

TARTALOMJEGYZÉK

DOMÁNY-BARKI KFT.

7633, PÉCS, SZÁNTÓ U. 4/A

ADATKEZELÉSI SZABÁLYZAT

KÉSZÍTETTE:

MAPOSZ ORVOS-AUDITORI BIZOTTSÁGA:

DR. KOLLA BALÁZS, orvos, minőségügyi auditor, kockázatelemző.

A/2004/005/MSZT

DR. PRINCZ JÁNOS, orvos, minőségügyi auditor. A/2004/009/MSZT

DR. KOVÁCS SÁNDOR, orvos, minőségügyi auditor A/2004/008/MSZT

DR. BEH JÓZSEF, orvos, minőségügyi auditor A/2004/002/MSZT

ÉRVÉNYES: 2025. DECEMBER 31-IG

PÉCS

2022

TARTALOMJEGYZÉK

A Vállalkozás/Praxis Bemutatása	1
A Szabályzat célja, témája, tartalma. A megújítás indoklása és szempontjai	2
A GDPR elvi-koncepcionális, jogi alapjai	3
Mi indokolja a GDPR, vagyis az Általános AdatVédelmi Szabályozás megfogalmazását Európai Unió Rendeletként?	3
A GDPR által megfogalmazott adatkezelési, adatvédelmi elvek	5
A GDPR által megfogalmazott gyakorlati követelmények az adatkezelés, adatvédelem területén	7
Praxisunk adatkezelési gyakorlata —megfeleltetve a GDPR előírásainak	9
4. cikk. Fogalommeghatározások	10
5. cikk. A személyes adatok kezelésére vonatkozó elvek	12
5. 1. jogszerűség, tisztességes eljárás és átláthatóság	12
5.1.1. célhoz kötöttség	12
5.1.2. adattakarékosság	12
5.1.3. pontosság	12
5.1.4. korlátozott tárolhatóság	13
5.1.5. integritás és bizalmas jelleg	13
5.2. elszámoltathatóság	13
6. cikk. Az adatkezelés jogszerűsége	14
7-8. cikk A hozzájárulás feltételei	14
9. cikk. A személyes adatok különleges kategóriáinak kezelése	14
12. cikk. Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlása	15
13-14. cikk. Rendelkezésre bocsátandó információk	15

15. cikk. Az érintett hozzáférési joga	16
16. cikk. A helyesbítéshez való jog	16
17. cikk. A törléshez való jog („az elfeledtetéshez való jog”)	17
18-19. cikk Az adatkezelés korlátozásához való jog. – Értesítési kötelezettség.	17
20. cikk. Az adathordozhatósághoz való jog	17
24. cikk. Az adatkezelő feladatai	18
25. cikk. Beépített és alapértelmezett adatvédelem	19
28. cikk. Az adatfeldolgozó	19
30. cikk. Az adatkezelési tevékenységek nyilvántartása	19
31. cikk. Együttműködés a felügyeleti hatósággal	20
32. cikk. Az adatkezelés biztonsága	20
33. cikk. Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak	20
34. cikk. Az érintett tájékoztatása az adatvédelmi incidensről	21
35. cikk. Adatvédelmi hatásvizsgálat	21
36. cikk. Előzetes konzultáció	21
37-38-39. cikk. Az adatvédelmi tisztviselő kijelölése – jogállása – feladatai.	22
40. cikk Magatartási kódex	23
1. Melléklet. A praxisunkban lefolytatott Adatvédelmi Hatástanulmány (Privacy Impact Assessment, PIA)	24
A Hatásvizsgálat kockázatértékelő táblázatai – módosítási javaslatok	34
2. Melléklet. 01. Adatkezelés nyilvántartása	38
2. Melléklet. 01. Adatkezelés nyilvántartása. Kitöltési útmutató	39
2. Melléklet. 02. Adattovábbítás nyilvántartása	40
2. Melléklet. 02. Adattovábbítás nyilvántartása. Kitöltési útmutató	41
2. Melléklet. 03. Hozzáférés, helyesbítés, korlátozás, törlés, hordozás és hatósági megkeresések nyilvántartása	42

2. Melléklet. 03. Hozzáférés, helyesbítés, korlátozás, törlés, hordozás és hatósági megkeresések nyilvántartása. Kitöltési útmutató	43
2. Melléklet. 04. Adatvédelmi incidensek nyilvántartása	44
2. Melléklet. 04. Adatvédelmi incidensek nyilvántartása. Kitöltési útmutató	45
2. Melléklet. 05. Adatkezelés biztonságára irányuló technikai és szervezési intézkedések nyilvántartása	46
2. Melléklet. 05. Adatkezelés biztonságára irányuló technikai és szervezési intézkedések nyilvántartása. Kitöltési útmutató	47
2. Melléklet. 06. Harmadik fél felé irányuló szerződés kiegészítés, módosítás kezdeményezésének, lefolyásának nyilvántartása	48
2. Melléklet. 06. Harmadik fél felé irányuló szerződés kiegészítés, módosítás kezdeményezésének, lefolyásának nyilvántartása. Kitöltési útmutató	49
2. Melléklet. 07. Az adatvédelmi hatástanulmány áttekintésének, aktualizálásainak nyilvántartása	50
2. Melléklet. 07. Az adatvédelmi hatástanulmány áttekintésének, aktualizálásainak nyilvántartása. Kitöltési útmutató	51
3. Melléklet. Iratminták. Az érintettek adataikba betekintésének szabályozása. Az Adatkezelési Szabályzat 34. oldal 3-as sorához kapcsolódóan	52
3. Melléklet. Iratminták. A NEAK felé történő adattovábbítás rendje. Az Adatkezelési Szabályzat 34. oldal 5-6-os sorához kapcsolódóan	53
3. Melléklet. Iratminták. Az ÁNTSZ-Kormányhivatal felé történő adattovábbítás rendje. Az Adatkezelési Szabályzat 34. oldal 7-es sorához kapcsolódóan	54
3. Melléklet. Iratminták. Tudományos feldolgozás céljaira történő adattovábbítás szabályozása. Az Adatkezelési Szabályzat 34. oldal 15-ös sorához kapcsolódóan	55
3. Melléklet. Iratminták. A hozzátartozók felé történő adattovábbítás rendje. Az Adatkezelési Szabályzat 35. oldal 17-18-as sorához kapcsolódóan	56
3. Melléklet. Iratminták. A beteg adatkorlátozási és törlési joga biztosításának szabályozása. Az Adatkezelési Szabályzat 35. oldal 19-es sorához kapcsolódóan	57
4. Melléklet. A közeljövő, adatkezelést is érintő, Európai Unió dokumentumok listája és megtalálási helyük.	58

A VÁLLALKOZÁS/PRAXIS BEMUTATÁSA

A PRAXIST VEZETŐ ORVOS:	Dr. Domány Eszter
VÁLLALKOZÁS NEVE:	Domány-Barki Kft.
VÁLLALKOZÁS SZÉKHELYE:	7633 Pécs, Szántó K. J. u. 4/A
POSTACÍM, AHOVÁ A KÜLDEMÉNYEKET KÉRI:	7633 Pécs, Szántó K. J. u. 4/A
RENDELŐ VAGY ZELEPHELY CÍME:	7633 Pécs, Szántó K. J. u. 4/A
TELEFONSZÁM/MOBIL:	06 20 453 9760
E-MAIL CÍM:	drdomanyeszter@gmail.com
ASSZISZTENS 1:	Ács Tímea
ASSZISZTENS 2:	—
ADATKEZELŐ:	Dr. Domány Eszter, Ács Tímea
ADATFELDOLGOZÓ:	Ács Tímea
PRAXIS TÍPUSA:	Felnőtt
SZAKVIZSGÁK:	Családorvostan
MAGÁNTEVÉKENYSÉG:	—
ÉRDEKVÉDELMI SZERVEZETI TAGSÁG:	Magyarországi Praktizáló Orvosok Szövetsége
MINŐSÉGIRÁNYÍTÁSI RENDSZERE:	ISO-EMI

ADATKEZELÉSI SZABÁLYZAT

CÉGNÉV, ORVOS NEVE, ALAPELLÁTÓ HÁZIORVOSI PRAXIS,

CÉG CÍME/RENDELŐ-TELEPHELY CÍME: A FEDLAPON!

A Szabályzat célja

Jelen szabályzat célja, hogy az orvosi gyógyító-, megelőző komplex feladataink végzése kapcsán, azonosított folyamataink sorában, a vonatkozó jogszabály alapján főtevékenységként (GDPR 37.1.) megfogalmazható adatkezelési-, adattárolási-, adatfeldolgozási tevékenységünk napi gyakorlatát azonosítsa, rögzítse és ezáltal szabályokba foglalja oly módon, hogy ezen szabályaink mentén működve, minden tekintetben és teljes körűen megfelelhessünk az európai Általános AdatVédelmi Szabályozás (GDPR) előírásainak.

A Szabályzat megújítása indoklása és szempontjai

A GDPR szellemében és konkrét előírásait követő adatkezelési szabályzattal 2018 óta rendelkezünk. Időközben, a felmerülő újabb szempontok, részben az EU-s szabályozások terén, részben a praxisunkban bekövetkezhető változások (személyek, alkalmazottak, munkatársak, informatikai eszközök, tevékenységeink, stb.) szükségessé teszik a Szabályzat időről-időre történő megújítását, aktualizálását.

Noha maga a GDPR lényegében nem változott, csak kisebb pontosításokat hajtottak végre, az értelmezések kiigazítására, ám az Unió egészségüggyel kapcsolatos ajánlásai, az EU Bizottság Jelentése a digitalizációs egészségügy irányában, az egészségügyi-járványügyi adatbázisok határokon átnyúló egységesítésére, szabványosítására, vagy akár a precíziós betegellátás igényére és lehetőségére, számos új feladatot, komoly kihívást jelent számunkra is. Fontos EU-s szempont a páciens edukáció kiteljesítése, a testmozgás életminőség megőrző gyakorlatának hangsúlyozása, a lakosság (polgárok) tudatos bevonása saját egészségük és jóllétük fejlesztésében, megőrzésében. Előre gondolkodva, minőségirányítási rendszerszemlélettel és folyamatszemlélettel felvértezve ezen új tevékenységeket eredendően az Adatkezelési Szabályzat előírásaira figyelemmel fogjuk tudni végezni. A felemlített Uniós dokumentumok felsorolását a Szabályzat végén, a 4. számú mellékletben helyeztük el.

A Szabályzat témája, tartalma

Mivel a GDPR egyik alapvető igénye a tudatosság növelése a résztvevők körében, ezért ilyen célzattal, munkatársaink, partnereink és önmagunk adatvédelmi tudatosságának elmélyítését, fejlesztését célozva áttekintjük a GDPR elvi-koncepcionális, jogi alapjait, a GDPR megalkotásának indokait, motivációit valamint a GDPR által megfogalmazott elveket, amelyekre a konkrét Európai Uniós szabályozás épül.

Ezt követi a Szabályzat praxisunk gyakorlatára vonatkozó érdemi része, amely megfogalmazása, összeállítása során a minőségügyi gyakorlatunkban bevált módszert alkalmazva, jelen esetben a GDPR cikkei pontjain végighaladva értelmezzük a ránk vonatkozó kötelezettségeket és feleltetjük meg saját adatkezelési gyakorlatunkat a jogszabály előírásaival.

Tesszük ezt azon ismeretek birtokában, miszerint „Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban” (GDPR 99.2.), valamint hogy figyelembe kell venni a mikro-, kis-, és középvállalatok sajátos szükségleteit. (GDPR preamb.13.). A gyakorlatban ez azt jelenti, hogy a józan ész és a realitások szerint kell értelmeznünk azon előírásokat, amelyek alapvetően globalizált világcégekre, százmillió fős adatkezelést végző internetes portálokra, sokmilliárd dolláros világ webáruházakra készült, de nekünk a két, legfeljebb 3 fős orvosi praxisokra vagy a nem sokkal több fős egyéb orvosi vállalkozásokra kell „testre szabnunk” az általános érvényű szabályozást.

A következőkben a rendeletből részleteket veszünk csak ki, aszerint összeválogatva, hogy melyek vonatkoztathatóak orvosi vállalkozásainkra, de a teljes paragrafus, vagyis itt cikknek nevezett feltalálási helyet minden esetben zárójelben közöljük. Ezt az eljárást követjük a Szabályzat teljes terjedelmére érvényesen.

A GDPR elvi-koncepcionális, jogi alapjai

1. A természetes személyek személyes adataik kezelésével összefüggő védelme alapvető jog. Az Európai Unió Alapjogi Chartája (Charta) 8. cikkének (1) bekezdése és az Európai Unió működéséről szóló szerződés (EUMSZ) 16. cikkének (1) bekezdése rögzíti, hogy mindenkinek joga van a rá vonatkozó személyes adatok védelméhez.

