PÁNMED
magánklinika

Egészségügyi és Szolgáltató Betéti Társaság

ÁNTSZ eng. szám:
45688/2/08-09/2008

Telefon: 06-1-2151-898
Postacím: 1461 Budapest, Postafiók 3.
E-mail: panmed@panmed.t-online.hu,
Honlap: www.panmed.hu

Adatvédelmi és Adatkezelési Szabályzat

TARTALOM

1. BEVEZETŐ

A PÁNMED Egészségügyi és Szolgáltató Betéti Társaság (1093 Budapest, Lónyay u. 24.. továbbiakban, mint Vállalkozás, Adatkezelő) mint **Adatkezelő**, magára nézve kötelezőnek ismeri el jelen jogi szabályzat tartalmát. Kötelezettséget vállal arra, hogy tevékenységével kapcsolatos minden adatkezelés megfelel a jelen szabályzatban és a hatályos nemzeti jogszabályokban, valamint az Európai Unió aktusaiban meghatározott elvárásoknak.
Az Adatkezelő elkötelezett ügyfelei és partnerei személyes adatainak védelmében és kiemelten fontosnak tartja ügyfelei és munkatársai információs önrendelkezési jogainak tiszteletben tartását. Az adatkezelő a személyes adatokat bizalmasan kezeli és megtesz minden olyan biztonsági, technikai és szervezési intézkedést, mely az adatok biztonságát garantálja.
Az Adatkezelő kijelenti, hogy a személyes adatok kezelése során az alábbi szabályokat mindenképpen betartja:

- A személyes adatok kezelését jogszerű és átlátható módon kell végezni, biztosítva a személyeknek a rájuk vonatkozó személyes adatok kezelésének tisztességességét és a kezelés átláthatóságát.
- A személyes adatkezelésnek konkrét célja kell, hogy legyen, és ezt már az adatok gyűjtésének időpontjában közölnünk kell az érintettel.
- Az Adatkezelő soha nem gyűjt személyes adatokat célhoz kötöttség nélkül.
- Az Adatkezelő. kizárólag olyan személyes adatokat gyűjthet és kezelhet, amelyek a cél eléréséhez szükségesek.
- Az Adatkezelő működése során biztosítania kell, hogy a személyes adatok pontosak és naprakészek legyenek, szem előtt tartva, hogy a pontatlan személyes adatokat kijavítsák.
- Biztosítania kell továbbá, hogy a személyes adatokat kizárólag az adatkezelés céljainak eléréséhez szükséges ideig tárolják.
- A személyes adatok kezelését az adatkezelőnek olyan módon kell elvégeznie, hogy a technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, ideértve az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is.

Az Adatkezelő a fenti célok eléréséhez szükséges alábbi tevékenységek elvégzését írásbeli dokumentumokkal támasztja alá:

- már az üzleti tervekben figyelembe vette az adatvédelem szabályait (beépített és alapértelmezett adatvédelem)
- a GDPR szabályainak megfelelően tevékenykedő adatfeldolgozót bízott meg,
- az adatkezelési nyilvántartásai naprakészek,
- megtett minden szükséges adatbiztonsági intézkedést,
- az incidenseket megelőző intézkedéseket megtette, és az adatsértéseket azonnal kezelni tudná (van rá technológia és eljárási rend is),
- adatvédelmi tisztviselőt nevezett ki.

Az Adatkezelő az alábbiakban ismerteti adatkezelési gyakorlatát.

2. AZ ADATKEZELŐ ADATAI

2.1. AZ ADATKEZELŐ

Név: **PÁNMED Egészségügyi és Szolgáltató Betéti Társaság**
Székhely: 1093 Budapest, Lónyay u. 24.
Cégjegyzékszám: 01-06-712012
A bejegyző bíróság megnevezése: Fővárosi Cégbíróság
Adószám: 29121878-2-43

2.2. AZ ADATVÉDELMI TISZTVISELŐ

A Vállalkozás adatvédelmi tisztviselőt nem alkalmaz.

3. A SZEMÉLYES ADATOK KÖRE

Az Adatkezelő. tevékenységének adatkezelése önkéntes hozzájáruláson, illetve törvényi felhatalmazáson alapul.

- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, GDPR)
- 2011. évi CXII. törvény- az információs önrendelkezési jogról és az információszabadságról (Infotv.)
- 2013. évi V. törvény - a Polgári Törvénykönyvről (Ptk.)
- 2000. évi C. törvény – a számvitelről (Számv. tv.)
- 2007. évi CXXXVI. törvény- a pénzmosás és terrorizmus finanszírozása megelőzéséről és megakadályozásáról (Pmtv.)
- 2017. évi CL törvény – az adózás rendjéről (Adótv.)
- 1995. évi CXIX. törvény – a név és lakcímadatokról
- 1997. évi CLIV. törvény- az egészségügyről
- 1997. évi XLVII. törvény - az eü.-i személyes adatokról
- 2017. évi LIX. törvény – az EESZT-ről
- 33/1998. (VI. 24.) NM rendelet
- a munkaköri, szakmai, illetve személyi higiénés alkalmasság orvosi vizsgálatáról és véleményezéséről

3.1 A KEZELT ADATOK KÖRE

3.1.1 EGÉSZSÉGÜGYI TEVÉKENYSÉG SORÁN

Az Adatkezelő járóbeteg-ellátás és oktatási tevékenységeket végez.

A társaság kizárólag akkor kezelhet különleges adatokat, ha fennáll az alábbi feltételek egyike:

- megkapta az érintett magánszemély kifejezett hozzájárulását;
- uniós vagy magyar jog, vagy kollektív megállapodás értelmében a vállalkozásnak kötelessége az adatkezelés elvégzése;
- az adatkezelés az érintett személy létfontosságú érdekeinek a védelme miatt szükséges, vagy az érintett személy fizikailag vagy jogilag képtelen a hozzájárulás megadására,
- az adatkezelés olyan személyes adatokra vonatkozik, amelyet az érintett személy kifejezetten nyilvánosságra hozott;
- az adatkezelés jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez szükséges;
- az adatkezelés jelentős közérdek miatt szükséges, uniós jog vagy magyar jog alapján;
- az adatkezelés a következő célokból történik: megelőző egészségügyi vagy munkaegészségügyi cél, munkavállaló munkavégzésének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy magyar jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében;
- az adatkezelés a népegészségügy területét érintő közérdekből szükséges, uniós vagy magyar jog alapján;
- az adatkezelő valamely politikai, világnézeti, vallási vagy szakszervezeti célú alapítvány, egyesület vagy bármely más nonprofit szervezet, az adatkezelés pedig az ilyen szerv jelenlegi vagy volt tagjaira, vagy a szervezettel rendszeres kapcsolatban álló személyekre vonatkozik;
- az adatkezelés archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból szükséges uniós vagy magyar jog alapján.

Az Adatkezelő – kivételekkel- csak akkor kezeli egy gyermek személyes adatait, ha rendelkezik a gyermek törvényes képviselőjének a kifejezett írásbeli hozzájárulásával.
Az adatkezelés célja: általános járóbeteg - ellátás tevékenység szerződésen alapuló teljesítése, végrehajtása, a szerződés alapján vállalt szolgáltatás nyújtása, a szerződéssel kapcsolatos kötelezettségek és jogosultságok igazolása, kötelező statisztikai feladatok ellátása, kapcsolattartás, az igénybe vett szolgáltatások nyomon követése.
Az adatkezelés jogalapja: jogi kötelezettség teljesítése és létfontosságú érdek GDPR 9. cikk (2) bekezdés 4) pont, és az érintett önkéntes hozzájárulása, GDPR 6. cikk (1) bek. b) pont.
A kezelt adatok köre: azonosítószám, név, születési név, születési hely, idő, cím, egészségügyi adatok, genetikai adatok. Valamint, levelezési cím, telefonszám, e-mail cím.
Az adatok törlésének határideje egészségügyi adatok tekintetében 50 év minden más adat tekintetében a Számv. tv. és az Adótv. szabályai alapján megfelelő 7 év.

