minden ellátási szinten, a megfelelő információk birtokában a lehető leghatékonyabb kezelést, ellátást kapják az érintettek. Az EESZT szolgáltatásait minden ellátó az informatikai rendszerén keresztül használja, vagy szükség esetén, szűkített funkcionalitással, a kizárólag szakmai felhasználók által elérhető ágazati portál felületén.

Az ágazati portál publikálja a közhiteles törzsadatokat is, amelyek történeti sorrendben, verziókezeléssel és időpecséttel megjelölve, akár hitelesítési dokumentummal együtt tölthetőek le.

A digitális önrendelkezés keretében minden ellátottnak lehetősége nyílik, hogy bármely kormányablak ügyintézőjénél ugyanazokat az önrendelkezési szolgáltatásokat vegye igénybe, mint amiket ügyfélkapus regisztrációval a Lakossági portálfelületen tehetne meg.

Az eProfil modul biztosítja, hogy nyilván lehessen tartani a páciensekre legjellemzőbb egészségügyi összefoglaló adatokat, egészségügyi profiljukat (Health Characteristic). Az itt tárolt információk – az EESZT több moduljával ellentétben – nem a páciensek egészségügyi eseményeinek adatai, hanem a páciensre magára jellemző egészségügyi összefoglaló.

Tartalmukat tekintve a bejegyzéseknek két fő követelménynek kell megfelelniük:

A páciens élete során felmerült olyan egészségügyi eseményt, betegséget, orvosi beavatkozást, stb. nyilván kell tartani, ami hosszú ideig befolyásolja az egészségügyi állapotát, illetve az esetlegesen szükségessé váló vizsgálatokat és kezeléseket.

Minden olyan egészségügyi (és az egészségügyi ellátást befolyásoló) információt tartalmaznia kell a szükséges időtartamig, ami fontos lehet az egészségügyi ellátás során.

A bejegyzések egy, a rögzített szerkezetnek megfelelő egységes, konszolidált formában tartalmazzák és jelenítik meg azokat az információkat, amelyek fontosak az egészségügyi ellátás során.

A bejegyzések megtekintésének esetei is két fő kategóriába sorolhatók:

- Sürgősségi ellátás során a legfontosabb egészségügyi információk gyorsan és összefoglalva legyenek elérhetők.

- Egyéb ellátás során azon információk, amelyek befolyásolják az ellátást, egységes formában álljanak rendelkezésre.

Az adattár, mint szolgáltatás kettős célt szolgál ki. Egyrészt lehetővé teszi, hogy sürgősségi esetben az aktuális ellátás tekintetében kiemelt jelentőségű egészségügyi jellemzők hatékonyan rendelékezésre álljanak az ellátó személyzet számára. Másrészt bármilyen más ellátás során is konszolidált módon teszi áttekinthetővé azokat az egészségügyi adatokat, amelyek hosszú távon érvényesek, illetve változásuk nyomon követése kiemelt jelentőséggel bír.

Az eProfilban kezelt adatok jellemzően nem, vagy ritkán változnak, és az ellátott egészségi állapotára hosszú távon jellemzőek. Ezekben az adatcsoportok tartozik például az allergiák, gyógyszerérzékenységek, implantátumok, krónikus betegségek, gondozásban történő részvétel, megállapított betegségek, elváltozások, aktuális gyógyszerezés adatai.

Az eProfilba Adatkezelő vihet fel adatokat. Azonban az ellátott, az önrendelkezés keretében rendelkezhet ennek megtiltásról. Az EESZT lakossági felületén beállíthat teljes tiltást az eProfiljára, így sem adatokat bevinni, sem lekérdezni nem lehetséges. Megtilthatja új adat beküldését, ez esetben a korábban felvitt adatok lekérdezhetőek maradnak, vagy visszaállíthatja az alapértelmezést, miszerint a beküldés és lekérdezés is engedélyezett. Az eProfilba történő adatfelvételt megelőzően Adatkezelő a tiltakozás jogáról az érintettet kioktatja.

A digitális technikában az elfogadott szabványok alkalmazásával, az internet lehetőségeinek kihasználásával mód nyílik a digitális felvételek gyors és biztonságos továbbítására a különböző intézmények között a „Digitális Képtovábbítás” (DKTK) modulban, növelve ezzel a betegellátás hatékonyságát és biztonságát.