2. A természetes személyek személyes adataik kezelésével összefüggő védelméhez kapcsolódó elvek és szabályok a természetes személyek állampolgárságától és lakóhelyétől függetlenül tiszteletben tartják e természetes személyek alapvető jogait és szabadságait, különösen, ami a személyes adataik védelméhez való jogukat illeti. Ez hozzájárul a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség, valamint a gazdasági unió megteremtéséhez, a gazdasági és társadalmi fejlődéshez, a belső piacon belüli gazdaságok erősödéséhez és konvergenciájához, valamint a természetes személyek jólétéhez. (GDPR preamb. 2. pont)

4. A személyes adatok kezelését az emberiség szolgálatába kell állítani. A személyes adatok védelméhez való jog nem abszolút jog, azt az arányosság elvével összhangban, a társadalomban betöltött szerepének függvényében kell figyelembe venni, egyensúlyban más alapvető jogokkal. Ez a rendelet minden alapvető jogot tiszteletben tart, és szem előtt tartja a Chartában elismert és a Szerződésekben rögzített szabadságokat és elveket, különösen ami a magán-, és a családi élet, az otthon és a kapcsolattartás tiszteletben tartásához és a személyes adatok védelméhez, a gondolat-, a lelkiismeret- és a vallásszabadsághoz, a véleménynyilvánítás szabadságához és a tájékozódás szabadságához, a vállalkozás szabadságához, a hatékony jogorvoslathoz és a tisztességes eljáráshoz, és a kulturális, vallási és nyelvi sokféleséghez való jogot illeti. (GDPR preamb. 4. pont)

Mi indokolja a GDPR, vagyis az Általános AdatVédelmi Szabályozás megfogalmazását Európai Uniós Rendeletként?

1. A belső piac működéséből eredő gazdasági és társadalmi integráció lényegesen megnövelte a személyes adatok határokon átnyúló áramlását. Megnövekedett az állami és a magánszereplők, köztük a

természetes személyek, egyesületek és a vállalkozások között Unió-szerte zajló személyes adatok cseréje. Az uniós jog együttműködésre és személyes adatok cseréjére kötelezi tagállamok nemzeti hatóságait annak érdekében, hogy képesek legyenek feladataikat ellátni, illetve hogy más tagállam hatóságai nevében eljárjanak. (GDPR preamb. 5. pont)

2. A személyes adatok gyűjtése és megosztása jelentős mértékben megnőtt. A technológia a vállalkozások és a közhatalmi szervek számára tevékenységük folytatásához a személyes adatok felhasználását minden eddiginél nagyobb mértékben lehetővé teszi. Az emberek egyre nagyobb mértékben hoznak nyilvánosságra és tesznek globális szinten elérhetővé személyes adatokat. A technológia egyaránt átalakította a gazdasági és a társadalmi életet, és egyre inkább elősegíti a személyes adatok Unión belüli szabad áramlását és a személyes adatok harmadik országok és nemzetközi szervezetek részére történő továbbítását, biztosítva egyúttal a személyes adatok magas szintű védelmét. (GDPR preamb. 6. pont)

3. E fejlemények egy olyan szilárd és az eddiginél következetesebb uniós adatvédelmi keretet igényelnek, amelyet erős kikényszeríthetőség támogat. ... A természetes személyek számára biztosítani kell, hogy saját személyes adataik felett maguk rendelkezzenek. ... (GDPR preamb. 7. pont)

4. Az a tény, hogy a személyes adatok kezelése tekintetében a természetes személyek jogai és szabadságai egyes tagállamokban eltérő szintű védelmet élveznek, különösen, ami személyes adatok védelméhez való jogot illeti, a személyes adatok Unióban történő szabad áramlásának útjában állhat. Ebből eredően ezek az eltérések a gazdasági tevékenységek uniós szinten való folytatásának akadályát képezhetik, torzíthatják a versenyt, és hátráltathatják a hatóságokat az uniós jog szerinti feladataik ellátásában. ... (GDPR preamb. 9. pont)

5. ... A természetes személyeknek a személyes adataik kezeléséhez kapcsolódó alapvető jogai és szabadságai védelmére vonatkozó szabályok következetes és egységes alkalmazását az Unió egész területén biztosítani kell. ... (GDPR preamb. 10. pont)

6. ... a személyes adatok védelmére vonatkozó szabályok betartásának ellenőrzéséhez és biztosításához egyenértékű hatáskört is biztosítani szükséges, és a jogsértőkre azonos szankciókat kell alkalmazni. (GDPR preamb. 11. pont)

7. ... rendelettel kell biztosítani a jogbiztonságot és az áttekinthetőséget valamennyi tagállam gazdasági szereplői részére – beleértve a mikro-, kis- és középvállalkozásokat is –, továbbá rendelettel kell biztosítani a természetes személyek részére minden tagállamban azonos szintű, jogi úton érvényesíthető jogokat és kötelezettségeket, az adatkezelők és adatfeldolgozók számára azonos felelősséget, a személyes adatok kezelésének következetes nyomon követését, valamennyi tagállamban azonos szankciók alkalmazását... A belső piac megfelelő működése érdekében a személyes adatok Unión belüli szabad áramlását ... nem szabad korlátozni vagy megtiltani. ... E rendelet alkalmazása során az uniós intézményeket és szerveket, és a tagállamokat és azok felügyeleti hatóságait ösztönözni kell, hogy vegyék figyelembe a mikro-, kis- és középvállalkozások sajátos szükségleteit. (GDPR preamb. 13. pont)

8. ... a természetes személyek védelmének technológiailag semlegesnek kell lennie és nem függhet a felhasznált technikai megoldásoktól. ... a manuális kezelésre is vonatkozik... (GDPR preamb. 15. pont)

A Szabályzat további részeiben a GDPR hivatkozott pontja után azon saját magyarázatokat fűzzük, amelyek az általános szabályozás orvosi vállalkozásokra értelmezhetőségét szolgálják. A jól elkülöníthetőség érdekében a magyarázatot **vastag betűvel írjuk**.

A GDPR által megfogalmazott adatkezelési, adatvédelmi elvek

1. Az adatvédelem elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell. Az álnevesített személyes adatok, amelyeket további információ felhasználásával valamely természetes személlyel kapcsolatba lehet hozni, azonosítható természetes személyre vonatkozó adatnak kell tekinteni. ... (GDPR preamb. 26. pont).

Ez számunkra azt jelenti, hogy a TAJ számot, de a személyi számot is az adott személyre vonatkozó adatnak kell tekinteni, felfoghatjuk álnevesítésként, hiszen ezzel a személy egyértelműen beazonosítható.

2. Az adatkezelésre csak akkor kerülhet sor, ha az érintett egyértelmű megerősítő cselekedettel, például írásbeli – ideértve az elektronikus úton tett –, vagy szóbeli nyilatkozattal önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulását adja a természetes személyt érintő személyes adatok kezeléséhez. ... (GDPR preamb. 32. pont).

Ezt a szabályt nem kell alkalmaznunk, mert az adatkezelés jogalapjai közül az érintett hozzájárulása csak az egyik. Az orvosi adatkezelés jogalapja az Egészségügyi Törvényben előírt jogszabályi kötelezettség, ami erősebb, mint az egyéni hozzájárulás. Magyarul: soha a betegeinktől semmilyen hozzájárulást nem kell kérni és aláírni az adataik kezeléséhez. Ez a mentesség nem vonatkozik a magán-tevékenység, vagy magánintézményi tevékenység során történő betegellátásra, ott tehát szükséges az adott személy felhatalmazó, beleegyező nyilatkozata.

3. A gyermekek személyes adatai különös védelmet érdemelnek. ... A közvetlenül a gyermek részére nyújtott megelőzési és tanácsadási szolgáltatások esetében nincs szükség a szülői felügyelet gyakorlójának hozzájárulására. (GDPR preamb. 38. pont). **Tehát: a gyermekeket ellátó gyermekorvosi és egyes praxisok esetében a gyermekek szüleitől, vagy a szülői jogokat gyakorló személytől sem kell semmilyen hozzájárulást kérni vagy aláírni.**

4. ... a természetüknél fogva különösen érzékeny személyes adatok egyedi védelmet igényelnek, mivel az alapvető jogokra és szabadságokra nézve a kezelésük körülményei jelentős kockázatot hordozhatnak. ... (GDPR preamb. 51. pont).

A személyes adatok különleges kategóriáira vonatkozó adatkezelési tilalomtól való eltérés ... megengedhető, ha erről az uniós vagy tagállami jog rendelkezik. (GDPR preamb. 52. pont).

... a sajátos adatkezelési szükségletek tekintetében ebben a rendeletben harmonizált feltételeket kell meghatározni az egészségügyi személyes adatok különleges kategóriáinak kezelésére vonatkozóan, különösen azt illetően, ha ezen adatok kezelését bizonyos egészséggel kapcsolatos célokból olyan személyek végzik, akikre jogszabályban megállapított szakmai titoktartási kötelezettség vonatkozik. ... (GDPR preamb. 53. pont).

A népegészség területén közérdekből szükséges lehet a személyes adatok különleges kategóriáinak az érintett hozzájárulása nélkül történő kezelése. Ilyen ... valamennyi, az egészséggel kapcsolatos elem,

nevezetesen az egészségi állapot – beleértve a morbiditást és a fogyatékossgot –, az egészségi állapotot meghatározó tényezők, az egészségügyi ellátással kapcsolatos igények, az egészségügyi ellátásra biztosított források, az egészségügyi ellátás nyújtása és az ahhoz való általános hozzáférés, valamint az egészségügyi ellátással kapcsolatos kiadások és finanszírozás, továbbá a halálokok. Az egészségügyi adatok ilyen közérdekű kezelése nem eredményezheti a személyes adatok más célokból harmadik személyek, így munkáltatók, vagy biztosítók és bankok általi kezelését. (GDPR preamb. 53. pont).

Az általunk kezelt adatok tehát az adatok különleges (érzékeny, fokozott kockázatot hordozó) adatok, amelyek kezeléséhez egyértelműen nem szükséges az érintett hozzájárulása, ám kizárólag a beteg érdekében használhatjuk fel. Érdekes momentum, hogy a foglalkozás-egészségügyi ellátás terén, tehát a munkáltatónak nem adhatjuk ki a dolgozóra vonatkozó adatokat, csak az „alkalmas-nem alkalmas” tényről közölhetjük, amit ő köteles tudomásul venni. Az adatok különleges kategóriájából sok minden más kötöttség, olykor könnyebbég fakad, amire részleteiben a konkrét gyakorlati szabályzati részben térünk ki.

5. A tisztességes és átlátható adatkezelés elve megköveteli, hogy az érintett tájékoztatást kapjon az adatkezelés tényéről és céljairól, ... figyelembe véve a személyes adatok kezelésének konkrét körülményeit és kontextusát. (GDPR preamb. 61. pont).

Ezt megoldottuk azzal az adatkezelési tájékoztatóval, amelyet kihelyeztünk a rendelőben a várószobában, jól látható helyen.

6. Az érintett jogosult, hogy hozzáférjen a rá vonatkozóan gyűjtött adatokhoz. ... Ez magában foglalja az érintett jogát arra, hogy az egészségi állapotára vonatkozó személyes adatokhoz – mint például a diagnózis, a vizsgálati leletek, a kezelőorvosok véleményei, valamint a kezeléseket és a beavatkozásokat tartalmazó egészségügyi dokumentációk – hozzáférjen. (GDPR preamb. 63. pont).

Ezt megvalósítjuk azzal, hogy a vizsgálat során tapasztalt észleleteket (=status), mért eredményeket (=pulzus, vérnyomás), valamint a labor és eszközös vizsgálatok leleteit átadjuk a betegnek, valamint szakvélemény vagy jelentés, vagy zárójelentés formájában, illetve a beteg számára saját magunk készítette magyarázatokat, leírásokat adunk a kezébe. Fokozottan kell ügyelnünk az EESZT-n keresztül történő kommunikációra, hogy az illető beteg érdekei az adatkezelés során ne sérüljenek. Ugyanakkor figyelni kell a Covid járvány kikényszerítette telefonos és más, telemedicinális információk, mint érzékeny adatok kezelésére. Jelenleg nincs megnyugtató saját eljárásrendünk sem, adott esetben a mobil telefontal lefotózott, látható tünetek (bőrkiütés, sérülés, stb.) továbbítására és a vizsgálati eredményekre sem.

7. Az érintett jogosult arra, hogy kérhesse a rá vonatkozó személyes adatok helyesbítését és megilleti őt az „elfeledtetéshez való jog”. ... Az érintett jogosult különösen arra, hogy személyes adatait törölje és a továbbiakban ne kezelje. ... Ugyanakkor a személyes adatok további megőrzése jogszerűnek tekinthető, ha az ... valamely jogi kötelezettségnek való megfelelés, illetőleg közérdekből végzett feladat végrehajtása vagy ... a népegészségügy területét érintő közérdekből ... szükséges. (GDPR preamb. 65. pont).