Az adatrögzítők (az orvosi vizsgálatot végzők orvosok és ápolók, valamint az oktatás szervezésében résztvevő munkatársak) a név, lakcím, születési hely, születési idő, anyja neve, TAJ szám, törzsadatok, egészségügyi, munkakörre és egyéb másra vonatkozó adatokat veszik fel.

Adatkezelő
Adatkezelő feladata:
Az adatkezelő a keletkezett személyes adatokra vonatkozó szabályozást betartatja az adatrögzítőkkel és a rögzítés folyamatába bármikor betekinthet.
Adatkezelő neve: Pánovics Balázs
Adatkezelő időtartama: folyamatos

Adatfeldolgozó: azonosítószám, név, születési név, születési hely, idő, cím, állampolgárság, TAJ szám, adószám, személyi adóazonosító, cégjegyzékszám, székhely, anyanyelv. Valamint, levelezési cím, telefonszám, e-mail cím, a Nemzeti Adó és Vámhivatal felé az ügyfélkapu/ gov.hu titkosított felületen az ügyfél saját ügyfélkapu azonosító számával, az ügyfél saját Ügyfélkapu felületéről.
Az adattovábbítás jogalapja: szerződés érdekében; jogi kötelezettség teljesítése, és az érintett önkéntes hozzájárulása.
Adatfeldolgozó neve: Tóth Katalin
Az Adatkezelő és az adatfeldolgozó által kötött vállalkozói szerződésekben a következő pontok kötelező jelleggel szerepelnek:

- a személyes adatok kezelése kizárólag az adatkezelő írásbeli utasításai alapján történik majd,
- az adatfeldolgozó biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek, titoktartási kötelezettséget vállalnak, vagy más jogszabály miatt már ilyen titoktartási kötelezettség alá esnek,
- az adatfeldolgozó biztosítja az adatkezelő által meghatározott minimális biztonsági szintet,
- az adatfeldolgozónak segítenie kell az adatkezelőt a GDPR rendeletnek való megfelelésben.

Az adatszolgáltatás elmaradásának lehetséges következményei: adóeljárás indulása és adóbírság.

3.1.2 EGYÉB ADATKEZELÉS

Jelen szabályzatban fel nem sorolt, újonnan keletkező adatkategória kezeléséről az adat felvételekor tájékoztatást adunk.
Tájékoztatjuk az ügyfeleinket, hogy a bíróság, az ügyész, a nyomozó hatóság, a szabálysértési hatóság, a közigazgatási hatóság, a Nemzeti Adatvédelmi és Információszabadság Hatóság, illetőleg jogszabály felhatalmazása alapján más szervek tájékoztatás adása, adatok közlése, átadása, illetőleg iratok rendelkezésre bocsátása végett megkereshetik az adatkezelőt.

Az Adatkezelő a hatóságok részére – amennyiben a hatóság a pontos célt és az adatok körét megjelölte – személyes adatot csak annyit és olyan mértékben ad ki, amely a megkeresés céljának megvalósításához elengedhetetlenül szükséges.

3.1.3 AZ ÉRINTETT HOZZÁJÁRULÁSÁN ALAPULÓ ADATKEZELÉS

Az Adatkezelő. hozzájáruláson alapuló adatkezelés esetén, csak akkor kezel személyes adatokat, ha a hozzájárulás önkéntes alapon, tájékoztatáson alapul, konkrét célt szolgál, az adatkezelés minden okát világosan meghatározva, explicit és pozitív művelet eredménye.
A hozzájárulás előtt az érintettek minden esetben, egyértelmű és egyszerű nyelvezetű, jól látható, visszavonható és a hozzájárulás visszavonásának lehetőségét elmagyarázó írásbeli tájékoztatót kapnak és írnak alá. A tájékoztatás mindig tömör, érthető és könnyen hozzáférhető formában, világos nyelven és mindenki számára közérthetően megfogalmazva kerül megadásra.
A tájékoztatónak az alábbi pontokat kötelezően tartalmaznia kell:

- az adatkezelő, és az adatvédelmi tisztviselő elérhetősége;
- meg kell jelölni milyen célból, gyűjtjük az adatokat;
- meg kell jelölni az adatok kategóriáit;
- meg kell jelölni az adatkezelés jogalapját;
- ha más adatkezelő is megkaphatja az adatokat, ezt is közölni kell;
- továbbítjuk-e az EU-n kívülre az adatokat;
- tájékoztatást kap az érintett arról, hogy megkaphatja a gyűjtött adatokat, mert ehhez hozzáférési joga van;
- tájékoztatni kell az adatvédelmi jogairól;
- tájékoztatni kell, hogy joga van panaszt benyújtani az adatvédelmi hatósághoz;
- tájékoztatni kell, hogy bármikor joga van visszavonni a hozzájárulását;
- tájékoztatni kell az automatizált adatkezelésen alapuló döntéshozatal létezéséről, annak logikájáról és annak következményeiről;
- végül tájékoztatni a hozzájárulás megtagadásának következményeiről.

A tájékoztatásnak díjmentesnek kell lennie.

4.AZ ADATKEZELÉS JOGALAPJAI

A jogszerű adatkezelés feltétele, hogy a személyes adatok kezelése rendelkezzen GDPR-ban szabályozott valamely jogalappal.

4.1. HOZZÁJÁRULÁS

A hozzájárulás az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló egyértelmű kinyilatkoztatása. Az önkéntesség fogalmilag, valódi választási lehetőséget biztosít az érintettnek. Így nem értelmezhető a hozzájárulás megadásának megtagadása együtt jár valamely szolgáltatásból történő kizárással, tehát negatív következménye van. A hozzájáruláson alapuló adatkezelés nem értelmezhető olyan helyzetben sem, amikor a két fél között hatalmi egyensúlyhiány van.

Kifejezett a hozzájárulás szükséges speciális, az érintettre jelentős adatvédelmi kockázattal járó esetekben.
Az elszámoltathatóság elve értelmében az adatkezelőt igazolási kötelezettség terheli, így az Adatkezelőnek igazolnia kell, hogy az érintett személyes adatai kezeléséhez hozzájárult.
A hozzájárulás bármikor visszavonható és erről az érintettet a hozzájárulása megadása előtt tájékoztatni kell.

4.2. SZERZŐDÉS TELJESÍTÉSE

Az adatkezelés megfelelő alapja, ha arra valamely szerződés vagy szerződéskötési szándék keretében van szükség. Szűken kell értelmezni, vagyis a szerződés megkötését megelőző, a szerződéskötéshez vezető adatkezelés esetén a szerződés teljesülése után már nem megfelelő jogalap az adatkezelésre.

4.3. JOGI KÖTELEZETTSÉG TELJESÍTÉSE

Az adatkezelés jogalapja lehet egy uniós vagy nemzeti jogban foglalt kötelezettségnek a teljesítése. A kötelezettségnek kötelező erejű jogszabályon kell alapulnia, ebben az esetben az adatkezelés célját is az uniós vagy nemzeti jogszabályban kell meghatározni.

4.4. LÉTFONTOSSÁGÚ ÉRDEK

A létfontosságú érdek, mint adatkezelési jogalap akkor alkalmazható, ha az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekének védelme miatt szükséges. A létfontosságú érdek, mint jogalap korlátozottan alkalmazható, kizárólag komoly veszélyhelyzet fennállása esetén.

4.5. KÖZÉRDEKŰ ADATKEZELÉS

A közérdekű adatkezelés jogalapként akkor alkalmazható, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges.
Ide tartozik, amikor az Adatkezelőtől adatszolgáltatást kérnek közfeladat teljesítése érdekében és a személyes adat adatszolgáltatásának nem a hatóság megkeresésén és nem jogszabályon alapul.