Az eKórtörténet lehetővé teszi az egyes ellátási események kapcsán keletkező egészségügyi dokumentumok központi tárolását és visszakeresését. Az esettörténet csak az ellátási dokumentációkat tárolja, az ellátás során keletkezett egyéb dokumentáció tárolása az EESZT más moduljaiban történik.

Kétféle módon helyezhető el dokumentum az eKórtörténetben:

- Fizikailag tárolt (belső) dokumentum, amiket az EESZT eKórtörténet modulja tárol.

- Hivatkozás formájában tárolt (külső) dokumentum, amelyeket az EESZT más moduljai tárolnak.

Az eKórtörténeti dokumentumok hierarchikus rendszerben tárolódnak és abban kereshetők. A páciens azonosítására szolgál a TAJ szám, mint egyedi azonosító. Az eKórtörténet saját, országosan egyedi, belső azonosítót rendel minden pácienshez. Az eset azonosítására szolgál az esetszám, a dokumentum azonosítására pedig a dokumentumazonosító, amelyet a beküldő rendszer – Adatkezelő rendszere - ad át az eKórtörténet modulnak – a beküldő rendszerben egyedi –, valamint az eKórtörténet saját, országosan egyedi, belső azonosítót rendel minden esethez.

Jogszabályi rendelkezés alapján az orvosi ellátás megkezdéséről és befejezéséről Adatkezelőnek jelentést kell küldenie az EESZT felé. Az események rögzítése megadja egy-egy beteg életútját az egészségügyi ellátó rendszerben a törvény által megfogalmazott történések esetében.

Az EESZT használatához szükséges azonosítás egyik fajtája (a személyazonosító igazolvány mellett) az egyszeri jelszót generáló token használata. A jelszót kizárólag Adatkezelő ügyvezetője ismerheti és használhatja.

Az egészségügyi adatokra vonatkozó önrendelkezés állampolgári jog és felelősség. A személyes adatok védelme érdekében az EESZT rendszer lehetőséget biztosít minden TAJ számmal rendelkező érintettnek, hogy a rendszerbe bekerülő adatainak hozzáférését szabályozza. A digitális önrendelkezés lehetőségét az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény 2015. évi CCXXIV. törvényben módosított rendelkezések teszik lehetővé

.Az érintett a EESZT rendszerben adatainak használatáról a bejelentkezését követően a https://www.eeszt.gov.hu/hu/onrendelkezes oldalon nyilatkozhat.

14.2.15. Adattovábbítás kívüli harmadik személyek és hatóságok részére

Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvényben meghatározott szervezetek írásbeli megkeresésére a kezelést végző orvos az érintett egészségügyi és a megkereső szerv által törvény alapján kezelhető, az azonosításhoz szükséges személyazonosító adatait átadja a megkereső szervnek. A megkeresésben fel kell tüntetni a megismerni kívánt egészségügyi és személyazonosító adatokat, valamint az adatkezelés célját.

Amennyiben az érintett egészségügyi adatai más személyt is érintenek, az egészségügyi és személyazonosító adatok továbbításához e harmadik személy (törvényes képviselője) írásbeli hozzájárulását be kell szerezni. Nincs szükség a hozzájárulásra, ha az adattovábbítást az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény lehetővé teszi.

A Társaság haladéktalanul továbbítja az egészségügyi államigazgatási szervnek az adatfelvétel során tudomására jutott egészségügyi és személyazonosító adatot, ha az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény 1. számú melléklet A) pontjában szereplő fertőző betegséget észlel, vagy annak gyanúja merül fel.

14.3. Üzleti partnerekhez, alvállalkozókhoz kapcsolódó adatkezelések

A Társaság a tevékenységét magánszemélyek és a vele szerződő egyéni és társas vállalkozások, illetve azok foglalkoztatottjai számára is nyújtja, illetve a működésének feltételeit szerződéses partnereitől történő beszerzésekkel biztosítja. A szerződésekben a Felek kapcsolattartói is megnevezésre kerülnek e-mail címük és telefonszámuk feltüntetésével.