Az uniós és a tagállami jog olyan mértékig korlátozhat bizonyos elveket, a tájékoztatáshoz való jogot, a hozzáférési, helyesbítési és törlési jogot, az adathordozhatósághoz való jogot, a tiltakozáshoz való

jogot, ... amilyen mértékig ez egy demokratikus társadalomban szükségesnek és arányosnak tekinthető. (GDPR preamb. 73. pont).

Tekintettel arra, hogy az Egészségügyi tv. előírásai erősebb érvek, ezért a betegek személyes adatai helyesbítési joga csupán a hétköznapi adataira vonatkozhat (lakcím, életkor, telefonszám, stb.). Törlési joga más orvoshoz távozás esetén értelmezhető, csakúgy, mint adathordozási joga, de orvosi adatait akkor is meg kell őriznünk a mindenkor érvényes, ránk vonatkozó törvényi előírásnak megfelelően.

A GDPR által megfogalmazott gyakorlati követelmények az adatkezelés, adatvédelem területén, amit a szabályzatoknak is tükrözniük kell.

1. Az érintett jogait és szabadságait érintő kockázat valószínűségét és súlyosságát az adatkezelés jellegének, hatókörének, körülményeinek és céljainak függvényében kell meghatározni. A kockázatot olyan objektív értékelés alapján kell felmérni, amelynek során szükséges megállapítani, hogy az adatkezelési műveletek kockázattal, illetve nagy kockázattal járnak-e. (GDPR preamb. 76. pont).

Ezt megteesszük az adatvédelmi hatástanulmány keretében a TQM eszköztár segítségével konkrétan számszerűsítve, amelynek az érintettekkel történő konzultáció alapján elfogadott végleges változata az adatvédelmi szabályzat 1. számú Mellékletét képezi.

2. természetes személyeket személyes adataik kezelése tekintetében megillető jogok és szabadságok védelme megköveteli az e rendelet követelményeinek teljesítését biztosító megfelelő technikai és szervezési intézkedések meghozatalát. Ahhoz, hogy az adatkezelő igazolni tudja az e rendeletnek való megfelelést, olyan belső szabályokat kell alkalmaznia, valamint olyan intézkedéseket kell végrehajtania, amelyek teljesítik különösen a beépített és az alapértelmezett adatvédelem elveit. (GDPR preamb. 78. pont).

Ezen követelménynek részben a hatástanulmány jobb oldali oszlopában rögzített megfelelést szolgáló módosító intézkedésekkel teszünk eleget, részben pedig megfelelünk azzal, hogy belső szabályainkat jelen adatkezelési szabályzatban írásba foglaljuk.

3. Az adatkezelő vagy az adatfeldolgozó az e rendeletnek való megfelelés bizonyítása érdekében nyilvántartást vezet a hatásköre alapján végzett adatkezelési tevékenységekről. Minden adatkezelő és adatfeldolgozó köteles a felügyeleti hatósággal együttműködni és ezeket a nyilvántartásokat kérésre hozzáférhetővé tenni az érintett adatkezelési műveletek ellenőrzése érdekében. (GDPR preamb. 82. pont).

Ehhez a ponthoz hozzá kell fűznünk a következőket: a GDPR más helyen azt mondja, hogy nyilvántartást nem kell vezetni a 250 fő alatti munkavállalói létszámú szervezeteknek, ugyanakkor megint más helyen kötelezővé teszi a nyilvántartás vezetését, ha különleges adatokat kezelünk. Mivel ez az erősebb érv, tehát nyilvántartásokat vezetünk és jelen szabályzat mellékletében dokumentált információként rögzítjük.

4. A biztonság fenntartása és az e rendeletet sértő adatkezelés megelőzése érdekében az adatkezelő vagy az adatfeldolgozó értékeli az adatkezelés természetéből fakadó kockázatokat, és az e kockázatok csökkentését szolgáló intézkedéseket, például titkosítást alkalmaz. ... Az adatbiztonsági kockázat felmérése során a személyes adatok kezelése jelentette olyan kockázatokat – mint például a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés –mérlegelni kell, amelyek fizikai, vagyoni vagy nem vagyoni károkhhoz vezethetnek. (GDPR preamb. 83. pont).

Az e rendeletnek való megfelelés olyan esetek érdekében történő előmozdítása érdekében, amikor valószínűsíthető, hogy az adatkezelési műveletek magas kockázattal járnának a természetes személyek jogaira és szabadságaira nézve, az e kockázat forrását, jellegét, egyediségét és súlyosságát felmérő adatvédelmi hatásvizsgálat elvégzéséért az adatkezelő felel. A hatásvizsgálat megállapításait figyelembe kell venni annak meghatározásakor, hogy mely intézkedések a megfelelőek annak bizonyítására, hogy a személyes adatok kezelése megfelel e rendeletnek. (GDPR preamb. 84. pont).

Adatvédelmi hatásvizsgálatot végzünk az ISO/IEC 29134 európai szabvány konkrét, hatástanulmányra vonatkozó előírásainak szigorú követésével, és így teljesítjük ezen előírt követelményeket. Az ISO/IEC 29134 európai szabvány 2018 óta nem változott, így jelen 2022-es megújítás során változatlan formában alkalmazzuk.

5. Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek. ... Következésképpen, amint az adatkezelő tudomására jut az adatvédelmi incidens, azt indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenteni köteles az illetékes felügyeleti hatóságnál, kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani tudja, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. ... (GDPR preamb. 85. pont).

Megfelelésképpen jelen szabályzatunkban egy önálló fejezetben foglalkozunk az adatvédelmi incidensek fajtáival, a reálisan a praxisban értelmezhető formáival, megelőzésükre tett intézkedésekkel, a mégis bekövetkezés esetére vonatkozó megoldásokkal, valamint dokumentált információként rögzítjük az adatvédelmi incidensek nyilvántartásának és jelentéseinek jegyzőkönyvét a Szabályzat 2. számú Mellékletében.

6. A természetes személyek jogaira és szabadságaira nézve magas kockázattal járó ilyen esetekben az adatkezelő – annak érdekében, hogy az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a kockázat forrásait figyelembe véve felmérje a magas kockázat különös valószínűségét és súlyosságát – az adatkezelés előtt adatvédelmi hatásvizsgálatot végez. Ez a hatásvizsgálat magában foglalja különösen az említett kockázat mérséklését, a személyes adatok védelmét, valamint az e rendeletnek való megfelelés bizonyítását célzó tervezett intézkedéseket, garanciákat és mechanizmusokat. (GDPR preamb. 90. pont).

Ez különösen vonatkozik ... azokra a ... műveletekre, amelyek ... az adatok érzékenysége folytán valószínűsíthetően magas kockázattal járnak. (GDPR preamb. 91. pont).

Ez esetben is az érvényes, hogy adatvédelmi hatásvizsgálatot végzünk az ISO/IEC 29134 európai szabvány konkrét, hatástanulmányra vonatkozó előírásainak szigorú követésével, és így teljesítjük ezen előírt követelményeket.

Praxisunk adatkezelési gyakorlata —megfeleltetve a GDPR előírásainak.

Adatkezelési szabályzatunk összeállítását megelőzően adatvédelmi hatástanulmány készült a vonatkozó ISO/IEC 29134 szabvány alkalmazásával. A hatástanulmány számszerűsített adatvédelmi kockázatelemzéséhez kapcsolódóan módosító javaslatokat fogalmazott meg. A javasolt módosításokat a lehető mértékig végrehajtottuk, illetve a jövőben reális időpontokban végrehajjtjuk. A módosítások nyomán valamennyi „maradék kockázat” az elviselhető kategóriába kerül. Adatvédelmi Szabályzatunk ezen tények és körülmények figyelembe vételével készült. A hatástanulmány a Szabályzat részét képezi, annak 1. számú Mellékleteként.

Adatkezelési Szabályzatunkban a GDPR előírásainak sorrendjét követjük, a GDPR elvei szerint (GDPR preamb.13.) fókuszálva az orvosi tevékenységet folytató vállalkozás méretéből, létszámából és speciális működési területéből fakadó sajátosságokra. Számba vesszük azokat a pontokat is, amelyek jelenleg praxisunkat nem érintik, azért, hogy a jövőbeni esetleges változásokra tekintettel könnyedén bővíthető legyen a Szabályzat alapvető szerkezetének megtartása mellett.

Minden pontban, ha szükséges, értelmezzük, hogy az abban megfogalmazott elvárások hogyan értelmezhetőek a mi esetünkben, megfogalmazzuk az általunk követett gyakorlatot és megfeleltetjük az elvárással.

1. cikk. Tárgy (1) Ez a rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a személyes adatok szabad áramlására vonatkozó szabályokat állapít meg.

Praxisunkban az adatkezeléssel érintett természetes személyek a hozzánk bejelentkezett, illetve a területi kötelezettség alapján jelentkező, valamint az akut szükség szülte helyzetekben hozzánk sürgősségi ellátásra jelentkező személyek. Emellett kezelünk munkaügyi jellegű adatokat, amelyek alkalmazottunkra vagy alkalmazottainkra vonatkoznak. Az Ő esetükben nem egészségügyi értelemben vett érzékeny adatokról van szó, így az Ő betekintési, adattörlési, adtmódosítási, adathordozási jogait szabadon gyakorolják, ezen jogait maximálisan biztosítjuk.

2. cikk. Tárgyi hatály. E rendeletet kell alkalmazni a személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik ...

Tehát az 1-es pontban részletezett pácienseinkre és munkavállalóinkra terjed ki a Rendelet tárgyi hatálya.

3. cikk. Területi hatály. E rendeletet kell alkalmazni a személyes adatoknak az Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére ...

Praxisunk Magyarországon, tehát az EU területén működik, így ránk is kötelezően érvényes a Rendelet.

4. cikk. Fogalommeghatározások. Azokat a fogalmakat emeljük csak ki, amelyek a mi esetünkben relevánsak.

4.1. „személyes adat”: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, ... például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható. (4.cikk.1.)

Személyes adatként értelmezzük fentiekben túlmenően a TAJ számot, minden egészségügyi-orvosi tartalmú leletet, véleményt. A jövőben figyelniünk kell az újabb és újabb digitális egészségügyi és ellátási megoldások során is, különösen a határokon átnyúló adatforgalom terén.

4.2. „adatkezelés”: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás ... (4.cikk.2.)

Így adatkezelésnek minősül a betegeinkről rögzített valamennyi információ, magával hozott zárójelentés, lelet és az általunk észlelt vizsgálati leletek rögzítése, status leírás és az általunk kért vizsgálatok eredményeinek rögzítése, valamint a törvényi kötelezettségből eredő adattovábbítások pl. a NEAK és az ÁNTSZ felé is. Újdonság az EESZT-n keresztül, illetve a különféle, fejlődőben lévő telemedicinális megoldások során megvalósuló adatkezelés, hogy megvalósuljon a GDPR-nak való megfelelés.

4.3. „adatkezelő”: az a természetes vagy jogi személy, közhatalmi szerv, ... amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza. ... ; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt ... a tagállami jog is meghatározhatja. (4.cikk.7.)

Az Eü. tv. (=tagállami jog) kötelezi az orvost a betegek adatainak kezelésére, így praxisunkban az adatkezelő az orvos, és az általa megnevezett asszisztens. Ugyanakkor ma már adatkezelőnek kell tekinteni az EESZT-t, illetve az azt működtető szervezetet is.

4.4. „adatfeldolgozó”: az a természetes vagy jogi személy, közhatalmi szerv, ... amely az adatkezelő nevében személyes adatokat kezel. (4.cikk.8.)

A mi esetünkben az adatfeldolgozó az orvos és/vagy az asszisztens. Egyéb esetben külön szerződést kötünk olyan feldolgozóval, aki megfelel a GDPR előírásainak.

4.5. „címezett”: az a természetes vagy jogi személy, közhatalmi szerv, ... akivel vagy amellyel a személyes adatot közlik. ... (4.cikk.9.)

Ilyen például az ÁNTSZ, a NEAK, a KSH, a saját könyvelőnk, olykor az Önkormányzat, a Gyámhivatal.

4.6. „harmadik fél”: az a természetes vagy jogi személy, ... amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak. (4.cikk.10.)

Praxisunkban ez megegyezik a 4.5. pontban leírtakkal: ÁNTSZ, a NEAK, a KSH, a saját könyvelőnk, olykor az Önkormányzat, a Gyámhivatal. A praxisközösségekben résztvevő többi praxis, valamint a velük szerződésben álló egyéb ellátó szakszemélyzet, mint a gyógytornász, dietetikus, logopédus és mások.

4.7. „az érintett hozzájárulása”: ... (4.cikk.11.)