4.6. JOGOS ÉRDEK

Jogos érdek esetén a személyes adatok kezelése az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekkel szemben elsőbbséget élvez az érintett olyan érdeke vagy alapvető joga és szabadsága, amely a személyes adatok védelmét teszi szükségessé.
Annak eldöntésére, hogy az Adatkezelő jogos érdekével szemben elsőbbséget élvez-e az érintett érdeke vagy alapvető joga vagy szabadsága, az úgynevezett érdekmérlegelési tesztet kell elvégezni. Az érdekmérlegelési teszt írásbeli dokumentálása annak, hogy az Adatkezelő által tervezett személyes adat kezelésre miért van szükség, azt az adatkezelő hogyan végezné el, és milyen az érintettek érdekeit védő, garanciákat tartana be a folyamat során.

4.6.1. AZ ÉRDEKMÉRLEGELÉSI TESZT

1. Az adatkezelés céljának pontos meghatározása, milyen adatkategóriák, mennyi ideig tartó kezelését igényli a jogos érdek.
2. Az adatkezelő jogos érdekének a lehető legpontosabb meghatározása.
3. A cél elérése érdekében feltétlenül szükséges a személyes adatok kezelése? Vannak-e alternatív megoldások, amelyek alkalmazásával a személyes adatok kezelése nélkül, vagy kevesebb személyes adattal is megvalósítható a tervezett cél?
4. Annak meghatározása, hogy melyek lehetnek az érintett érdekei az adott adatkezelés vonatkozásában, amelyeket felhozhatna az adatkezeléssel szemben?
5. Annak meghatározása, hogy miért korlátozza arányosan az adatkezelői jogos érdek az érintett jogokat.

5. AZ ADATKEZELÉS ALAPELVEI

Az adatkezelési alapelveket az Adatkezelő az adatkezelése minden momentumában betartja és betartatja.

6. AZ ÉRINTETTEK JOGAI

6.1. AZ ÁTLÁTHATÓ TÁJÉKOZTATÁS

Az érintettek tájékoztatása az adatkezelő kötelezettsége, amely az átláthatóság alapelvének megvalósítását szolgálja. Az érintetteket tájékoztatni kell az adatkezelő elérhetőségéről, az adatkezelés lényeges körülményeiről, az érintett jogairól és a jogérvényesítés lehetőségeiről.
A tájékoztatást abban az esetben is meg kell adni az érintetteknek, ha a személyes adatokat nem tőlük gyűjtötték. A tájékoztatás megadásának határideje a két esetkörben a következők szerint változik:

- ha a személyes adatokat az érintettől gyűjtik, az adatok gyűjtésekor,
- ha a személyes adatok más forrásból származnak, az adatok megszerzésétől számított 1 hónapon belül (ha kapcsolattartásra használják az adatokat, az első kapcsolat felvételekor) kell az érintetteket tájékoztatni.

A tájékoztatás garanciális jellegű az érintett jogok gyakorlása szempontjából, ezért az érintettet

- érthető és átlátható módon
- főszabály szerint írásban (elektronikus út is ideértendő), az érintett kérésére szóban
- díjmentesen kell tájékoztatni.

6.2. HOZZÁFÉRÉSHEZ VALÓ JOG

A hozzáféréshez való jog az átláthatóság alapelvének megvalósítását szolgálja. Az érintett kérelmére vissza kell neki igazolni, hogy a személyes adatai kezelése folyamatban van-e, és ha igen, akkor hozzáférést kell biztosítani számára a kezelt személyes adataihoz, valamint hozzáférést kell biztosítani neki az alábbi információkhoz:

- az adatkezelés célja,
- a kezelt személyes adatok kategóriái,
- a címzettek,
- a tárolás tervezett időtartama,
- az érintett jogai,
- a panasz benyújtásának joga (jogorvoslati jog)
- az automatizált döntéshozatal ténye, ideértve a profilalkotást is.

6.3. HELYESBÍTÉSHEZ VALÓ JOG

Ez a jog a pontosság alapelvének való megfeleltetést érvényesíti. Ha az Adatkezelő. által kezelt adatok nem pontosak az érintett kérheti a rá vonatkozó pontatlan személye adat helyesbítését vagy kiegészítését.

6.4. TÖRLÉSHEZ VALÓ JOG

Az Adatkezelő. köteles törölni az érintett kérésére a rá vonatkozó személyes adatot, ha

- az adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték,
- az érintett visszavonja a hozzájárulását és az adatkezelésnek nincs más jogalapja,
- az érintett a saját helyzetével összefüggő okokból a jogos érdeken, vagy közfeladat teljesítésén alapuló adatkezelés ellen tiltakozik, ideértve a profilalkotást is és nincs elsőbbséget élvező jogszerű ok az adatkezelésre, vagy marketingtevékenység ellen tiltakozik,
- a személyes adatokat jogellenesen kezelték,
- a személyes adatokat az adatkezelőre alkalmazandó uniós vagy nemzeti jogban előírt jogi kötelezettség teljesítéséhez törölni kell.

Az Adatkezelő nem köteles törölni az adatokat az érintett kérelmére, ha valamelyik alább felsorolt kivétel alkalmazandó. Nem törölhető az érintettre vonatkozó személyes adatok, ha az adatkezelés szükséges

- a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából,
- az adatkezelőre alkalmazandó uniós vagy nemzeti jog szerinti kötelezettség teljesítése, illetve közérdekből vagy közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából,
- népegészségügy területét érintő közérdek alapján,
- közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból, amennyiben a törléshez való jog valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezt az adatkezelést,
- jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.

6.5. KORLÁTOZÁSHOZ VALÓ JOG

Az adatok korlátozása esetén az Adatkezelő csak tárolhatja a személyes adatokat, de egyéb módon nem kezelheti őket. Ez alól kivétel az érintett hozzájárulásával történő adatkezelés, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy más természetes
vagy jogi személy jogainak védelme érdekében vagy az unió illetve valamely tagállam fontos közérdekéből történő adatkezelés.
Az érintett kezelt személyes adatai korlátozását az alábbi esetekben kérheti:

- ha az érintett vitatja a személyes adatok pontosságát, a korlátozás arra az időtartamra vonatkozik, amíg az adatkezelő ellenőrzi a személyes adatok pontosságát,
- az adatkezelés jogellenes, de az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását,
- az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez,
- az érintett a saját helyzetével összefüggő okokból a jogos érdeken vagy közfeladat teljesítésén alapuló adatkezelés ellen tiltakozik, ideértve a profilalkotást is, a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

6.6. ADATHORDOZHATÓSÁGHOZ VALÓ JOG

Az adathordozhatóság joga a GDPR által bevezetett új jog, ami az adatok szabad áramlását biztosítja az Európai Unión belül. Az érintett akkor élhet-e jogával, ha

- az adatkezelés hozzájáruláson alapul vagy szerződés teljesítése érdekében és
- automatizált módon történik.

Az adathordozhatóság nem egy általános jog, csak a fenti esetben élhet vele az érintett. Amennyiben az érintett él-e jogával, jogosult arra, hogy

- a rá vonatkozó személyes adatokat géppel olvasható formátumban megkapja, vagy
- kérheti, hogy az adatkezelő közvetlenül továbbítsa az érintettre vonatkozó személyes adatokat egy másik adatkezelő részére.

6.7. TILTAKOZÁSHOZ VALÓ JOG

Az érintett akkor élhet e jogával, ha az adatkezelés jogos érdeken vagy közérdekű adatkezelésen alapul és az érintett saját helyzetével kapcsolatos okból tiltakozik az adatkezelés során bármikor. Következménye főszabály szerint az, hogy az adatkezelő a személyes adatokat nem kezelheti tovább.
Kivétel, ha az adatkezelő bizonyítja, hogy

- az adatkezelést kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy
- jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak,

az Adatkezelő ezekben az esetekben jogosult a személyes adatokat tovább kezelni.