Jogi személy partnerek cégjegyzékben nem szereplő természetes személy képviselőinek személyes adatai kezelése során a kezelhető személyes adatok köre az alábbi: a természetes személy neve, címe, telefonszáma, e-mail címe.

Amennyiben a gazdálkodó szervezet szerződő fél az Adatkezelővel kötött szerződésben a vezető tisztségviselő vagy cégvezető, illetve a cégjegyzékben szereplő törvényes képviselő adatait adja meg, úgy a cégjegyzékből ismert, nyilvános adatok kezeléséhes egyéb jogcím nem szükséges.

A cégjegyzékben nem szereplő kezelt adatok: a magánszemély neve, telefonszáma, e-mail címe.

A személyes adatok kezelésének célja: a Társaság jogi személy partnerével szerződés megkötése, teljesítése, üzleti kapcsolattartás.

Az adatkezelés jogalapja: természetes személy partner esetében az érintettel kötött szerződés, azaz a GDPR 6. cikk (1) bekezdés b) pontja, jogi személy esetében a kapcsolattartó, illetve a bejegyzett képviselő nem nyilvántartott adataira nézve a Társaság jogos érdeke, a partnerrel fennálló üzleti kapcsolat fenntartása, a kapcsolattartás megkönnyítése, azaz a GDPR 6. cikk (1) bekezdés f) pont.

A Társaság a jogos érdeket érdekmérlegelési teszt alapján vizsgálta és igazolta. Az érdekmérlegelési teszt igazolta, hogy ezen adatkezelés az adatkezelő érdekei érvényesítése érdekében szükséges, az érintettek szabadságait és érdekeit az adatkezelés ilyen módja hátrányosan nem érinti. A Társaság a jogos érdeket érdekmérlegelési teszt alapján vizsgálta és igazolta. Az érdekmérlegelési teszt igazolta, hogy ezen adatkezelés az adatkezelő érdekei érvényesítése érdekében szükséges, az érintettek szabadságait és érdekeit az adatkezelés ilyen módja hátrányosan nem érinti.

A személyes adatok tárolásának időtartama: az üzleti kapcsolat, illetve az érintett képviselői minőségének fennállását követő 8 év. Ha jogszabály (pl. adótörvény stb.) ennél hosszabb időt állapít meg a szerződések nyilvántartására, illetve tárolására, akkor e jogszabályokban meghatározott időtartam.

Ha az érintettre vonatkozó személyes adatokat az Adatkezelő az érintettől gyűjti, az adatkezelő a személyes adatok megszerzésének időpontjában az érintett rendelkezésére bocsátja a következő információk mindegyikét:

a) az adatkezelőnek és az ügyvezetőnek a kiléte és elérhetőségei;
b a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
c) az adatkezelő vagy harmadik fél jogos érdekei;

A Társaság által ilyen célból gyűjtött adatok más adatkezelő vagy adatfeldolgozó részére átadásra nem kerülnek, harmadik országba Adatkezelő nem továbbítja őket.

15. Kamerás megfigyelőrendszer üzemeltetése

Adatkezelő az általa működtetett Magánklinikai orvosi rendeléseire érkezők figyelemmel kísérése, valamint a vagyonvédelem céljából elektronikus megfigyelőrendszert üzemeltet, amely megfigyelőrendszer kép- és hangrögzítést is lehetővé tesz.

A kamerarendszer működtetőjét a kamera által közvetített képek megismerése vonatkozásában titoktartási kötelezettség terheli. A kamerarendszer működtetője köteles rögzíteni, hogy kik jogosultak betekintésre. A Társaság a kamera által készített felvételeket 7 napig jogosult megőrizni.

Ezen adatkezelés jogalapja a Társaság jogos érdeke (Rendelet 6. cikk (1) bek. f) pont): a Társaság vagyonvédelme. A Társaság a jogos érdek igazolására érdekmérlegelési tesztet készített.