Esetünkben nem értelmezhető, mert adatkezelésünk jogalapja jogszabályi, törvényi kötelezettség, az érintett hozzájárulását ezért semmilyen módon kérnünk nem kell. Kivétel a magán-tevékenység vagy magán egészségügyi intézmény keretei közt végzett tevékenység során ellátott személy, aki ez esetben „érintett” és adatai kezeléséhez a hozzájárulása szükséges.

4.8. „adatvédelmi incidens”: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. (4.cikk.12.)

Számunkra ennek a pontnak a jelentése egyértelmű.

4.9. „genetikai adat”: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz. ... (4.cikk.13.)

Számunkra ennek a pontnak a jelentése egyértelmű.

4.10. „biometrikus adat”: egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat. (4.cikk.14.)

Számunkra ennek a pontnak a jelentése egyértelmű.

4.11. „egészségügyi adat”: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra

vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról. (4.cikk.15.)

Számunkra ennek a pontnak a jelentése egyértelmű.

5. cikk. A személyes adatok kezelésére vonatkozó elvek

5. 1. A személyes adatok ... kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („jogszerűség, tisztességes eljárás és átláthatóság”)

Adatkezelésünk jogszerű, mert törvényi előírás kötelez rá. (Eü. tv. 1997). Tisztességességét orvosi szaktudásunk, hivatásunk és orvosi eskünk garantálja, amúgy ellenőrizhetetlen, nem is érdemes külső, nem szakembernek ezzel próbálkoznia... Adatkezelésünk átlátható, hiszen a betegeinkkel mindent megbeszélünk, elmagyarázunk, megértetünk, és csak ezt követően végzünk bármely olyan orvosi tevékenységet, amely az érintett adatai kezelését vonja magával.

5.1.1. A személyes adatok ... gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjék, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. ... ; nem minősül az eredeti céllal össze nem egyeztethetőnek a ... tudományos ... kutatási célból vagy statisztikai célból történő további adatkezelés (GDPR 89. cikk.1) („célhoz kötöttség”)

A célhoz kötöttség egyértelműen érvényesül: kizárólag a ránk bízott páciensek egészségének fejlesztése, megőrzése, helyreállítása, betegségei gyógyítása célját szolgálja. Ez ellenőrizhető, tárgyszerűen bizonyítható.

5.1.2. A személyes adatok ... az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („adattakarékosság”).

Ezzel az előírással némileg ellenkezik a gyűjtendő és kezelendő adatok köre és mennyisége az orvos társadalom többségének a véleménye szerint, az alapvető cél szempontjából nem megfelelőek, nem relevánsak és messze túlmennek a szükséges mértéken. Ugyanakkor jogszabály (tagállami jog) kötelez rá. Az Eu-s ajánlások ugyanakkor igen szélesre tárhatják a gyűjtendő adatok körét, mivel a ritka betegségek elleni hatásos megoldások, kutatások, valamint a személyre szabott, célzott kezelések alapját széleskörű adatgyűjtés és egységes adatformátumok tehetik csak lehetővé.

5.1.3. A személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük. ... („pontosság”)

Pácienseink adatait minden egyes rendelőben történő megjelenésük alkalmával áttekintjük, az esetleges pontatlanságokat, időközben történt változásokat bejegyezzük, az újabb orvosi vizsgálat és diagnosztikus-terápiás ténykedés valamennyi adatát naprakészen rögzítjük. Valamint most már az EESZT-ben is rögzítjük, aminek adatbiztonságát (kiberbiztonság) a működtető garantálja.

5.1.4. A személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé. ... („korlátozott tárolhatóság”).

Az adatok tárolásának az idejét tagállami jogszabály kötelezően határozza meg, ami nem feltétlenül esik egybe ezen GDPR előírással, de nekünk továbbra is a magyar, tagországi jogszabályt kell követnünk.

5.1.5. 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 („integritás és bizalmas jelleg”).

Adatkezelési folyamataink sorrendjében haladva, a folyamatszmléletnek megfelelően a következő gyakorlatot honosítjuk meg és erősítjük a reális lehetőségeinkhez mérten napról-napra:

5.1.5.1. számítógépeink, laptopjaink, pendrive-jaink és okos telefonjaink életkorát igyekszünk az újszerű kategóriában tartani, ezzel csökkentve a meghibásodás kockázatát.

5.1.5.2. Valamennyi esetben törekszünk a jelszavas védelem megvalósítására.

5.1.5.3. Új beszerzés esetén alapvető szempont, hogy például a pendrive is eleve jelszavas védelemmel ellátott fajta legyen.

5.1.5.4. Eszközünk elvesztését a legnagyobb mértékben igyekszünk megelőzni. Az ebben a kategóriában leginkább esendő pendrive-okra nyakba akasztható, táskába becsatolható biztosító zsinórt erősítünk.

5.1.5.5. Lopás ellen fokozatosan riasztóval, rendőrségre vagy biztonsági szolgálathoz bekötött, távfelügyeletet ellátó riasztóval szereljük fel, illetve kezdeményezzük a felszerelést.

5.1.5.6. Megelőző intézkedéseink ellenére bekövetkező meghibásodás kockázatának a csökkentése érdekében meghatározott időközönként adatmentést végzünk. Ezeknek egy részét a szoftvert szolgáltató cég biztosítja, saját laptop, okos telefon, tablet és pendrive esetén magunk végezzük vagy végeztetjük el.

5.1.5.7. Papír alapon rögzített dokumentált információinkat (=törzskarton, karton, jelentések, stb.) zárt szekrényben, lehetőség szerint egyre inkább biztonsági zárral ellátott zárt szekrényben őrizzük.

5.1.5.8. A számítógéphez való hozzáférést, a jelszavak ismeretét, a zárt szekrény kulcsának kezelését írásban rögzítjük és erről dokumentált információt csatolunk Szabályzatunk mellékleteként.

5.1.5.9. Tűzoltó készülékeinket a Kockázatkezelési Kézikönyvünk rendelkezései szerinti időközönként ellenőrzítetjük, működőképességük biztosítása céljából.

5.2. Az adatkezelő felelős 5.1. bekezdésnek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására („elszámoltathatóság”).

A felelősséget, illetve ennek igazolását szolgálja Adatkezelési Szabályzatunk, Adatvédelmi hatástanulmányunk, részleteiben pedig a Szabályzat Mellékletét képező adatkezelési nyilvántartások vezetése.

6. cikk. Az adatkezelés jogszerűsége.

6.1. A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül: ... az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges.

A többi jogszerűség felsorolásától eltekintünk, a mi adatkezelésünk az Eü. tv szabta jogi kötelezettségünk teljesítéséhez szükséges.

7. cikk A hozzájárulás feltételei. ...

Felsorolnunk nem szükséges, mert a mi adatkezelésünkhöz semmilyen hozzájárulás beszerzése az érintettektől nem írható elő, adatkezelésünk jogszerűségét a jogi kötelezettség teljesítése adja. Kivétel a magántevékenység vagy magán egészségügyi intézmény keretei közt végzett tevékenység során ellátott személy, akinek adatai kezeléséhez a hozzájárulása szükséges.

8. cikk A gyermek hozzájárulására vonatkozó feltételek az információs társadalommal összefüggő szolgáltatások vonatkozásában

Ránk nem vonatkozik, mert a gyermek szüleitől vagy törvényes képviselőitől sem szükséges hozzájárulást beszerezni az egészségügyi ellátásával kapcsolatos adatkezeléshez. Az információs társadalom egyéb összefüggései pedig kívül esnek orvosi tevékenységünk határain.

9. cikk. A személyes adatok különleges kategóriáinak kezelése.

9.1. A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése tilos.

9.2. A fenti bekezdés nem alkalmazandó abban az esetben, ha: ... az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében, ... ha ezen adatok kezelése olyan szakember által vagy olyan szakember felelőssége mellett történik, aki uniós vagy tagállami jogban, illetve az arra hatáskörrel rendelkező tagállami szervek által megállapított szabályokban meghatározott szakmai titoktartási kötelezettség hatálya alatt áll, illetve olyan más személy által, aki szintén

uniós vagy tagállami jogban, illetve az arra hatáskörrel rendelkező tagállami szervek által megállapított szabályokban meghatározott titoktartási kötelezettség hatálya alatt áll.

Tehát: az általunk kezelt (egészségügyi) adatok a személyes adatok különleges kategóriái közé tartoznak, ezért általában tilos a kezelésük. Mi, orvosok azért kezelhetjük ezen adatokat, mert (tagállami) jog által hozott jogszabály kötelez rá. Az előírt további feltételnek mindenben megfelelünk, hiszen az orvosi titoktartás eskü alatt kötelező számunkra.

10. cikk. A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok kezelése.

11. cikk. Azonosítást nem igénylő adatkezelés.

E két, 10. és 11. cikkben megfogalmazottak nem vonatkoznak ránk, ezért nem részletezzük.

12. cikk. Átlátható tájékoztatás, kommunikáció és az érintett jogainak gyakorlására vonatkozó intézkedések.

12.1. Az adatkezelő megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó, a 13. és a 14. cikkben említett valamennyi információt és a 15–22. és 34. cikk szerinti minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

Tájékoztatót készítünk pácienseink, tehát az érintettek számára, amelyben egyértelműen, érthetően leírjuk, hogy az egészségügyi adatok különleges kategóriája miatt a 13-14. cikkben meghatározott adatokat (tehát a tőlük beszerzett és a máshonnan velük kapcsolatban beszerzett információkat, illetve az ezekből alkotott orvosi véleményünket) minden esetben az ő nyelvükön, az általuk hétköznapi módon érthető megfogalmazásban, röviden, tömören, de minden, a megértést szolgáló részletre kitérően adjuk meg, személyesen szóban, és a szükségesnek ítélt mértékben írásban is. Páciens tájékoztatónkban kitérünk arra is, hogy a 15-22. cikkben felsorolt jogaikkal (hozzáférés, helyesbítés, törlés, korlátozás, adathordozhatóság, tiltakozás) milyen mértékben élhetnek, tekintettel arra, hogy ezen jogaikat jelentős mértékben felülírja a ránk szabott, ezen adatok kezelésére vonatkozó jogszabályi kötelezettség. Ezeket a jogokat és korlátozott mértéknek a magyarázatát részletezzük. A Páciens Tájékoztató szövegét a Szabályzat Mellékletében is rögzítjük.

13. cikk. Rendelkezésre bocsátandó információk, ha a személyes adatokat az érintettől gyűjtik.

14. cikk. Rendelkezésre bocsátandó információk, ha a személyes adatokat nem az érintettől szerezték meg.

Fenti két, 13. és 14. cikkben foglaltakat összevonva kezeljük, mert orvosi gyakorlatunkban szerves egységet alkot és közös outputban ölt eredményt az érintettől beszerzett adatok hordozta információ és a diagnózis felállítása, a hatásos terápia meghatározásához szükséges, elrendelt és elvégzett

vizsgálatokból, azokat végző vizsgáló orvosoktól, tehát nem az érintettől beszerzett adatok hordozta információ.

13-14.1. az adatkezelő az érintett rendelkezésére bocsátja a következő információkat:

13-14.1.1. az adatkezelőnek és – ha van ilyen – az adatkezelő képviselőjének a kiléte és elérhetőségei. (13.1.a) (14.1.a)

Közzöljük a praxist vezető orvos nevét, ha van rezidense, akkor a rezidens nevét, az asszisztens nevét közzöljük, noha általában a beteg számára ez már akkor ismert, amikor hozzánk fordul.

13-14.1.2. az adatvédelmi tisztviselő elérhetőségei, ha van ilyen. (13.1.b) (14.1.b)

Igen van, a nem egyértelmű szabályozás miatt, biztonság kedvéért önkéntes alapon adatvédelmi tisztviselőt jelöltünk ki, akinek a személyét, elérhetőségét a Szabályzatban és a már említett Páciens tájékoztatóban is rögzítjük és az érintettek számára elérhetővé tesszük.

13-14.1.3. a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja. (13.1.c) (14.1.c)

Egyértelmű, és az Adatkezelési Tájékoztatóban rögzítettük, közzétettük.

13-14.1.3. a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen. (13.1.e) (14.1.e)

Az Adatkezelési Tájékoztatóban szintén rögzítettük és közzétettük. Ide tartozik a NEAK, az ÁNTSZ, esetileg a Gyámhatóság és az Önkormányzat.

15. cikk. Az érintett hozzáférési joga.

15.1. Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és ... információkhoz hozzáférést kapjon. (15.1. a-e)

Az adataihoz való hozzáférés joga teljesül a Szabályzatunk 13-14. pontjában leírtak alapján, az ott megfogalmazott módon.

15.2. Az adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. (15.3.)

Pácienseinknek, mint érintetteknek valamennyi nálunk őrzött adata alapján készült orvosi véleményeket, konziliáriusi véleményeket, zárójelentéseket és egyéb leleteket másolatban rendelkezésére bocsátjuk, kérés nélkül is, hiszen ez orvosi tevékenységünk sikeres folytatásának lényeges eleme.