Speciálisan alakul a tiltakozáshoz való jog direkt marketing tevékenység esetén. Ebben az esetben, ha az érintett tiltakozik az adatok kezelése ellen, ideértve a profilalkotást is, az adatkezelő nem kezelheti tovább a személyes adatokat (ebből a célból).

6.8. JOGORVOSLATHOZ VALÓ JOG

Az érintett jogosult a felügyeleti hatóságnál panasz benyújtására (panasztételhez való jog), illetve bírósági jogorvoslatra.
A felügyeleti hatóság Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatósága (NAIH) (cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/c., telefon: +36 (1) 391-1400, honlap: http://naih.hu), akihez az érintett jogosult panaszt benyújtani, amennyiben úgy ítéli meg, hogy a rá vonatkozó személyes adatok kezelése megsérti a GDPR-t.
Az érintett a felügyeleti hatóság döntése ellen a felügyeleti hatóság székhelye szerinti tagállam bírósága előtt élhet bírósági jogorvoslati jogával mind az érintette, mind pedig az adatkezelő/adatfeldolgozó és megtámadhatja a döntést.
Az érintett jogosult közvetlenül a bírósághoz fordulni, amennyiben megítélése szerint a személyes adatainak, a Rendeletnek nem megfelelő kezelése következtében megsértették a Rendelt szerinti jogait. Az Infotv. rendelkezése szerint a hatáskörrel rendelkező bíróság az érintett lakhelye vagy tartózkodási helye szerinti törvényszék.

7. AZ ADATVÉDELEM ÉS A TECHNIKAI FELTÉTELEK

A PÁNMED Bt. a személyes adatok kezeléséhez a szolgáltatás nyújtása során alkalmazott informatikai eszközöket úgy választja meg és üzemelteti, hogy a kezelt adat:

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

A PÁNMED Bt. az adatokat megfelelő intézkedésekkel védi a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés ellen.
Az adatkezelő olyan műszaki, szervezése és szervezeti intézkedésekkel gondoskodik az adatkezelés biztonságának védelméről, amely az adatkezeléssel kapcsolatban jelentkező kockázatoknak megfelelő szintet nyújt.
Az adatkezelő az adatkezelés során megőrzi:

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

A papíralapon kezelt személyes adatok biztonsága érdekében az adatkezelő az alábbi intézkedéseket alkalmazza:

- az adatokat csak az arra jogosultak ismerhetik meg, azokhoz más nem férhet hozzá, más számára fel nem tárhatóak;
- a dokumentumokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben helyezi el;
- a folyamatos aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá;
- a PÁNMED Bt. adatkezelést végző munkatársa a nap folyamán csak úgy hagyhatja el az olyan helyiséget, ahol adatkezelés zajlik, hogy a rá bízott adathordozókat elzárja, vagy az irodát bezárja;
- a PÁNMED Bt. adatkezelést végző munkatársa a munkavégzés befejeztével a papíralapú adathordozót elzárja;
- amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó biztonsági szabályokat alkalmazza az adatkezelő.

A számítógépen, illetve hálózaton tárolt személyes adatok biztonsága érdekében az adatkezelő az alábbi intézkedéseket és garanciális elemeket alkalmazza:

- az adatkezelés során használt számítógépek fölött tulajdonosi jogkörrel megegyező joggal bír az adatkezelő;
- a számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal - legalább felhasználói névvel és jelszóval – lehet csak hozzáférni, a jelszavak cseréjéről az adatkezelő rendszeresen gondoskodik;
- a hálózati kiszolgáló gépen (a továbbiakban: szerver) tárolt adatokhoz csak megfelelő jogosultsággal és csakis az arra kijelölt személyek férhetnek hozzá;
- amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül, az adat újra vissza nem nyerhető;
- a személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan gondoskodik;

a rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával megakadályozza illetéktelen személyek hálózati hozzáférését.

7.1.ADATTITKOSÍTÁS

Az adatkezelő támogatja a személyes adatok titkosítását, így adatszegés esetén a publikussá vált információ olvashatatlan ezért nem okoz kárt az érintettek számára, valamint a titkosított adatok adatvédelmi incidense kapcsán az érintetteket sem kell tájékoztatni.

7.2. A MUNKAVÁLLALÓK ÁLTALÁNOS FELELŐSSÉGE

Valamennyi munkavállaló (gyakornok, önkéntes), aki a jelen szabályzatban meghatározott adatokhoz hozzáfér a megszerzett adatokat kizárólag a munkavégzése körében és céljából kezelheti, rögzítheti, tarthatja nyilván.
A PÁNMED Bt. biztosítja, hogy a munkavállalók képzés/oktatás keretében megismerhessék a pontos teendőiket és faladataikat, valamint felelősségüket az adatvédelem és az adatkezelés tekintetében.

A munkavállalók kötelesek valamennyi birtokukba jutott adatot biztonságosan kezelni, munkavégzésük során elővigyázatosnak lenni és a jelen adatvédelmi szabályzatban meghatározott feladatokat végrehajtani.
A munkavállaló köteles a szoftveres hozzáférés esetén erős és titkos jelszavakat alkalmazni, a jelszót megosztani, másnak felfedni szigorúan tilos.
Arra fel nem hatalmazott személlyel nem oszthat meg személyes adatokat, sem a vállalkozáson belül, se azon kívül.
A munkavállaló köteles rendszeresen felülvizsgálni és aktualizálni a rendelkezésre álló adatokat annak érdekében, hogy személyes adat szükségtelenül ne kerüljön sem tárolásra, sem egyéb kezelésre. A már szükségtelenné váló adatok törlése a munkavállaló felelőssége.
Amennyiben a munkavállaló bizonytalan a helyes adatkezelés vagy az adatvédelmi szempontok tekintetében, úgy köteles tanácsért a vezetőjéhez vagy az adatvédelmi tisztségviselőhöz fordulni.
Ha a munkavállaló tudomást szerez arról, hogy az általa kezelt személyes adat hibás, hiányos vagy időszerűtlen, köteles azt helyesbíteni vagy a helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni.
A PÁNMED Bt. adatkezelést végző alkalmazottja fegyelmi, kártérítési, szabálysértési és büntetőjogi-felelősséggel tartozik a munkavégzés során tudomására jutott személyes adatok jogszerű kezeléséért, a PÁNMED Bt. nyilvántartásaihoz rendelkezésére álló hozzáférési jogosultságok jogszerű gyakorlásáért.

7.3. PAPÍR ALAPÚ ADATKEZELÉS

A jelen bekezdés célja annak a meghatározása, hogy az adatokat hol és milyen módon szükséges kezelni ahhoz, hogy az adatok biztonsága biztosítható legyen. Az adattárolásra vonatkozó további esetleges kérdésekkel a vezető munkatárshoz fordulhat a vállalkozás munkatársa.
A papír alapon kezelt adatokat olyan biztonságos helyen szükséges tárolni, ahol arra jogosulatlan személy nem ismerheti meg.
Azokat az elektronikus úton érkezett vagy kezelt adatokat, melyek valamely okból nyomtatásra kerülnek elzárt irattartókban, illetőleg elkülönítetten szükséges kezelni. A vállalkozás munkatársai kötelesek gondoskodni arról, hogy a kinyomtatott iratokhoz arra jogosulatlan személyek ne férjenek hozzá. A kinyomtatott adatokat tartalmazó iratokat azonnal szükséges megsemmisíteni akkor, amikor a kinyomtatás oka megszűnik.