Az elektronikus megfigyelőrendszer adott területen történő alkalmazásáról jól látható helyen, jól olvashatóan, a páciensek, az alkalmazottak és egyéb harmadik személyek tájékozódását elősegítő módon figyelemfelhívó jelzést, tájékoztatást kell elhelyezni. A tájékoztatásnak ki kell terjednie az elektronikai vagyonvédelmi rendszer által folytatott megfigyelés tényére, valamint a rendszer által rögzített, személyes adatokat tartalmazó kép felvétel készítésének, tárolásának

céljára, az adatkezelés jogalapjára, a felvétel tárolásának helyére, a tárolás időtartamára, a rendszert alkalmazó (üzemeltető) személyére, az adatok megismerésére jogosult személyek körére, továbbá az érintettek jogaira és érvényesítésük rendjére.

A kezelt adatok köre az érintettek képmása.

A rögzített felvételek felhasználás hiányában maximum 7 (hét) napig őrizhetők meg, 7 nap elteltével megsemmisítésre, illetve törlésre kerülnek.

Felhasználásnak minősül, ha a rögzített felvételt, valamint más személyes adatot bírósági, hatósági, munkajogi vagy egyéb eljárásban bizonyítékként felhasználják.

Az, akinek jogát vagy jogos érdekét a kép felvétel adatának rögzítése érinti, rögzítésétől számított 7 napon belül jogának vagy jogos érdekének igazolásával kérheti, hogy az adatot annak kezelője ne semmisítse meg, illetve ne törölje.

Nem lehet elektronikus megfigyelőrendszert alkalmazni olyan helyiségben, amelyben a megfigyelés az emberi méltóságot sértheti, így különösen az öltözőkben, zuhanyzókban, az illemhelyiségekben, továbbá az olyan helyiségben sem, amely a munkavállalók munkaközi szünetének eltöltése céljából lett kijelölve.

Munkaidőn kívül vagy munkaszüneti napokon a munkahely teljes területe megfigyelhető.

A kamerák közül 2 db a rendelő recepcióján és a váróhelyiségben (folyosón) kerültek elhelyezésre, míg további 6 db a rendelő épületén kívül, az épületen a jelen szabályzathoz mellékelten csatolt rajz alapján. A kültérre kihelyezett kamerák egyike sem irányul közterületre és/vagy a szomszédos ingatlanokra. Amennyiben a kamerák beállítása során az általuk adott kép ilyen részleteket tartalmazna, úgy a Társaság maszkolással, torzítással biztosítja a kamerák jogszerű használatát.

Az elektronikus megfigyelőrendszer adott területen történő alkalmazásáról jól látható helyen, jól olvashatóan, a területen megjelenni kívánó harmadik személyek tájékozódását elősegítő módon figyelemfelhívó jelzést, tájékoztatást kell elhelyezni. A tájékoztatásnak ki kell terjednie az elektronikai rendszer által folytatott megfigyelés tényére, valamint a rendszer által készített, személyes adatokat tartalmazó közvetített képfelvétel készítésének céljára, az adatkezelés jogalapjára.

16. A Társaság WEB lapja

16.1. A weblap funkciói

A Társaság weblapjainak címe: https://szofiaklinika.hu/

A Társaság WEB lapján az érdeklődök egyrészt a Társaság szolgáltatásairól a Társaság elérhetőségeiről tájékozódhatnak, másrészt foglalhatnak időpontot és küldhetnek üzenetet a Magánklinika által biztosított szolgáltatások igénybevétele céljából.

Ugyanezen oldalon a „kapcsolat” menüpont alatt (https://szofiaklinika.hu/kapcsolat/) lehetőség van arra, hogy az érdeklődök a Társaság részére közvetlenül küldjenek üzenetet a nevük, e-mail címük, valamint üzenetük tárgyának és tartalmának megadásával. Az üzenet elküldése csak abban az esetben lehetséges, ha az érdeklődő az adatvédelmi tájékoztatóra mutató link után lévő kis négyzet bejelölésével kifejezetten nyilatkozik, hogy a Társaság adatkezelési tájékoztatóját megismerte, az abban foglaltakat elfogadja és kifejezetten hozzájárul megadott adatainak a kezeléséhez.