16. cikk. A helyesbítéshez való jog. Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését. (16.)

Az orvosi gyakorlatban helyesbítés az érintett kérésére két esetben értelmezhető és kezelhető, ami szerint eljárunk. Az egyik, ha lakcímében, nevében, telefonszámában pontatlanságot észlel. A másik eset, ha a vizsgálatkor nem jutott eszébe valamilyen, az egészségi állapota szempontjából érdekelges adat, és később ezzel kiegészítené a róla felvett és rögzített információkat. Ennek elbírálása orvosi kompetencia. Minden más helyesbítés kizárt.

17. cikk A törléshez való jog („az elfeledtetéshez való jog”)

17.1. Az érintett jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje ... (17.1.)

17.2. Az (1) (17.1.)... bekezdés nem alkalmazandó, amennyiben az adatkezelés szükséges ... a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából. (17.3.b.)

Eszerint kell eljárunk, tehát pácienseink semmilyen módon nem élhetnek törlési jogukkal, mert az ellenkezik a tagállami, vagyis a magyar, érvényes, ránk kötelező jogszabályi előírásokkal. Ennek értelmében bármiféle törlési igényt ezen tények alapján el kell utasítanunk.

18. cikk Az adatkezelés korlátozásához való jog

18.1. Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha az ... érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát. (18.1.a)

Ez a jog kizárólag az adminisztratív jellegű adatokra, tehát név, lakcím, születési dátum, TAJ szám, telefonszám és ehhez hasonlókra vonatkozhat. Ennek tudatában alkalmazzuk és eszerint járunk el.

19. cikk A személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség.

19.1. Az adatkezelő minden olyan címzettet tájékoztat a ... helyesbítésről, ... vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték. (19.)

Ha az érintett (páciens, beteg) adatait a fenti adatok tekintetében módosítottuk, akkor a módosításokat közöljük azon címzettekkel, akikhez az érintett páciens adatait esetleg továbbítottuk. Magyarul, ha a NEAK vagy ÁNTSZ felé adatot továbbítottunk, akkor abban is helyesbítjük (a címet, TAJ számot, telefonszámot, stb.).

20. cikk. Az adathordozhatósághoz való jog.

20.1. Az érintett jogosult arra, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa... (20.1.)

20.2. Az említett jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges. (20.3.)

Orvosi gyakorlatunkban az adathordozáshoz való jog ennek ellenére, korlátozott módon ugyan, de fontos célból és jó eredménnyel alkalmazható és alkalmazzuk is abban az esetben, ha páciensünk más országba, más településre költözik és önszántából vagy körülményei kényszerítő jellege miatt más orvoshoz kéri át az ellátását. Ebben az esetben valamennyi adatát orvos-orvos kapcsolaton keresztül, közvetlenül továbbadjuk az új ellátó orvosnak, tehát az adathordozási jog érvényesül. Annyi különbség van, hogy az érintett adatait magunknál is meg kell őriznünk a jogszabályi előírásban foglaltak szerint, amíg ezen nem változtatnak. Némileg módosítja a helyzetet, és jobban megfelel az adataival való rendelkezés GDPR szellemének az EESZT léte és alkalmazása, ami segítségével a páciens adatait azzal osztja meg, akivel saját döntése alapján azt célszerűnek vagy fontosnak ítéli meg.

21. cikk A tiltakozáshoz való jog

Orvosi gyakorlatunkban nem gyakorolható, az erősebb tagállami jogszabályi kötelezettségünk miatt.

22. cikk. Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást.

23. cikk. Korlátozások.

Gyakorlatunkban a 23-24. cikkben foglaltakat nem alkalmazzuk, illetve nem értelmezhető, ezért Szabályzatunkban részleteiben nem taglaljuk.

24. cikk. Az adatkezelő feladatai.

24.1. Az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése e rendelettel összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi.

Az itt megfogalmazott elvárásnak való megfelelés érdekében bevezetett, illetve végrehajtott vagy végrehajtandó intézkedéseket Szabályzatunk 5.1.5.1 – 5.1.5.9. pontjában részletezzük. (Lásd ott!). Ezen intézkedéseket, működőképességüket, eredményességüket, elégséges mivoltukat időről időre ellenőrizzük és a PDCA elvnek megfelelően módosításokat hajtunk végre. Mindezen akciókat és tényeket dokumentált információként megőrizzük és felhasználjuk Adatkezelési Szabályzatunk 3 évente esedékes megújításához.

24.2. A 40. cikk szerinti jóváhagyott magatartási kódexekhez vagy a 42. cikk szerinti jóváhagyott tanúsítási mechanizmushoz való csatlakozás felhasználható annak bizonyítása részeként, hogy az adatkezelő teljesíti kötelezettségeit. (24.3.)

Ezzel kapcsolatos álláspontunkat, gyakorlatunkat a 40. cikknél kifejtjük részletesen.

25. cikk. Beépített és alapértelmezett adatvédelem.

25.1. Az adatkezelő a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket – például álnevesítést – hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt az e rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.

A Szabályzatunk 5.1.5.1 – 5.1.5.9. pontjaiban részletezett intézkedéseket további, garanciális elemekkel tesszük teljessé, nevezetesen valamennyi harmadik féllel kötött szerződés módosítását kezdeményezzük abban az értelemben, hogy egyértelműen egészüljenek ki ezek a szerződések részben a harmadik fél által vállalt kötelezettséggel az ő részéről a GDPR alkalmazására, valamint ahol az értelmezhető és célszerű egészüljön ki a titoktartási kötelezettség beépítésével.

26. cikk. Közös adatkezelők.

Nincs közös adatkezelésünk, ezért nem részletezzük.

27. cikk. Az Unióban tevékenységi hellyel nem rendelkező adatkezelők vagy adatfeldolgozók képviselői.

Az Unióban tevékenykedünk, székhelyünk, telephelyünk is az Unióban van, tehát ez a pont nem értelmezhető számunkra.

28. cikk. Az adatfeldolgozó.

28.1. Ha az adatkezelést az adatkezelő nevében más végzi, az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés e rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására. (28.1-10.)

Jelenleg nem végzi más az általunk kezelt adatok feldolgozását. Ha bármikor sor kerülne rá, hogy más adatfeldolgozót bízunk meg, akkor abban az esetben az előírások pontos követésével fogjuk azt megtenni, és Szabályzatunkat kiegészítjük az erre vonatkozó bekezdésekkel.

29. cikk. Az adatkezelő vagy az adatfeldolgozó irányítása alatt végzett adatkezelés.

Jelenleg gyakorlatunkban nem történik.

30. cikk. Az adatkezelési tevékenységek nyilvántartása.

30.1. Minden adatkezelő ... a felelősségébe tartozóan végzett adatkezelési tevékenységekről nyilvántartást vezet. E nyilvántartás a következő információkat tartalmazza: a) az adatkezelő neve és elérhetősége, ... az adatvédelmi tisztviselőnek a neve és elérhetősége; b) az adatkezelés céljai; c) az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése; d) olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják ... (30.1.a-e.)

30.2. Az (1) ... bekezdésben foglalt kötelezettségek nem vonatkoznak a 250 főnél kevesebb személyt foglalkoztató vállalkozásra vagy szervezetre, kivéve, ha az általa végzett adatkezelés az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal jár, ha az adatkezelés nem alkalmi jellegű, vagy ha az adatkezelés kiterjed a személyes adatok 9. cikk (1) bekezdésében említett különleges kategóriáinak ... kezelésére. (30.5.)

Ebből egyértelmű, hogy orvosi gyakorlatunkban, praxisunkban az adatkezelési tevékenységről nyilvántartást kell vezetnünk. a nyilvántartásban rögzítjük az adatkezelő és adatfeldolgozó nevét, elérhetőségét, az adatvédelmi tisztviselő nevét elérhetőségét, az adatkezelés célját, noha azt jogszabály írja elő, és a címzetteket konkrétan, ahová adatokat továbbítunk, bár szintén jogszabályi kötelezettség által. Adatkezelési nyilvántartás a Szabályzat 2. számú Mellékletében található.

31. cikk. Együttműködés a felügyeleti hatósággal. Az adatkezelő és az adatfeldolgozó, valamint – ha van ilyen – az adatkezelő vagy az adatfeldolgozó képviselője feladatai végrehajtása során a felügyeleti hatósággal – annak megkeresése alapján – együttműködik.

Együttműködünk, Szabályzatunkat és Adatvédelmi hatástanulmányunkat, nyilvántartásainkat betekintésre, ellenőrzésre rendelkezésükre bocsátjuk.

32. cikk. Az adatkezelés biztonsága.

32.1. Az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja.

A kockázatokat elemeztük, értékeltük, a kockázatok megszüntetését, de legalábbis elviselhető, kezelhető szintre csökkentését célzó intézkedéseket megtettük, illetve tervbe vannak véve. A konkrétumokat a Szabályzat mellékletét képező Adatvédelmi hatástanulmányban részleteztük, és összefoglaltuk a Szabályzat 5.1.5.1 -5.1.5.9. pontjaiban.

33. cikk. Az adatvédelmi incidens bejelentése a felügyeleti hatóságnak.

33.1. Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az 55. cikk alapján illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. (33.1.)

Bármilyen adatvédelmi incidens esetén, adatvédelmi hatástanulmányunkat felhasználva a számszerű értékeléshez, megállapítjuk, hogy jár-e olyan veszéllyel, ami miatt jelenteni szükséges, és annak megfelelően járunk el: vagy jelentjük, vagy nem jelentjük, de mindenképp dokumentáljuk és intézkedünk az ismétlődés megelőzéséről.

33.2. Az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az e cikk követelményeinek való megfelelést. (33.5.)

Az adatvédelmi incidensekről a fenti előírás szerint nyilvántartást vezetünk, és azt elhelyezzük a Szabályzatunk mellékletében.

34. cikk. Az érintett tájékoztatása az adatvédelmi incidensről.

34.1. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. (34.1.)

Ha előfordul adatvédelmi incidens, és Hatástanulmányunk értékelő rendszerét alkalmazva, magas kockázatúnak állapítjuk meg, akkor az incidens tényéről részletesen tájékoztatjuk az érintetteket.

35. cikk. Adatvédelmi hatásvizsgálat.

35.1. Ha az adatkezelés ... valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelő ... hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetők.

Praxisunkban részletes hatásvizsgálatot végeztünk az ISO/IEC 29134. számú (Information technology — Security techniques — Guidelines for privacy impact assessment) szabvány előírásai szerint. A hatástanulmányban számszerűsítettük valamennyi fellelhető adatvédelmi kockázat következményének súlyosságát valamint bekövetkezésének valószínűségét. A két számból kalkulált érték (=szorzat) alapján soroltuk be a kockázatokat és az értékekhez rendeltük a módosító, korrigáló javaslatokat, cselekvéseket. Ezt a hatástanulmányt a Szabályzatba 1. számú Mellékletként befoglaltuk. A hatásvizsgálatot minden jelentősebb változás esetén áttekintjük, megújítjuk, de 3 évente a Szabályzat megújítását megelőzően, a megújítási folyamat részeként ismét elvégezzük.

36. cikk. Előzetes konzultáció.

36.1. Ha a 35. cikkben előírt adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az adatkezelő által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az adatkezelő konzultál a felügyeleti hatósággal. (36.1.)

Adatkezelőként a Hatástanulmány ajánlásait a lehető mértékig teljesítettük, így nem volt szükség a felügyeleti hatósággal való konzultációra.

37. cikk. Az adatvédelmi tisztviselő kijelölése.

37.1. Az adatkezelő és az adatfeldolgozó adatvédelmi tisztviselőt jelöl ki minden olyan esetben, amikor: ... az adatkezelő ... fő tevékenységei a személyes adatok 9. cikk szerinti különleges kategóriáinak ... kezelését foglalják magukban.

Bizonytalansági faktor a „fő tevékenység” definiálása. Mivel orvosi tevékenységünk betegeink adatainak ismerete, kezelése nélkül nem lehetne eredményesen folytatható, ezért a Rendelet szelleme szerint a betegek orvosi-egészségügyi adatainak kezelését definíció szerint fő tevékenység kategóriájába kell sorolni. Ebben az esetben pedig ki kell jelölni adatvédelmi tisztviselőt. Enyhítő körülmény, hogy élhetünk a Rendelet más helyén (38.6.) rögzített betűjével, miszerint „az adatvédelmi tisztviselő más feladatokat is elláthat”. Így kijelölhető maga az orvos vagy az asszisztens is.

38. cikk. Az adatvédelmi tisztviselő jogállása.

38.1. Az adatkezelő és az adatfeldolgozó biztosítja, hogy az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjék.

38.2. Az adatkezelő és az adatfeldolgozó támogatja az adatvédelmi tisztviselőt a 39. cikkben említett feladatai ellátásában. ...