7.4. ELEKTRONIKUS ADATKEZELÉS

Az elektronikusan tárolt adatokat védeni szükséges a jogosulatlan eléréstől, véletlen törléstől és kémprogramokkal, vírusokkal, illetéktelen rendszer feltörésekkel és rendszertámadásokkal szemben.
Az adatokat erős jelszavakkal szükséges védeni, melyek cseréjére rendszeresen, de legalább fél évente sor kerül. A jelszavak titkosnak, hozzáférhetetlennek kell lenniük, a munkavállalók/ vezetők nem oszthatják meg azt sem egymás között, sem más személyekkel.
Amennyiben az adat hordozható adattárolón (cd, DVD, pendrive, SSD) kerül rögzítésre ezeket az adattároló eszközöket a használatot követően biztonságos helyen, jogosulatlan személyek számára hozzáférhetetlenül szükséges tárolni.

Adatokat csak az arra kijelölt szervereken és hardver eszközökön szabad tárolni. Felhő alapú szolgáltatás igénybevételével adat csak a kijelölt és maghatározott szolgáltatóval kötött szerződés alapján és szerint tárolható. A vállalkozás vezetője az adattárolás megkezdése előtt meggyőződik arról, hogy a felhő alapú szolgáltatást biztosító partner megfelel az adatvédelem jogszabályi és technikai követelményének.
Valamennyi adattárolásra szolgáló szervert és számítógépet szükséges tűzfallal és vírusirtóval védeni.
A tárolt adatokat rendszeresen szükséges felülvizsgálni.
A személyes adatokat tartalmazó szervereket a nyitott irodahelységen kívüli elkülönített helyen szükséges tárolni.
Az adattárolásra alkalmazott szoftvereket rendszeresen frissíteni szükséges. A frissítés megkezdése előtt a szoftverfrissítési metódust az adatvesztés elkerülése érdekében tesztelni szükséges.
A személyes adatokat tilos közvetlenül a laptopra vagy egyéb mobileszközre (tablet, okostelefon) menteni.

7.5.TECHNOLÓGIA AZ E-MAIL ÜZENETEK MENEDZSELÉSÉRE

A PÁNMED Bt. megállapítja, hogy az interneten továbbított elektronikus üzenetek protokolltól (e-mail, web, ftp, stb.) függetlenül sérülékenyek az olyan hálózati fenyegetésekkel szemben, amelyek tisztességtelen tevékenységre, szerződés vitalitására, az információk felfedésére, módosítására vezetnek. Az ilyen fenyegetésekkel szemben az adatkezelő megtesz minden tőle levárható óvintézkedést. A rendszereket megfigyeli annak érdekében, hogy minden biztonsági eltérést rögzíthessen és bizonyítékokkal szolgálhasson minden biztonsági esemény esetében. A rendszermegfigyelés ezen kívül lehetővé teszi az alkalmazott óvintézkedések hatékonyságának ellenőrzését is. Az adatkezelő által biztosított védelmi eljárásoknak képesnek kell lenniük a rosszindulatú tartalom kiszűrésére.

7.6.TECHNOLÓGIA AZ ESZKÖZÖK ÉS A HOZZÁFÉRÉSEK MENEZSELÉSÉRE

A PÁNMED Bt. szegmentálja és korlátozza a hálózatának azon részeire vonatkozó hozzáférést, amelyek tárolják és feldolgozzák a rendkívül érzékeny személyes adatokat. A hálózati sebezhetőségek és külső fenyegetések felismerése és elemzése, amelyek célja az adatlopás és adatmegsemmisítés. A hálózat folyamatos figyelemmel kísérése és védelme a megoldás annak érdekében, hogy a személyes adatok sérülését célzó fenyegetések ellen hatékonyan fellépjen.

Alkalmazott eszközök:

- …személyes tűzfal: Microsoft Firewall
- …adathalászat elleni eszköz
- …jelszókezelő
- … biztonságos törlés
- … biztonsági levélszűrő: clamAV
- …szerver spam szűrő: Spamassasin

- … kódoló szoftver
- …. behatolás jelző szoftver

7.7. AZ ADATOK FIZIKAI TÁROLÁSI HELYE

Személyes adatok az alábbi módon kerülhetnek a PÁNMED Bt. kezelésébe: egyfelől elektronikus levélben másfelől, az ügyfél személyes adatszolgáltatása útján. Az adatkezelő számítástechnikai rendszere és más adatmegőrzési rendszere a székhelyén és az adatfeldolgozójánál találhatóak meg.
Az adatkezelő székhelye és az adatfeldolgozó székhelye és számítástechnikai rendszere védett a számítógéppel támogatott csalás, kémkedés, szabotázs, vandalizmus, tűz és árvíz, továbbá számítógép vírusok, a számítógépes betörések és a szolgálatmegtagadásra vezető támadások ellen. Az adatkezelő a biztonságról a 4.4. pontban részletezett szerverszintű és alkalmazásszintű védelmi eljárásokkal gondoskodik.
A PÁNMED Bt. közös rendelőben működik az azonos tevékenységet végző (járóbeteg ellátás) más vállalkozóval, amely adatvédelmi és adatkezelési rendszere megegyezik. Az esetleges adatvédelmi incidensek kiküszöbölésére a PÁNMED Bt. megteszi a szükséges lépéseket.

8. AZ ADATOK FELHASZNÁLÁSA

A vállalkozás az adatkezelés eltérő célja alapján ügyviteli és nyilvántartási célú adatkezeléseket végez. Az ügyvitelhez kapcsolódó adatkezelés a szerződés/megállapodás nyilvántartásaihoz (iktatásához), feldolgozásához kapcsolódik. Alapvető célja az adott szerződéshez/megállapodáshoz tartozó feladatok elvégzéséhez (szerződések teljesítése), az adatkezelés szereplőinek azonosításához és a szerződés lezárásához szükséges adatok biztosítása. Az ügyviteli célú adatkezelés során a személyes adatok kizárólag az adott szerződés irataiban és az ügyviteli segédletekben szerepelnek: kezelésük ebből a célból csak az alapul szolgáló irat selejtezéséig lehetséges.
A nyilvántartási célú adatkezelés az egyes adatfajtákból álló adatállományt hoz létre, az adatkezelés időtartama alatt biztosítva az adatok különböző jellemzők alapján történő visszakereshetőségét, lekérdezhetőségét. A személyes adatok kezelésének célja a vállalkozás üzletviteli tevékenysége során történő felhasználása, ennek megfelelően az alábbi feladatok azonosíthatóak:

- az adatkezelővel munkavégzésre irányuló jogviszonyban álló személyek adatait tartalmazza,
- a foglalkozás-egészségügyi ellátásban kezelt személy betegségére, egészségügyi állapotára vonatkozó személyes adatokat tartalmaz, gyógykezelés vagy az egészség megőrzése céljából,
- az érintett anyagi vagy egyéb szociális támogatása céljából nyilvántartott személyes adatokra vonatkozik
- a vállalkozással szerződéses kapcsolatba került személyek személyes adataira vonatkozik (ügyviteli célú adatkezelés)

- a hivatalos statisztika célját szolgáló személyes adatokat tartalmaz, feltéve, hogy a törvényben meghatározottak szerint, az adatok érintettel való kapcsolatának megállapítását véglegesen lehetetlenné teszik,
- tudományos kutatás céljait szolgálja, ha az adatokat nem hozzák nyilvánosságra
- levéltári őrzésre átadott iratokkal összefüggésben valósul meg.