16.2. Cookie (süti) kezelés

A honlapon a sütik használatának célja, hogy a későbbiekben jobban testre szabhatóak legyenek a weboldalak, az Érintett érdeklődésének és igényeinek megfelelően, ezáltal könnyebbé válik az oldalak használata. A sütik célja továbbá a jövőbeni felhasználói tevékenységek gyorsítása és a felhasználói élmény javítása az oldalak használata közben. A sütik anonim, összesített statisztika készítésére is alkalmasak, így jobban megérthető, hogy az emberek hogyan használják az oldalakat és így javítani lehet azok struktúráján és tartalmán. Ebből az információból nem lehet a természetes személyt azonosítani.

A használt sütik fajtái:

- Anonim látogatóazonosító (süti) elhelyezése

Az anonim látogatóazonosítók (sütik) olyan fájlok vagy információdarabok, amelyek a felhasználó számítógépén (vagy más internetképes készülékén, mint okostelefon vagy táblagép) tárolódnak, amikor meglátogat egy oldalt. Egy süti általában tartalmazza a webhely nevét, ahonnan az jött, a saját „élettartamát" (vagyis, hogy milyen hosszan marad a készüléken) és az értékét, ami általában egy véletlenszerűen generált egyedi szám

- Szükséges sütik

Ahhoz szükségesek, hogy az oldalak jól működjenek, lehetővé teszik a felhasználóknak, hogy mozogjon webhelyeken és használja a különböző funkciókat. Például a korábbi lépésekre, beírt szövegre való emlékezés megkönnyíti a használatot, amikor visszanavigál egy oldalra ugyanabban a munkamenetben.

Ezek a sütik nem azonosítják egyénileg a felhasználót. Ha a felhasználó nem fogadja el ezen sütik használatát, annak hatása lehet a webhelyre és annak teljesítményére.

- Teljesítmény sütik

Segítik megérteni, hogy a látogatók hogyan lépnek kapcsolatba webhelyekkel azáltal, hogy információt szolgáltatnak a meglátogatott helyekről, arról, hogy mennyi időt töltenek az oldalon, és bármely problémáról, amivel találkoztak, mint például a hibaüzenetek. Ez segít a Szolgáltató webhelyeinek teljesítményének javításában.

Ezek a sütik nem azonosítanak egyénileg felhasználót. Az adatokat összesítve és névtelenül gyűjtik.

- Funkcionalitás sütik

Lehetővé teszik a webhelyeknek, hogy emlékezzenek arra, mik kerültek kiválasztásra (mint például a felhasználónév, nyelv, vagy a régió, ahol tartózkodik az oldal látogatója), hogy egy személyesebb online tapasztalatot nyújtsanak. Azt is lehetővé teszik, hogy videókat nézzen, játékokat játsszon és társasági eszközöket használjon, mint például a blogok, chatszobák és fórumok.

Az ilyen sütik által gyűjtött információkban lehetnek személyes azonosító adatok, amelyeket a felhasználó megosztott, mint a felhasználóneve vagy profilképe. Mindig nyilvánvalóan tájékoztatni kell az Ügyfelet arról, hogy milyen információt gyűjt a Társaság, mit csinál vele és kivel osztja meg azt. Ha nem fogadja el az oldalt használó ezeket a sütiket, annak hatása lehet a webhely teljesítményére és funkcionalitására és korlátozhatja hozzáférését a webhely tartalmához.

- Célzás vagy Reklám sütik

Ezeket a sütiket olyan tartalmak szállítására használja a Társaság, amelyek relevánsabbak a felhasználó számára és érdeklődési köre számára. Ezeket arra lehet használni, hogy célzott hirdetést juttassanak el, és hogy korlátozzák, hogy hányszor néz meg valaki egy hirdetést.

Abban is segítenek, hogy mérni lehessen a reklám kampányok hatékonyságát az oldalakon. Ezeket a sütiket arra lehet használni, hogy emlékezzenek a webhelyekre, amelyeket meglátogatott a felhasználó és megoszthatja a Társaság ezt az információt más felekkel, ideértve hirdetőit és az ügynökségeket.

Az ilyen sütik legtöbb fajtája követi a fogyasztókat IP címükön keresztül ez által gyűjthetnek személyesen azonosítható információkat.

17. Záró rendelkezések

Jelen Szabályzat 2021. augusztus 1. napján lép hatályba.