38.3. Az adatkezelő és az adatfeldolgozó biztosítja, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el. ...

38.4. Az érintettek a személyes adataik kezeléséhez és az e rendelet szerinti jogaik gyakorlásához kapcsolódó valamennyi kérdésben az adatvédelmi tisztviselőhöz fordulhatnak.

38.5. Az adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség vagy az adatok bizalmas kezelésére vonatkozó kötelezettség köti.

Praxisunkban valamennyi, adatvédelmi tisztviselőre vonatkozó előírást teljesítjük, aszerint járunk el. Adatvédelmi tisztviselői megbízatásának dokumentumát a Szabályzat Melléklete tartalmazza.

39. cikk Az adatvédelmi tisztviselő feladatai.

Az adatvédelmi tisztviselő legalább a következő feladatokat ellátja:

39.1. tájékoztat és szakmai tanácsot ad az adatkezelő vagy az adatfeldolgozó ... részére

39.2. ellenőrzi az e rendeletnek, valamint ... az adatkezelő vagy az adatfeldolgozó személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést.

39.3. együttműködik a felügyeleti hatósággal ...

Praxisunkban az adatvédelmi tisztviselő elsajátítja a Szabályzat tartalmát, tanulmányozza az Adatvédelmi Hatástanulmányt, elmélyed a kockázatok megítélésének és számszerűsítésének módozataiban és ez alapján igyekszik tanácsot adni, ha szükséges. Fontos feladata, hogy az érintettek tájékoztatásáról gondoskodjék, és az érintettek kéréseit továbbítsa, vagy, ha lehet önmaga teljesítse. Ellenőrzés kapcsán a Hatóság felé képviseli a praxist. A magatartási Kódex kialakítását szorgalmazza, az ahhoz való csatlakozást elősegíti, támogatja, a tanúsításokban aktívan részt vesz.

40. cikk Magatartási kódexek

40.1. A tagállamok, a felügyeleti hatóságok, a Testület és a Bizottság ösztönzik olyan magatartási kódexek kidolgozását, amelyek – a különböző adatkezelő ágazatok egyedi jellemzőinek, valamint a mikro-, kis- és középvállalkozások sajátos igényeinek figyelembevételével – segítik e rendelet helyes alkalmazását.

40.2. Az adatkezelők vagy az adatfeldolgozók kategóriáit képviselő egyesületek és egyéb szervezetek magatartási kódexeket dolgozhatnak ki, illetve a már meglévő magatartási kódexeket módosíthatják vagy bővíthetik abból a célból, hogy pontosítsák e rendelet alkalmazását. ...

Üdvözljük az Unió szándékát, bízunk benne, hogy tagállami szinten is hasonlóan gondolkodnak majd. Jelenleg Magatartási Kódexszel még nem rendelkezünk, de érdekvédelmi szervezetünkkel, a Magyarországi Praktizáló Orvosok Szövetségével (MAPOSZ) karöltve törekszünk rá, hogy az ISO-EMI Minőségirányítási rendszerünk, az általunk alkalmazott Infekciókontroll valamint a kötelező Kockázatkezelési Kézikönyvet kiegészítő Minőségügyi Kockázatkezelés már meglévő dokumentumait felhasználva, beépítve, kiegészítsük a most elkészült Adatvédelmi Szabályzatban foglaltakkal, az ISO/IEC 29134 szabvány alapján elkészített Adatvédelmi hatástanulmánnyal, valamint az Evidence Based Medicine-re (EBM) épülő, fokozatosan bővülő szakmai eljárásrendjeinkkel és folyamatábráinkkal, egységes Magatartási Kódexet hozunk létre. A MAPOSZ orvos-minőségügyi auditorai, kockázatkezelő szakemberei döntő szerepet vállalhatnak a magatartási Kódex auditálásában, illetve az ahhoz csatlakozó praxisok komplex auditálásában. Ez a szép jövőképünk sajnos a Covid pandémia miatt időben odább tolódott, de annál inkább tervezzük megvalósítását.

41. cikk. A jóváhagyott magatartási kódexeknek való megfelelés ellenőrzése.

42. cikk. Tanúsítás.

43. cikk. Tanúsító szervezetek.

A 41-43. cikk tartalma sajnos még nem aktuális, ezért nem részletezzük. Amint azonban elmozdulás lesz, vagy mi magunk elmozdulást tudunk generálni, Szabályzatunkat e tekintetben nyomban kibővítjük.

44-59. cikk. A személyes adatok harmadik országokba vagy nemzetközi szervezetek részére történő továbbítása.

Ez a terület minket nem érint, nem foglalkozunk vele ezért.

60-76. cikk. Az Unión belül a felügyeleti hatóságok közti együttműködéssel foglalkozik.

Ez a terület közvetlenül minket nem érint, ezért nem foglalkozunk vele.

77-99. cikk. Jogorvoslat, jogi aktusok, hatályba lépés, záró rendelkezések.

Ez a terület közvetlenül minket nem érint, ezért nem foglalkozunk vele.

1. Melléklet. A fedlapon azonosított orvosi praxisban elkészített

ADATVÉDELMI HATÁSTANULMÁNY

(Privacy Impact Assessment, PIA)

Az adatvédelmi hatástanulmány célja, hogy megvizsgálja az adott szervezet valamennyi olyan tevékenységét, vagy alaptevékenységéhez szükséges, kapcsolódó tevékenységeket, amelyek kapcsán olyan adatokat kell rögzíteni, kezelni, tárolni, adott esetben továbbítani, amely adatok alkalmasak az adathoz kötődő személyek beazonosítására. (PII: Personally Identifiable Information).

Az adatvédelmi hatástanulmányt folyamatosan kell „kezelni”, karbantartani és bizonyos, előre meghatározott időszakonként ismételt elkészíteni. Tekintettel arra, hogy az Adatvédelmi Hatástanulmány „kimenete” az adatok kezelésében rejlő kockázatok megszüntetésére, illetve elfogadható szintre mérséklésére adandó javaslat, így módon a kötelezően elkészítendő Adatkezelési Szabályzat tényszerű alapját képezi.

Az Adatvédelmi Hatástanulmány készítését pontosan szabályozó európai szabvány, az ISO/IEC 29134:2017 legfrissebb elérhető változata az ISO/IEC 29134:2020 semmilyen alapvető változást nem tartalmaz, mindenben azonos az előző szerkezetével, így alapvetően a korábbi Hatástanulmányunk szerkezetét tudjuk követni. Fontos hangsúlyozni a Szabvány azon határozott meghagyásait (1., 7.1.)*, miszerint az útmutatások, előírások alkalmasak bármekkora méretű, bárhol a világon létező, bármely foglalkozást vagy hivatást folytató szervezetre, a sok-ezer alkalmazottat és milliós létszám ügyfélkört kezelő multi vállalattól az egyszemélyes egyéni vállalkozóig, így tehát az ennél általában alig nagyobb orvosi praxisokra, de a praxisközösségekre is. Ugyanakkor az is lényeges szempontja a Szabványnak, hogy messzemenőig figyelembe kell venni a szóban forgó szervezet vagy vállalkozás sajátosságait, mind a hatástanulmány, mind pedig az Adatvédelmi Szabályzat elkészítése során.

A Hatástanulmány elkészítésénél a Fedlapon azonosított Orvosi Praxis vezetők és munkatársai részvételével

A vizsgálódás során az adatkezelési folyamat valamennyi részfolyamatát és az adatkezeléshez, adatfeldolgozáshoz szükséges eszközöket számba kell venni, olyan szemmel nézve, hogy hol, melyikben, milyen módon keletkezhet olyan kockázat, más szóval adatvédelmi veszélyhelyzet, amely a kezelt adatok tulajdonosára nézve veszélyt jelenthetnek.

Ugyancsak vizsgálni kell, hogy ezen adatvédelmi veszélyhelyzetek milyen súlyos következményekkel járhatnak, valamint, hogy az esetleges bekövetkezésüknek mekkora az esélye, vagyis valószínűsége.

*: zárójelben az ISO/IEC 229134:2017 szabvány fejezetszámait írjuk, megfigyelve az átláthatóság követelményének.

A veszély, mint kockázat által okozható kár és a bekövetkeztének a valószínűségi foka együttesen szabják meg, hogy a szóban forgó veszélyhelyzet forrására nézve milyen módosító intézkedéseket, milyen változtatásokat szükséges bevezetni. Másképpen mekkora a veszély és mennyi a valószínűsége, hogy be is következik a veszélyt magában hordó esemény.

Az adatvédelmi hatástanulmány így nézve az adatkezelés kapcsán keletkező kockázatok elemzését, illetve ezen kockázatok kezelésére tett javaslatokat, megoldásokat tartalmazza.

Ha az adott szervezet elfogadja a hatástanulmány kimeneteként, konzultációk során közösen megfogalmazott javaslatokat, akkor készíthető el a GDPR-nak mindenben megfelelő adatkezelését leíró Adatkezelési Szabályzat.

Az orvosi praxisok speciális helyzetében a betegek, páciensek adatait Magyarországon az Egészségügyi Törvény kötelezően írja elő. Ezért nem szükséges a betegektől beleegyező nyilatkozatot kérni adataik kezeléséhez. Az, hogy miért kötelező mégis átvizsgálni adatkezelésünk részleteit, az orvosi titoktartás erős szabálya mellett is, abból a szempontból közelítve érthető meg, hogy az adatok kezelésében, tárolásában mind a személyi oldalról, mind az adattárolás fizikai, elektronikus, digitális oldaláról meg kell próbálnunk elérni a lehető legnagyobb biztonságot. Ezért elérhető helyen ki kell függeszteni az adatkezelői tájékoztatót.

Ugyanakkor követnünk lehet és célszerű is a GDPR-nak való megfelelés alapját képező Hatástanulmány készítését pontosan szabályozó, feljebb már említett európai szabvány, az ISO/IEC 229134:2017. A Szabvány pontos eljárásrendekben határozza meg az egyes rész folyamatok lépéseit, így a Szabvány követése lehetővé teszi a legkülönbözőbb szervezetek, szolgáltatók adatkezelési kultúrájának, adatkezelési biztonságának kvázi számszerű összehasonlítását, egybevetését.

Ezeket az elveket követjük, és az orvosi működés természetes környezetét, jogszabály meghatározta legszükségesebb külső kapcsolódásait nem lépjük túl.

A Hatástanulmány elkészítésében a Fedlapon azonosított Orvosi Praxis vezetője megbízása alapján, partnerként a Magyarországi Praktizáló Orvosok Szövetsége (MAPOSZ) orvos-minőségügyi auditori csoportja és Kockázatelemző szakemberei működtek közre.

Időszak: 2018. május 15-től 2021. december 31-ig, majd 2022. január 1-től kezdődően

A vizsgált Praxis címe, elérhetősége, a kapcsolattartó személy neve elérhetősége a Fedlapon azonosított adatok szerint.

0. Az Adatvédelmi Hatástanulmány tartalma

1. A hatástanulmány érdekében folytatott vizsgálódás kiterjedési körének meghatározása. (7.3.)
2. Adatvédelmi követelmények azonosítása, rögzítése. (7.4.)
3. Az adatvédelmi kockázatok elemzése. Számszerűsítése. (7.5.)
4. Adatvédelmi kockázatkezelési terv készítése, elképzelések megfogalmazása. (7.6.)
5. Következtetések és elhatározások, megfontolandó változtatási lehetőségek összefoglalása. (7.7.)
6. Az adatkezelésben érintett személyek összefoglaló, nyilvános tájékoztatása. (7.8)

1. A hatástanulmány hatókörének meghatározása. (7.3.)

1.1. A vizsgálat alatt álló szervezet (7.3.1.)

1.1.1. Általános információk. A praxis működése. (7.3.1.2.)

Az orvosi tevékenység során megismert, keletkezett és rögzített adatok a mindennapos gyógyító-megelőző, egészségfejlesztő, egészségmegőrző és páciens edukáció eredményes folytatását szolgálják. A tevékenység körébe tartoznak az akutan keletkező panaszok ellátásán kívül a korcsoportfüggő szűrővizsgálatok, amely kapcsán a tágabb családi anamnézis megismerése is szükséges lehet, így a közvetlen betegre vonatkozó adatokon kívül családi környezete adatait is rögzítenünk, tárolnunk kellhet.

A magunk észlelte tényekből, vizsgálati eredményekből származó adatokon túlmenően harmadik féltől kapunk adatokat a biztosított viszony érvényességéről, ami érdekében a betegspecifikus TAJ számot ellenőriznünk kell. Ez elektronikusan történik. A betegeinkről keletkezett, észlelt, mért és anamnézis útján nyert adatokat jogszabályi kötelezettség alapján, az érvényben lévő Egészségügyi Törvény előírásai szerint végezzük.