Az adatok jogszerű és célhoz kötött használata során az alábbiak betartása kötelező:

- a személyes adatokkal dolgozó munkavállalók a munkaterület elhagyása során kötelesek a felhasznált eszközt képernyőzárral védeni, melyhez egyedi belépési azonosító, illetőleg kód kapcsolódik
- személyes adat csak olyan levelezőrendszeren küldhető tovább, melynek biztonsága és zárt jellege garantált, továbbá olyan címzett számára, aki megfelelő és biztos módon beazonosítható olyan személyként, aki a fogadott személyes adatokat jogszerűen megismerheti
- a személyes adatokat tartalmazó fájlokat, üzeneteket kóddal, vagy egyéb módon titkosítani szükséges
- a személyes adatok Európai Gazdasági Térségen túli továbbítása fő szabály szerint tilos, amennyiben annak továbbítása mégis szükségessé válik, úgy azt csak olyan fogadó részére szabad továbbítani, aki igazoltan megfelel a GDPR-ban foglalt valamennyi adatvédelmi követelménynek.
- a vállalkozás napi operatív tevékenysége során tilos a saját gépre személyes adatokat menteniük, valamennyi adatot kötelező a vállalkozás saját belső rendszerére menteni
- a vállalkozás működése során nem vihetők ki a személyes adatokat tartalmazó iratok a vállalkozás székhelyéről/telephelyéről. Amennyiben ez mégis szükségessé válna, úgy ebben a tekintetben a munkavállalók kötelesek azt bejelenteni és egyedi jóváhagyást kérni a felettesüktől.

8.1. AZ ADATOK PONTOSSÁGÁNAK BIZTOSÍTÁSA

A vállalkozás jogszabályi kötelessége az általa kezelt személyes adatok naprakész és pontos nyilvántartása.
A vállalkozás kiemelt figyelmet fordít az esetlegesen és szükségesen nyilvántartott különleges adatok naprakészségére és pontosságára.
A fentiek okán a vállalkozás valamennyi munkavállalójának kiemelt feladata, hogy a tőle telhető legjobb módon az adatokat naprakészen és pontosan tartsa nyilván. Az adatokat a lehető legkevesebb adattároló helyen szükséges tartani, a vállalkozás munkavállalói feleslegesen és engedély nélkül semmilyen egyéb nyilvántartást vagy személyes adatokat tartalmazó egyéb forrást nem készíthetnek.
A vállalkozás az érintettek számára folyamatosan biztosítja az adatpontosítás lehetőségét.
Amennyiben a kezelt adatok körében pontatlan adatok kerülnek elő, azt haladéktalanul pontosítani szükséges, így különösen, ha az ügyfél az általa megadott telefonszámot vagy e-mail címet közöl. Az elektronikus levelezés mindaddig elérhetőnek tekinthető, ameddig az ügyfél a cím megváltoztatását nem jelenti be, vagy onnan a kézbesítés sikertelenségére vonatkozó rendszerüzenet vissza nem érkezik.

Az érintett jelzések hiányában is pontatlannak bizonyult adatot valamennyi rendszerből és adattárolóból a pontatlanság megállapítása után haladéktalanul törölni kell.
A vállalkozás marketingért felelős munkatársának a feladata a marketing levelezési és adatrendszerének naprakészen tartása, azzal, hogy annak teljes felülvizsgálata legalább fél évente különösebb ok nélkül is ütemezetten kötelező.

8.2. BIZTONSÁGI ELLENŐRZÉSEK A HATÉKONYSÁG FOKOZÁSA ÉRDEKÉBEN

Az adatvédelmi hiányosságok feltárására az adatkezelő rendszeres időközönként (4 havonta) ellenőrzéseket végez. Az ellenőrzések eredményét értékeli és felméri a lehetséges adatvédelmi kockázatokat. Szükséges tesztelni az incidensekre adott válaszlépések hatékonyságát, és adott esetben növelni a biztonsági szinteket. Értékelésre kerül az információs rendszerek rugalmassága az azonosított kockázatokkal szembeni védekezéshez, valamint a bevezetett biztonsági ellenőrzések hatékonysága az adatszegések megelőzésében.

9. ADATVÉDELMI INCIDENSEK KEZELÉSE

9.1. AZ ADATVÉDELMI INCIDENSEK BEJELENTÉSE

Az 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 adatokhoz való jogosulatlan hozzáférést eredményezi.
Az a munkavállaló vagy adatfeldolgozó, aki az adatkezelő által kezelt vagy feldolgozott személyes adatokkal kapcsolatban adatvédelmi incidenst észlel, azt köteles haladéktalanul az ügyvezetőnek és az adatvédelmi tisztviselőnek bejelenteni, megadva a nevét, telefonszámát és/vagy e-mail címét, az incidens tárgyát, valamint azt, hogy az incidens informatikai rendszert érint-e. Adatvédelmi incidensnek tekinti az adatkezelő a személyes adat jogellenes kezelését vagy feldolgozását, így különösen jogosulatlan hozzáférést, megváltoztatást, továbbítást, nyilvánosságra hozatalt, törlést vagy megsemmisítést, valamint véletlen megsemmisülést és sérülést. A bejelentő további olyan információkat is megadhat, amelyeket az incidens beazonosítása, megvizsgálása szempontjából lényegesnek ítél.
Amennyiben az adatvédelmi incidens informatikai rendszert érintően következett be, akkor az ügyvezető az illetékes rendszergazdát is tájékoztatja.
Adatfeldolgozó vállalkozási szerződésében rögzíteni kell, az adatvédelmi incidens bejelentés módját és tartalmát.

9.2. A BEJELENTÉS MEGVIZSGÁLÁSA ÉS AZ INCIDENS KEZELÉSE

Az ügyvezető – informatikai rendszert érintő incidens esetén az informatikussal együttműködve – a bejelentést haladéktalanul megvizsgálja és ésszerű mértékű ű bizonyosság esetén azonnali védelmi és kárenyhítési lépéseket tesz meg.
Az adatszolgáltatásnak tartalmaznia kell

- az incidens bekövetkezésének időpontját és helyét,
- az incidens leírását, körülményeit, hatásait,

- az incidens során kompromittálódott adatok körét, számosságát,
- a kompromittálódott adatokkal érintett személyek körét,
- az incidens elhárítása érdekében tett intézkedések leírását,
- a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.

Az adatszolgáltatás alapján az ügyvezető – informatikai rendszerben bekövetkezett adatvédelmi incidens esetében a rendszergazdával együtt – javaslatot tesz az adatvédelmi incidens elhárításához szükséges azonnali intézkedésekről az adatok kezelését vagy feldolgozását végző területnek, továbbá az adatgazdának.
Az adatvédelmi incidens elhárítása érdekében megvalósított egyes intézkedésekről az adatgazda az adott intézkedések végrehajtását követő 1 munkanapon belül köteles az ügyvezetőt tájékoztatni.
Az Adatkezelő. a lehető leghamarabb, de maximum 72 órával a tudomást szerzést követően az adatvédelmi incidenst bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóság felé.
Az Adatkezelő. az érintetteket is értesíti, amennyiben az incidens nagy kockázatot jelent számukra, és nem voltak bevezetve olyan védelmi intézkedések, amelyek biztosítják, hogy a kockázat bekövetkezése már nem valószínű. Az érintettek felé a tájékoztatás tartalma megegyezik a NAIH felé benyújtott tájékoztatás tartalmával, de nyelvezetében világosnak és könnyen érthetőnek kell lennie.
A NAIH felé benyújtandó adatvédelmi incidens bejelentésnek tartalmaznia kell:

- az incidens jellegét, az érintett adatok kategóriáját és számát, és az érintettek kategóriáját és számát,
- az adatvédelmi tisztviselő nevét és elérhetőségét,
- a valószínűsíthető következményeket,
- az orvoslásra tett vagy tervezett intézkedéseket, beleértve a bekövetkezett hatások enyhítését.

Az adatkezelőnek haladéktalan tájékoztatási kötelezettsége van az érintettek felé amennyiben az adatvédelmi incidens

- magas kockázattal jár az érintettek jogaira nézve
- vagy a NAIH erre utasítja.

Nem szükséges az érintettek tájékoztatása az adatvédelmi incidens bekövetkezéséről

- ha a védelmi intézkedések értelmezhetetlenné teszik az adatokat (titkosítás)
- hiába történt meg az adatsérülés, az utólag megtett lépések lecsökkentik a kockázatot.

Nyilvános közzétételre kerülhet sor abban az esetben, ha aránytalan erőfeszítést igényelne az érintettek értesítése.

9.3.AZ INCIDENS NYILVÁNTARTÁSA

Az adatvédelmi incidensről az Adatkezelő nyilvántartást vezet.
A nyilvántartásba rögzíteni kell:

- az érintett személyes adatok körét,
- az adatvédelmi incidenssel érintettek adatok kategóriáját és az érintettek körét és számát,
- a valószínűsíthető következményeket,
- az adatvédelmi incidens időpontját,
- az adatvédelmi incidens körülményeit, a személyes adatokra tett hatásait,
- az adatvédelmi incidens elhárítására megtett intézkedéseket,
- az adatkezelést előíró jogszabályban meghatározott egyéb adatokat
- az adatvédelmi tisztviselő nevét és elérhetőségét.

A nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatokat személyes adatokat érintő incidens esetében 5 évig, különleges adatokat érintő incidens esetében 20 évig köteles az adatkezelő megőrizni.

10. AUTOMATIZÁLT ADATKEZELÉSEN ALAPULÓ DÖNTÉS

A GDPR célja az érintettek személyes adatai lehető legszélesebb védelmének biztosítása. A technológia rohamos fejlődésével egyre nagyobb mértékben használják az adatkezelők a szoftvereket, vagy algoritmusokat személyes adatok kezelésére, hogy ezáltal például gazdasági előnyre tegyenek szert, javítsák a felhasználói élményt vagy gyorsítsák a döntéshozatalt. Ezen technológiák alkalmazása azonban kockázatos a személyes adatokra, így a GDPR kiemelt figyelmet fordít e területre.

10.1. KIZÁRÓLAG AUTOMATIZÁLT ADATKEZELÉSEN ALAPULÓ DÖNTÉS

A GDPR alapján az érintett jogosult arra, hogy kérje, hogy a kizárólag automatizált adatkezelésen alapuló döntés ne terjedjen ki rá, ha az az érintettre joghatással jár (kihat a törvényes vagy szerződéses jogaira) vagy jelentős mértékben érinti (nem hat ki a jogaira, de életkörülményeit befolyásolja).
Három esetben azonban mégis megengedett az ilyen döntéshozatal:
1) ha szerződés megkötése vagy teljesítése érdekében szükséges, mert például

- következetesebb és pártatlanabb döntéshozatalt eredményez a profilozás
- ügyfelek fizetési határidő elmulasztásának kockázatát csökkenti
- rövidebb döntéshozatali idő, hatékonyságnövelő hatás

1. Uniós vagy magyar jog lehetővé teszi.
2. Az érintett kifejezett hozzájárulása esetén.

Amennyiben az 1) -2) pont alatti kivétel alkalmazandó, az adatkezelő köteles megfelelő garanciákat biztosítani:

- érintett külön tájékoztatása (az adatkezelésről, a döntéshozatal során alkalmazott logikáról stb.),
- arról, hogy az érintett kérelmezheti, hogy emberi beavatkozást kapjon,

- lehetőség, hogy az érintett kifejtse álláspontját vagy magyarázatot kapjon az ilyen értékelés alapján hozott döntésről,
- lehetőség, hogy az érintett megtámadja a döntést.

10.2. PROFILALKOTÁS

Személyes adatok (legalább részben) automatizált kezelése, amely során az érintettre vonatkozó személyes jellemzők kiértékelése történik. Ide tartozik különösen az érintett gazdasági helyzetére, munkahelyi teljesítményére, személyes preferenciáira, egészségi állapotára vagy megbízhatóságára vonatkozó személyes jellemzőinek az elemzése vagy előre jelzése.
Az Adatkezelő. adatkezelése során sem automatizált adatkezelésen alapuló döntést sem profilalkotást nem alkalmaz.

11. AZ ADATKEZELÉSI TEVÉKENYSÉG NYILVÁNTARTÁSA

A GDPR általános kötelezettségként állapítja meg, hogy mind az adatkezelő, mind az adatfeldolgozó köteles a felelősségükbe tartozó adatkezelési tevékenységéről nyilvántartást vezetni.
Az Adatkezelő. nyilvántartása az adatkezelésre vonatkozó legfontosabb információkat tartalmazza, mint pl. az adatkezelés célja, kezelt adatok köre vagy, hogy történik-e adattovábbítás stb.
A nyilvántartások vezetése kiemelten fontos az elszámoltathatóság alapelvének való megfelelés érdekében.

12. NEMZETKÖZI ADATTOVÁBBÍTÁS

Harmadik országba személyes adatot továbbítani, kizárólag az alábbi esetekben lehet:

12.1. BIZOTTSÁG MEGFELELŐSÉGI HATÁROZATA

Személyes adatokat EGT államok területén kívülre, elsődlegesen az EU Bizottság megfelelőségi határozata alapján lehet. A Bizottság akkor hoz megfelelőségi határozatot, ha a Bizottság megállapította, hogy a harmadik ország megfelelő védelmi szintet biztosít. Az ilyen adattovábbításhoz nem szükséges külön engedély.
A határozat meghozatalához a Bizottság a következő tényezőket mérlegeli:

- jogállamiság kritériumai (az emberi jogok és alapvető szabadságok tiszteletben tartása, adatvédelmi szabályok, hatékony jogorvoslat stb.),
- létezik-e egy vagy több független és hatékonyan működő felügyeleti hatóság,
- nemzetközi kötelezettségei vagy egyéb, jogilag kötelező erejű egyezményekből vagy jogi eszközökből, valamint többoldalú vagy regionális rendszerekben való részvételéből eredő – különösen a személyes adatok védelmével kapcsolatos – kötelezettségei.

A 95/46/EC irányelv értelmében a Bizottság a következő országok tekintetében ismerte el a megfelelő védelmi szint biztosítását:

• Andorra
• Argentína
• Kanada
• Feröer szigetek
• Guernsey
• Izrael
• Man-sziget
• Jersey
• Új-Zéland
• Svájc
• Uruguay
• EU-US Adatvédelmi Pajzs.

Az irányelv alapján kiadott engedélyek hatályban maradnak mindaddig, amíg azokat szükség esetén a felügyeleti hatóság nem módosítja, nem váltja fel vagy nem helyezi hatályon kívül.

12.2. BIZOTTSÁG MEGFELELŐSÉGI HATÁROZAT HIÁNYÁBAN, MEGFELELŐ GARANCIÁK ALAPJÁN

Az adatkezelő vagy az adatfeldolgozó csak abban az esetben továbbíthat személyes adatokat EGT-n kívüli államokba, ha az adatkezelő vagy adatfeldolgozó megfelelő garanciákat nyújtott, és csak azzal a feltétellel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre.
Megfelelő garancia alapján az adattovábbítás történhet a hatóság engedélyével vagy engedélye nélkül is:

- Hatóság engedélye nélkül: kötelező erejű vállalati szabályok, általános adatvédelmi kikötések, jóváhagyott magatartási kódex vagy jóváhagyott tanúsítási mechanizmus által), vagy
- Hatóság engedélyével: adatkezelő és harmadik országbeli adatkezelő, feldolgozó vagy címzett között létrejött szerződéses rendelkezések vagy közigazgatási megállapodásba beillesztett rendelkezések.