Az eddigi gyakorlatban nemigen fordult elő, hogy betegeink a róluk tárolt adataikba betekinteni óhajtottak volna, és esetlegesen feleslegesnek vélt adataik törlését sem kezdeményezték. Valószínűsíthető, hogy az orvos-beteg kapcsolat bizalmi jellege biztonságot jelent számukra.

1.1.2. Az információs rendszer és követelményei. (7.3.1.2.)

Élve azzal a lehetőséggel, hogy a tanulmányt specializálni kell az adott szervezet sajátosságaira, így az orvosi praxisra vonatkoztatva az információs rendszerről röviden a következő foglalható össze. Belső hálózatban

összekapcsolt számítógépeket használunk, amelyhez szkennert, printer csatlakozik, van internet elérése, ami kötelező is, a NEAK-kal való on-line kapcsolattartás, valamint az EESZT használatának előírásai miatt.

A lehető legnagyobb mértékben törekszünk rá, hogy a számítógépeink biztonságosak legyenek. Ezért például célszerű az adattárolásra használt gépen kerülni a magán jellegű internethasználatot.

Az elektronikus adattárolás mellett papír alapú adattárolás az előző 3 éves időszakhoz képest is, lényegesen csökkent mértékben van már csak jelen.

1.1.3. A praxis adatkezelési folyamat (workflow) ábrája.

A praxisunkban működő eszközökről, az adatok tárolása módozatairól, a biztonságra törekedésről, a hozzáférés szabályozottságáról, harmadik fél felé történő adattovábbításról, a betegek és hozzátartozóik tájékoztatásának módjáról a következő oldalon megfogalmazott, ábrába foglalt adatkezelési munkamenet folyamata ad átlátható, egyértelmű képet. Ennek értelmezését szöveges magyarázatunkkal is elősegítjük.

1.1.4. Checklista. (Kérdőív)

A hatástanulmány végén közöljük azt a checklistát, aminek a vizsgált praxis vezetője általi kitöltése, megválaszolása szolgáltatta az alapját a hatástanulmány elkészítésének. A checklista kiegészül az adatvédelmi kockázat vélelmezett súlyossági fokának és bekövetkezése mérlegelt valószínűségének számszerű meghatározásával és e kettő értékből az adatvédelmi kockázati matrix inputját adó, cselekvést meghatározó konkrét számértékeket tartalmazó bekezdéssel.

A Fedlapon azonosított praxis/vállalkozás adatkezelési folyamata a GDPR előírásai szerint

Adatkezelésre jogosultak				
	Dr. Domány Eszter orvos	Ács Tímea asszisztens	Dr. Domány Eszter adatvédelmi megbízott	Jelmagyarázat: színek jelentése
Tevékenység megnevezése				
Új adatok felvétele	↑			Saját tevékenység Eü. tv., jogszabályi előírás szerint
Meglévő adatok frissítése, kiegészítése	↑	↑		
Az adatok tárolása (elektronikusan és papír alapon)	↑	↑		Az érintett kérésére történő adat változtatás
Adatok módosítása az érintett kérésére			↑	↑
Adatok továbbítása 3. fél felé	NEAK, Kormányhivatal		↑	Kötelező, illetve kötelező szerződés szerint
	Könyvelő	↑		↑
	tudományos munka statisztikai elemzések hozzátartozók		↑	Az orvos szabad döntésén alapuló magán szerződés szerint
	Javaslat a törlésre		↑	↑
Adatok törlése	Javaslat jóváhagyása	↑		Csak az érintettek előzetes írásbeli hozzájárulása alapján
	Törlés végrehajtása		↑	↑

1.1.5. A Praxis adatkezelési folyamatának szöveges magyarázata.

1.1.5.1. Formai tényezők:

Fentről lefelé haladva a tevékenységek időbeli sorrendjét lehető mértékig követve egy újonnan keletkezett adat életciklusát követjük végig az időről időre, a vizsgálatok során történő frissítésen, módosításon, az esetleg beteg által kezdeményezett módosításon, harmadik felek felé történő adattovábbításon keresztül egészen az adat feleslegessé válása miatt végrehajtandó törléséig.

Balról jobbra haladva az adatkezelésben, az adatkezelés ellenőrzésében, az adatok továbbításában szerepet játszó, illetve abban résztvevő személyek, tisztségviselők követik egymást az alapvető tevékenységet meghatározó orvostól, az asszisztensen és az adatfeldolgozást is végző adatvédelmi megbízottna át a 3. fél képviselőjéig.

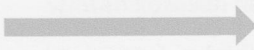
Az alkalmazott színek üzenete, értelmezése:



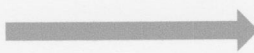
Világoskék: a saját kezdeményezésű mindennapos tevékenység közben felmerülő és végrehajtott adatrögzítés, adatkezelés jelzésére.



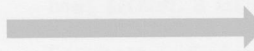
Narancssárga: külső kérésre történő beavatkozás az adatok tartalmába illetve tárolásába.



Zöld: jogszabály által előírt kötelező adattovábbítás, amely adatok biztonságáért a jogszabályi kötelezettségben megjelölt 3. fél köteles a GDPR-nak való megfeleléséért garanciát vállalni.



Lila: a praxis saját kezdeményezése nyomán szabadon kötött szerződés szerinti adattovábbítás



Piros: mindazon adattovábbítások jelzésére, amelyek esetében minden egyes érintett féltől előzetes írásbeli hozzájárulást kell beszerezni. Ebbe a kategóriába tartozik a külső körülményből fakadó, vagy külső kérésre történő adattörlés végrehajtása is.

1.1.5.2. Tartalmi tényezők:

Új adat felvétele új beteg jelentkezése esetén, orvos által végrehajtva, asszisztensi köreműködéssel.

Meglévő adat frissítése, amikor ismételtén jelenik meg a beteg vagy újabb panasszal, vagy kontrollra

Adatok továbbítása 3. fél felé. Kötelezően: NEAK, olykor Kormányhivatal felé, jogszabályi kötelezettség alapján. A könyvelő felé a praxis, mint cég saját kezdeményezésére, statisztikai felmérés, tudományos munka érdekében csak minden egyes beteg előzetes írásbeli hozzájárulása után.

Adatok törlése a beteg más háziorvoshoz kerülése, elköltözése, vagy halála miatt, csak az orvos tudtával és beleegyezésével történhet.

2. Adatkezelési – adatvédelmi kockázatok. (7.4.)

2.1. A kockázatok azonosítása.

Az adatvédelmi hatástanulmány elkészítéséhez meg kell határoznunk a kockázatok kritériumait, keletkezésük lehetséges helyeit. Mindezt egyeztetni kell a „vizsgálat alatt álló szervezet”, képviselőjével, tehát jelen esetben a praxist vezető orvossal. Cél, hogy Vele egyetértésben az adott praxis minden körülményét figyelembe véve váljék véglegessé a vizsgált tényezők, mint adatvédelmi veszélyforrások listája.

Ennek a listának a tartalma alapulhat az ISO/IEC 29134:2017 szabványban közölt minta felhasználásán, de ettől teljesen függetlenül is összeállítható a hatásvizsgálatot végző szakember és a vizsgált praxis vezetője által közösen. Bele kell értenünk ebbe annak a meghatározását is, hogy a listába felvett veszélyforrásokból támadható adatkezelési-adatvédelmi kockázat –bekövetkezése esetén– milyen mértékű káros hatást fejthetne ki, illetve annak a meghatározását is, hogy egy ilyen esemény bekövetkeztének mekkora a valószínűsége.

Szintén közösen határozandó meg az úgynevezett „maradék kockázat”, vagyis az elviselhető következményű kockázatok mértékének a meghatározása.

A kritériumokat úgy kell meghatározni, hogy azok összessége egyértelműen tükrözzék az adott szervezet, jelen esetben az orvosi praxis működésének céljait, feladatait, működési körülményeit, külső és belső feltételeit. Emellett figyelembe kell venni a praxis fizikai, felszereltségi és humán erőforrás adottságait, törvényi és más jogszabályi kötelezettségeit.

Más szóval: a GDPR bárkire, bármekkora létszámú és kiterjedésű, bárhol Európában működő szervezetre készített előírásai, javasolt lista tartalmi olyan módon fókuszálандók, tehát szűkítendő a jelen hatástanulmány által célzott orvosi praxis körülményeire, hogy a listába felvett kritériumok, tételek mindegyike egyértelműen összefüggésbe hozható legyen a praxis gyógyító-megelőző, egészségfejlesztő, egészségmegőrző és egészségnevelő, páciens edukációs funkcióival.

Éppen ezért, egyetlen tényező sem vizsgálendő, amely nem ezen célokkal, tevékenységekkel kapcsolatos adatvédelmi kérdésre utalna.

Ezen, listába felvett vizsgálendő kritériumok használhatók fel a tényleges adatvédelmi kockázatok megítéléséhez, elemzéséhez és egyben a kockázatok kezelésének, megoldásának kialakítására is.

2.2. Konzultáció az érintett felekkel.

Mind a lista tartalmának összeállítása, az érintettekhez történő eljuttatása érdekében a praxis vezetőivel kapcsolatot kell tartani. Ez döntő mértékben elektronikusan történik bizonyos, meghatározott részeiben postai úton. A hatástanulmány elkészülte után annak jóváhagyása és a módosító javaslatok elfogadása/elvetése/más megoldások beállítása szintén az érintett felekkel való konzultáció eredménye, ami alapján a végleges Adatkezelési Szabályzat elkészíthető.

3. Az adatvédelmi kockázatok elemzése, számszerűsítése. (7.5.)

A kockázatértékelés számszerű értékeinek jelentése

A kockázatból eredő károsodás bekövetkezésének valószínűsége:

- 1: valószínűtlen, szinte kizárható, rendkívüli események fellépése nélkül biztosan nem
- 2: csekély, az esetek kis százalékában történhet meg
- 3: valószínűleg bekövetkezik, ha nem tesszük meg a megelőző intézkedéseket
- 4: gyakori, csaknem biztosra vehető, hogy bekövetkezik

A kockázatból eredő károsodás súlyosságának a mértéke:

- 1: elhanyagolható
- 2: jelentős
- 3: kritikus
- 4: katasztrofális

Kockázati matrix

A fentiek értelmében tehát minden adatvédelmi veszélyeztetéshez hozzárendelhető egy bizonyos kockázat, amely függ az esemény bekövetkezésének a valószínűségétől és az esemény következményeinek súlyosságától. A kockázat eszerint valamely adott veszélyes esemény előfordulása valószínűségének vagy gyakoriságának, valamint a következmény súlyosságának kombinációja, legkézenfekvőbb ha a két tényező szorzatával értékelünk. (Az értékelés módját a GDPR is és az erre szolgáló fent már többször idézett ISO 29134:2017 szabvány is a vizsgált szervezet szabad döntésére bízta!)

Magyarul a matrix egy olyan táblázatos megjelenítés, amelyben az egyik oldalon a vizsgálandó kockázat bekövetkezésének a VALÓSZÍNŰSÉGE, a másik, erre merőleges oldalon a SÚLYOSSÁG fenti 1-4-ig kapott számértékei szerepelnek. Az értékelés a két elem metszéspontjában, a vonatkozó két szám szorzataként olvasható le.

Hogy be kell-e avatkozni, az ezen számértékektől (=szorzatoktól) függ, ám annak meghatározása szubjektív elhatározás és döntés eredménye kell, hogy legyen.

Kockázatértékelő matrix		Az adatvédelmi kockázati esemény bekövetkezésének valószínűsége			
		1 valószínűtlen	2 csekély	3 valószínűleg bekövetkezik	4 csaknem biztos
Az adatvédelmi kockázati következmények súlyossága	1 elhanyagolható	1	2	3	4
	2 jelentős	2	4	6	8
	3 kritikus	3	6	9	12
	4 katasztrofális	4	8	12	16

A fentiekben alkalmazott értékek és a hozzájuk rendelt értelmezés alapján a következő beavatkozási szintek határozhatók meg, javaslati szinten:

- 1-4: semmi teendő nincs
- 5-6: illik betervezni változtatást a soron következő alkalommal, amikor a rendszerhez amúgyis hozzányúlnánk, aktualizálnánk
- 7-8: a legrövidebb időn belül cselekedni kell, a megfogalmazott megoldási lehetőségek szerint
- 9-16: azonnal be kell avatkozni, a legszigorúbban végrehajtva a megfogalmazott és rögzített megoldási lehetőségek valamelyikét vagy valamennyit

Egész számok alkalmazása esetén 1, 2, 3, 4, 6, 8, 9, 12 és 16-os érték adódik. Annak, hogy az értékelésben mégis 5-6, 7-8, 9-16 szerepel, az az oka és értelme, hogy ki-ki meghatározhat a veszélyek megítélésnek finomításában nem egész számokat is, tehát lehet nem 2-es, hanem 2,5-ös, vagy bármely más nem egész szám 1-4 között.

4. Adatvédelmi kockázatkezelési terv készítése, elképzelések megfogalmazása. (7.6.)

Az eddigiek után egyszerű, egyértelmű a helyzet: kezelni kell valamennyi kockázatot, amely a sárga vagy piros mezőbe esik, illetve amelynek az értékelésben kapott számértéke 5-nél több. Azonnali, sürgős beavatkozást kíván a piros mezőbe eső, 9 vagy afölötti számértékű kockázat. Mielőbbi megoldást kell keresni a sárga mezőbe eső, 6-8 értékű kockázatokra. A 4-5 közötti zöld-sárga mezőbe eső kockázatokra az amúgyis soron következő változtatások, fejlesztések során kell gondolni a tervezés szakában.

5. Következtetések és elhatározások, megfontolandó változtatási lehetőségek összefoglalása. (7.7.)

A következő oldalakon található, a praxisok vezetői által kitöltött „Lista(2)”, a Fedlapon azonosított praxisra vonatkozó, konkrét adatai alapján készült kockázatelemzés, kockázatbecslés és kockázat értékelés található, a fenti, 4-es pontban meghatározott értékelési, illetve besorolási számok alkalmazásával. A jobb szélső oszlopban találhatóak az egyes kockázatok megoldására tett javaslatok.

Alapvetően a 4-nél nagyobb összérték esetén kell beavatkozni. Cél az, hogy a 4-nél nagyobb értékű kockázatok kezelésére olyan módot tudjunk találni, amelyek alkalmazásával a kockázat értéke 4-re, vagy az alá csökkenthető. Ez az úgynevezett „maradék kockázat”, más néven elviselhető kockázat mértéke. A módosító megoldás természetesen javaslat, amit a praxis vezetőjének kell elfogadnia-elvetnie-más megoldást javasolni helyette.

6. Az adatkezelésben érintett személyek összefoglaló, nyilvános tájékoztatása. (7.8)

Ennek a GDPR, illetve ISO szabvány előírásnak két úton is megfelelnünk az orvosi praxis és speciális beteg („ügyfél”) körből fakadó sajátosságokat szem előtt tartva. Egyrészt a következő oldali, az adott praxisra vonatkozó részletes elemzést és javaslatot átadjuk teljes egészében az érintett fél, tehát a praxis vezetőjének, másrészt a rendelő várószobájában kifüggesztik az adatvédelmi hatástanulmány eredményét summázva összefoglaló Adatkezelési Tájékoztatót.

Amelyik praxis már rendelkezik saját honlappal, mindkét dokumentumot a honlapon is elhelyezheti, de tekintettel arra, hogy az érintettek tömegesen nem a honlappal vannak kapcsolatban, ezért célszerű a rendelőben is kihelyezni.

S O R S Z Á M	ADATKEZELÉSI KOCKÁZAT/VESZÉLY AZONOSÍTÁSA	JELENLEGI GYAKORLA T	S Ú L Y O S S Á G	V A L Ó S Z Í N Ű S É G	É R T É K	MEGOLDÁSI JAVASLAT
1	Mennyire teljesül, hogy csak a legsükségesebb adatokat tárolja?	teljesül	1	2	2	Ebben a kérdésben nincs teendő
2	Kapnak-e tájékoztatást az érintettek, hogy adataikat hogyan tároljuk, ki férhet hozzá?	igen	1	2	2	Ebben a kérdésben nincs teendő. A végleges, kifüggeszthető Adatkezelési Tájékoztató az Adatkezelési Szabályzat mellett, külön megtalálható majd a küldeményben.
3	Megoldott-e, hogy az érintettek (betegek, páciensek, hozzátartozók) betekinthessenek a róluk tárolt adatokba?	igen	3	3	9	Ebben megfelelünk a GDPR-nak, de készítsünk pontos szabályozást a mikéntjéről, amit az érintettek megismerhetnek.
4	Megoldott-e, hogy az érintettek (a praxist működtető, mint munkáltató alkalmazottai) betekinthessenek a róluk tárolt adatokba?	igen	3	3	9	Ebben megfelelünk a GDPR-nak, de készítsünk pontos szabályozást a mikéntjéről, amit az érintettek megismerhetnek.
5	Adattovábbítás a NEAK felé	igen	3	2	6	Rögzítsük saját magunk számára az adattovábbítás mikéntjét, akkor is, ha jogszabály írja elő. Ez a saját dokumentumunk a MIR könyvünk részét képezheti a folyamatok között.
6		szabályozva van	3	1	3	Ebben a kérdésben nincs teendő.
7	Adattovábbítás a Kormányhivatal, (a Kormányhivatal Népegészségügyi szakigazgatási szerve) felé	igen	3	2	6	Rögzítsük saját magunk számára az adattovábbítás mikéntjét Ez a saját dokumentumunk a MIR könyvünk részét képezheti majd a folyamatok között.
8		szabályozva van	3	1	3	Ebben a kérdésben nincs teendő.
9	Adattovábbítás a Gyámügy felé	nem történik	1	1	1	Ha a jövőben mégis sor kerülne rá, akkor rögzítsük saját magunk számára az adattovábbítás rendjét és küldjük meg majdan a 3. félnek tájékoztatásul.
10						
11	Adattovábbítás az Önkormányzat felé	nem történik	1	1	1	Ha a jövőben mégis sor kerülne rá, akkor rögzítsük saját magunk számára az adattovábbítás rendjét és küldjük meg majdan a 3. félnek tájékoztatásul.
12						

S O R S Z Á M	ADATKEZELÉSI KOCKÁZAT/VESZÉLY AZONOSÍTÁSA	JELLENLEGI GYAKORLA T	S Ú L Y O S S Á G	V A L Ó S Z Í N Ü S É G	É R T É K	MEGOLDÁSI JAVASLAT
23	Adattovábbítás statisztikai célokra	igen történik	3	3	9	Rögzítsük saját magunk számára az adattovábbítás mikéntjét, akkor is, ha jogszabály írja elő. Ez a saját dokumentumunk a MIR könyvünk részét képezheti a folyamatok között.
24		Szabályozva van	3	1	3	Ebben a kérdésben nincs teendő.
25	Adatfelhasználás, illetve adat továbbítás tudományos tevékenység céljaira, vagy saját feldolgozás tudományos munka keretében	igen történik	3	3	9	Rögzítsük saját magunk számára az adattovábbítás mikéntjét. Ez a saját dokumentumunk a MIR könyvünk részét képezheti majd a folyamatok között.
26		Szabályozva van	3	1	3	Ebben a kérdésben nincs teendő.
27	Adattovábbítás hozzátartozók felé	igen történik	4	3	12	Rögzítsük saját magunk számára az adattovábbítás mikéntjét, akkor is, ha jogszabály írja elő. Ez a saját dokumentumunk a MIR könyvünk részét képezheti a folyamatok között.
28		Szabályozva van	3	1	3	Ebben a kérdésben nincs teendő.
29	Tudja-e biztosítani, hogy a beteg korlátozhassa a rá vonatkozó adatok kezelését?	biztosítva van	4	1	4	Ebben a kérdésben nincs teendő.
20	Megoldott-e a már nem érvényes adatok törlésének a kivitelezése?	meg van oldva	2	1	2	Ebben a kérdésben nincs teendő.
21	Az EESZT-hez történt csatlakozás és adatkezelés biztonsága megoldott-e?	igen	4	1	4	Ebben a kérdésben nincs teendő.
22	Csoportos egészség-felvilágosítás a betegek, hozzátartozók számára. Páciens edukáció.	nem	1	1	1	Kockázat szempontjából ugyan nincs teendő, de más szempontból megfontolandó a tevékenység megszervezése.
23	Mennyire tudja megoldani, hogy csoportos egészség-felvilágosítás során egymás adatai ne váljanak nyilvánossá a beteg társak között?					
24	Az informatikus rendszergazda karbantartás közben beletekinthet-e az adatokba?	igen	4	2	8	A szerződésében garanciát kell kikötni, hogy az általa látott adatokat nem használja fel semmilyen célra.
25	Ha igen, a vele kötött szerződésben van-e titoktartási kötelezettség előírva?	van	4	1	4	Ebben a kérdésben nincs teendő.

S O R S Z Á M	ADATKEZELÉSI KOCKÁZAT/VESZÉLY AZONOSÍTÁSA		JELLENLEGI GYAKORLA T	S Ú L Y O S S Á G	V A L Ó S Z Í N Ű S É G	É R T É K	MEGOLDÁSI JAVASLAT
26	A praxisban tárolt páciens adatok pontossága: mennyire pontosak		nagyon pontosak	1	2	2	Ebben a kérdésben nincs teendő.
27	A praxisban tárolt páciens adatok mennyire naprakészek?		teljesen naprakészek	1	2	2	Ebben a kérdésben nincs teendő.
28	Adattárolás számítógépen	életkora alapján	A készülék kiszolgált	3	3	9	Pendrive-ra, külső tárolóra végezzünk rendszeres biztonsági mentéseket. Tervezzük be a számítógép cseréjét a következő lehetséges alkalomra.
29		Jelszóval védett-e?	igen	3	1	3	Ebben a kérdésben nincs teendő.
30		fizikai védelem megoldott	igen	3	1	3	Ebben a kérdésben nincs teendő.
31	Adattárolás laptopon	életkora alapján	A készülék előregedőben	3	2	6	Pendrive-ra, külső tárolóra végezzünk időszakos biztonsági mentéseket.
32		Jelszóval védett-e?	igen	3	1	3	Ebben a kérdésben nincs teendő.
33		fizikai védelem megoldott-e	igen	3	1	3	Ebben a kérdésben nincs teendő.
34	Adattárolás tableten	életkora alapján	jelenleg nincs, ezért „0” évesnek tekintendő	4	1	4	Ha a jövőben esetleg majd alkalmazzuk, akkor 3 évente megújítjuk, jelszóval védjük és megoldjuk a fizikai védelmét is, megszabjuk, hogy ki férhet az eszközhöz és ki ismerheti a jelszót
35		Jelszóval védett-e?	nem adható reális válasz	4	1	4	
36		fizikai védelem megoldott-e	nem adható reális válasz	4	1	4	
37	Adattárolás pendriven	életkora alapján	A készülék előregedőben	3	2	6	Vegyünk új pendrive-ot és védjük jelszóval. Legjobb, ha eleve jelszóval védett típust szerzünk be.

S O R S Z Á M	ADATKEZELÉSI KOCKÁZAT/VESZÉLY AZONOSÍTÁSA		JELENL GI GYAKORLA T	S Ú L Y O S S Á G	V A L Ó S Z Í N Ű S É G	É R T É K	MEGOLDÁSI JAVASLAT
38		Jelszóval védett-e?	igen	3	1	3	Ebben a kérdésben nincs teendő.
39		fizikai védelem megoldott	igen	3	1	3	Ebben a kérdésben nincs teendő.
40	Adattárolás okostelefonon	életkora alapján	jelenleg nincs, ezért „0” évesnek tekintendő	4	1	4	Ha a jövőben esetleg majd alkalmazzuk, akkor 3 évente megújítjuk, jelszóval védjük és megoldjuk a fizikai védelmét is, megszabjuk, hogy ki férhet az eszközhöz és ki ismerheti a jelszót
41		Jelszóval védett-e?	nem adható reális válasz	4	1	4	
42		fizikai védelem megoldott-e	nem adható reális válasz	4	1	4	
43	Szabályozva van-e (írásban is!), hogy a jelszavas védelmet ki ismerheti, ki kezeli, ki módosítja?		nem	3	2	6	Rögzítsük írásba, és az adott személlyel írassuk alá, az így keletkezett saját dokumentumot az Adatkezelési Szabályzathoz becsatolhatjuk.
44	Meghibásodás esetére a tárolt adatok védelmének megoldása	nincs					
45		Felhő					
46		Külső adattároló	Külső adattároló	3	2	6	Figyelni kell a tároló életkorára, időnként második biztonsági mentésről gondoskodjunk.
47		Pendrive vagy egyéb más					
48	Papír alapú adattárolás során hol tárolja az adatokat tartalmazó dokumentumokat?		szabad polcon	4	4	1 6	A lehető legrövidebb időn belül zárható szekrénybe kell áthelyezni az iratokat.
49	Szabályozva van-e, hogy a dokumentumok zárt tárolójának a kulcsa kinél van, ki férhet hozzá?		nem	3	2	6	A kulcshoz hozzáférést írásban szabályozni szükséges, az így keletkezett saját dokumentumot az Adatkezelési Szabályzathoz csatolhatjuk.
50	Külső szolgáltatókkal kötött, érvényben lévő szerződésekben szerepel-e garancia vállalásuk arra nézve, hogy ők, mint partnerek a GDPR előírásai szerint végzik tevékenységüket?		részben	3	2	6	Korrigálni kell a szerződést olyan értelemben, hogy szerepeljen benne garanciavállalásként a GDPR általa történő megtartása