12.3. EGYEDI HELYZETEKBEN BIZTOSÍTOTT ELTÉRÉSEK

Megfelelőségi határozat és megfelelő garanciák nélkül abban az esetben lehet személyes adatot továbbítani, ha az alábbi feltételek közül legalább egy teljesül:

- az érintett kifejezetten hozzájárulását adta a tervezett továbbításhoz azt követően, hogy a kockázatokról tájékoztatták,
- az adattovábbítás az érintett és az adatkezelő közötti szerződés teljesítéséhez, szerződés megkötéséhez**,**
- az adattovábbítás fontos közérdekből szükséges,
- az adattovábbítás **jo**gi igények előterjesztése, érvényesítése és védelme miatt szükséges,

- az adattovábbítás az érintett vagy valamely más személy létfontosságú érdekeinek védelme miatt szükséges, és az
- érintett fizikailag vagy jogilag képtelen a hozzájárulás megadására,
- a továbbított adatok olyan nyilvántartásból származnak, amely az uniós vagy a tagállami jog értelmében a nyilvánosság tájékoztatását szolgálja.

12.4. EGYÉB FELTÉTELEK TELJESÜLÉSE ESETÉN

Ha az adattovábbítás nem alapulhat megfelelőségi határozaton, nem állnak rendelkezésre megfelelő garanciák és a különleges helyzetekre vonatkozó eltérések egyike sem alkalmazandó, akkor a harmadik országba történő adattovábbítás csak akkor történhet, ha:

- ha az adattovábbítás nem ismétlődő,
- korlátozott számú érintettre vonatkozik,
- az adatkezelő kényszerítő erejű jogos érdekében szükség, amely érdekhez képest nem élveznek elsőbbséget az érintett érdekei, jogai és szabadságai, és
- az adatkezelő az adattovábbítás minden körülményét megvizsgálta, és e vizsgálat alapján megfelelő garanciákat nyújtott a személyes adatok védelme tekintetében.

Ilyen esetekben az adatkezelőnek tájékoztatnia kell a felügyeleti hatóságot az adattovábbításról.

12.5. AZ UNIÓS JOG ÁLTAL NEM ENGEDÉLYEZETT TOVÁBBÍTÁS ÉS KÖZLÉS

Valamely harmadik ország bíróságának ítélete vagy közigazgatási hatóságának döntése, ami valamely adatkezelő vagy adatfeldolgozó számára személyes adatok továbbítását vagy közlését írja elő, kizárólag akkor ismerhető el vagy hajtható végre, ha az adattovábbítás a két ország közötti hatályos nemzetközi megállapodáson alapul (pl. jogsegélyszerződés).
Az Adatkezelő nem továbbít személyes adatokat 3. országba.

13. ADATVÉDELMI HATÁSVIZSGLAT

A GDPR rendelet az alábbi esetekben írja elő az adatvédelmi hatásvizsgálat lefolytatását:

- nyilvános helyek nagymértékű és módszeres megfigyelése,
- különleges személyi adatok nagy számban történő kezelése,
- automatizált adatkezelésen alapuló személyes adatok módszeres és kiterjedt értékelése, ide értve a profilalkotást is, ha erre alapulva joghatással bíró és természetes személyt jelentős mértékben érintő döntések épülnek.
- és minden olyan adatkezelés tekintetében, amelyek valószínűsíthetően magas kockázattal járnak.

Az adatvédelmi hatásvizsgálat lényegében egy eszköz az Adatkezelő számára, az adatvédelmi megfelelőség kialakítására és igazolására. Eredményeként elkészíti a kockázatmérséklési tervezetet.
Az adatvédelmi hatásvizsgálatban az adatkezelő

1. lefekteti, milyen adatkezelési műveleteket tervez és milyen célból,
2. a célok figyelembevételével elvégezi az adatkezelési műveletek szükségességi és arányossági vizsgálatát,
3. mérlegeli az érintettek jogaira gyakorolt kockázatokat,
4. majd a feltárt kockázatok kivédésére alkalmazott intézkedéseket mutatja be.

Az Adatkezelő a különleges személyi adatok kezelésére tekintettel az adatvédelmi hatásvizsgálatot végzett.

14. ELJÁRÁSI SZABÁLYOK

Az adatkezelő indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintetett a GDPR 15-22. cikk szerinti kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható.
A határidő meghosszabbításáról az Adatkezelő a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet. Ha az érintett elektronikus úton nyújtotta be a kérelmét, a tájékoztatást elektronikus úton kerül megadásra, kivéve, ha az érintett azt másként kéri.
Ha az Adatkezelő nem tesz intézkedéseket az érintett kérelme nyomán, késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet az intézkedés elmaradásának okairól, valamint arról, hogy az érintett panaszt nyújthat be valamely felügyeletei hatóságnál és élhet bírósági jogorvoslati jogával.
Az Adatkezelő a kért információkat és tájékoztatást díjmentesen biztosítja. Ha az érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt- túlzó, az adatkezelő, figyelemmel a kért információ vagy tájékoztatás nyújtásával vagy a kért intézkedés meghozatalával járó adminisztratív költségekre ésszerű mértékű díjat számolhat fel, vagy megtagadhatja a kérelem alapján történő intézkedést.
Az Adatkezelő minden olyan címzettet tájékoztat az általa végzett valamennyi helyesbítésről, törlésről, vagy adatkezelési-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintett kérésére az adatkezelő tájékoztatja e címzettekről.
Az Adatkezelő az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért az adatkezelő az adminisztratív költségeken alapuló, ésszerű mértékű díjat számíthat fel. Ha az érintett elektronikus úton nyújtotta be a kérelmét, az információk elektronikus formátumban kerülnek rendelkezésre bocsátásra megsértése kivéve, ha az érintett másként kéri.

15. KÁRTÉRÍTÉS ÉS SÉRELEMDÍJ

Minden olyan személy, aki az adatvédelmi rendelet megsértésének eredményeként vagyoni vagy nem vagyoni kárt szenvedett, az elszenvedett kárért az Adatkezelőtől vagy az adatfeldolgozótól kártérítésre jogosult.

Az adatfeldolgozó csak abban az estben tartozik felelősséggel az adatkezelés által okozott károkért, ha nem tartotta be a jogszabályban meghatározott, kifejezetten az adatfeldolgozókat terhelő kötelezettségeket, vagy ha az adatkezelő jogszerű utasításait figyelmen kívül hagyta vagy azokkal ellentétesen járt el.
Ha több adatkezelő vagy több adatfeldolgozó vagy mind az adatkezelő, mind az adatfeldolgozó érintett ugyanabban az adatkezelésben és felelősséggel tartozik az adatkezelés által okozott károkért, minden egyes adatkezelő vagy adatfeldolgozó egyetemleges felelősséggel tartozik a teljes kárért.
Az adatkezelő vagy az adatfeldolgozó mentesül a felelősség alól, ha bizonyítja, hogy a kárt előidéző eseményért őt semmilyen módon nem terheli felelősség.

16. JOGORVOSLATOK

16.1. PANASZ

Amennyiben az Adatkezelőtől adatkezelésével kapcsolatban az érintettnek problémája van, lehetősége van közvetlenül az adatvédelmi tisztségviselőhöz fordulni panaszával.

16.2. BÍRÓSÁGHOZ FORDULÁS JOGA

Az érintett a jogainak megsértése esetén az adatkezelő ellen bírósághoz fordulhat. A bíróság az ügyben soron kívül jár el.

16.3. ADATVÉDELMI HATÓSÁGI ELJÁRÁS

Adatvédelmi és Adatkezelési Szabályzat PÁNMED Bt.
Az érintett panaszával a Nemzeti Adatvédelmi és Információszabadság Hatósághoz fordulhat:
Név: Nemzeti Adatvédelmi és Információszabadság Hatóság
Székhely: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.
Levelezési cím: 1530 Budapest, Pf.: 5.
Telefon: 06-1-391-1400
E-mail: ugyfelszolgalat@naih.hu
Honlap: www.naih.hu
Készült, Budapest 2018. május 14.
A PÁNMED Egészségügyi és Szolgáltató Betéti Társaság taggyűlése 2018. május 14 napján az Adatvédelmi és Adatkezelési Szabályzatot elfogadta.