Adatvédelmi Szabályzat

MATERNITY Magánklinika Kft.

Tartalomjegyzék

I. Bevezetés

1. Az Adatkezelő adatai

A Net Média Kiadó és Internet Tartalomszolgáltató Zrt. (a továbbiakban: Adatkezelő vagy Társaság) adatkezelési folyamatainak szabályozása érdekében az alábbi Adatvédelmi szabályzatot (a továbbiakban: Szabályzat) alkotja belső használatra.

Adatkezelő: MATERNITY Magánklinika Kft. **(továbbiakban: Adatkezelő)**
Székhely: 1126 Budapest, Királyhágó tér 8-9.
Cégjegyzékszám: 01-09-918867
Adószám: 14766624-2-43
Honlap: www.maternity.hu
Telefon: +36-1-213-4220
Adatvédelmi tisztviselő elérhetősége: adatvedelem@maternity.hu

2. Vonatkozó jogszabályok

- Magyarország Alaptörvénye, VI. cikk
- az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (GDPR)
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)

3. A Szabályzat célja

Jelen Szabályzat a természetes személyek személyes adatainak az Adatkezelő által történő adatkezelésének szabályait tartalmazza a GDPR és az Infotv.-ben foglaltaknak való megfelelés céljából. Az Adatkezelő vállalja, hogy adatkezelési tevékenységét a megfelelő belső szabályok, technikai és szervezési intézkedések meghozatalával úgy végzi el, hogy megfeleljen ezen jogszabályok rendelkezéseinek. Az Adatkezelő a GDPR rendelkezéseit az adatkezelés során minden körülmények között szem előtt tartja.

4. A Szabályzat hatálya

A Szabályzat személyi hatálya kiterjed az Adatkezelővel szerződéses kapcsolatban álló természetes személyek (pl. munkavállaló, ügyfél, felhasználó, partner, beszállító) személyes adatainak az Adatkezelő által történő kezelésére.

A Szabályzat tárgyi hatálya kiterjed az Adatkezelő minden szervezeti egységében folytatott valamennyi személyes adatot tartalmazó adatkezelésre függetlenül attól, hogy az elektronikusan és/vagy papír alapon történik.

II. Fogalmak, alapelvek, jogalapok

1. Fogalmak

Személyes adat: azonosított vagy azonosítható természetes személyre („Érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható. Ilyen tipikus személyes adatok különösen: név, lakcím, születési hely és idő, anyja neve.

Nyilvántartási rendszer: a személyes adatok bármely módon – centralizált, decentralizált vagy funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető.

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, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.

Profilalkotás: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják.

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

Adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az Adatkezelőt vagy az Adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja.

Adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az Adatkezelő nevében személyes adatokat kezel.

Címzett: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel, vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e.

Harmadik fél: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az Érintettel, az Adatkezelővel, az Adatfeldolgozóval vagy azokkal a személyekkel, akik az Adatkezelő vagy Adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.

Az Érintett hozzájárulása: az Érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az Érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.

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.

Felügyeleti Hatóság: egy tagállam által a GDPR 51. cikkének megfelelően létrehozott független közhatalmi szerv, amely Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság (továbbiakban: NAIH vagy Felügyeleti Hatóság).

2. Alapelvek

Az Adatkezelő a személyes adatok kezelése során a következő alapelveket veszi figyelembe: A személyes adatok:

- kezelését jogszerűen és tisztességesen, valamint az Érintett számára átlátható módon kell végezni (**jogszerűség, tisztességes eljárás és átláthatóság**)
- gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon (**célhoz kötöttség**)
- adatkezelési céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk (**adattakarékosság**)
- pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék (**pontosság**)
- tárolásának olyan formában kell történnie, amely az Érintett azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé (**korlátozott tárolhatóság**)
- 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)**
- az Adatkezelő felelős a fentieknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására (**elszámoltathatóság**)

3. Jogalapok

Az Adatkezelő a személyes adatokat mindig a valamely jogalap szerint kezeli, amelyek az alábbiak lehetnek:

- az Érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez (GDPR 6. cikk (1) bekezdés a) pontja)
- az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az Érintett az egyik fél, vagy az a szerződés megkötését megelőzően az Érintett kérésére történő lépések megtételéhez szükséges (GDPR 6. cikk (1) bekezdés b) pontja)
- az adatkezelés az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges (GDPR 6. cikk (1) bekezdés c) pontja)
- az adatkezelés az Érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges (GDPR 6. cikk (1) bekezdés d) pontja)
- az adatkezelés közérdekű vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges (GDPR 6. cikk (1) bekezdés e) pontja)
- az adatkezelés az Adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az Érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az Érintett gyermek (GDPR 6. cikk (1) bekezdés f) pontja)

III. Szerepkörök

1. Adatvédelmi tisztviselő

Az adatvédelmi tisztviselőt (továbbiakban: DPO) szakmai rátermettség, az adatvédelmi jog és gyakorlat szakértői szintű ismerete alapján kell kijelölni. Az Adatkezelő az adatvédelmi tisztviselő elérhetőségét közzéteszi honlapján, valamint bejelenti a Felügyeleti Hatóság (NAIH) részére. Az adatvédelmi tisztviselő Felügyeleti Hatóság általi nyilvántartásba vételét itt ellenőrizheti: https://dpo-online.naih.hu/DPO/Search.

Az Adatkezelő biztosítja az adatvédelmi tisztviselő részére a feladat ellátásához szükséges forrásokat, valamint azt, hogy a feladatai ellátása során utasításokat senkitől ne fogadjon el, ezen feladatai ellátásával összefüggésben nem bocsátható el és szankcióval nem sújtható.

Az adatvédelmi tisztviselő szervezetileg közvetlenül az Adatkezelő vezető tisztségviselőjének tartozik felelősséggel. Az adatvédelmi tisztviselő felett a munkáltatói vagy a szerződésben meghatározott jogokat az Adatkezelő vezető tisztségviselője gyakorolja.

Az adatvédelmi tisztviselő feladatai:

- tájékoztat és szakmai tanácsot ad az adatkezelést végző alkalmazottak részére a GDPR, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban
- ellenőrzi a GDPR-nak, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá a személyes adatok védelmével kapcsolatos belső szabályoknak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is

- kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését
- együttműködik a Felügyeleti Hatósággal
- az adatkezeléssel összefüggő ügyekben – ideértve a GDPR 36. cikkében említett előzetes konzultációt is – kapcsolattartó pontként szolgál a Felügyeleti Hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele
- egyéb esetekben: segítséget nyújt és szakmai tanácsot ad az adatvédelmet szabályozó dokumentumok elkészítése és az ezzel kapcsolatos feladatok elvégzése során.

2. Munkavállaló

A Szabályzatban előírtak betartatásáért a feladatkörében minden érintett önálló szervezeti egység vezetője is felelős.

A Vezetőség gondoskodik arról, hogy jogosulatlan személyek ne tekinthessenek be személyes adatokba, továbbá arról, hogy a személyes adat tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető.

Kiemelt területként kell kezelni a munkavállaló vonatkozásában az adatvédelmi- és biztonságtudatossági képzést. Ezen tudatos magatartások komoly üzleti károkat okozó hibák és támadások megelőzésében játszanak szerepet. A kialakított szabályrendszer és az informatikai eszközök önmagukban nem képesek garantálni a szervezet számára az adat- és információbiztonságot, ehhez a munkavállalónak is hozzá kell járulnia felelős magatartásukkal a napi munkájuk során. A munkavállaló megfelelő képzése a képzést követően kimutathatóan kevesebb adatvédelmi incidenst eredményez.

A munkavállaló általános adatvédelmi-, és biztonságtudatossági képzése évente legalább egy alkalommal dokumentáltan történik (jelenléti ív).

IV. Az Érintett jogainak érvényesítése

Az Érintettnek (azon személynek, akinek valamilyen személyes adata az Adatkezelő által kezelésre került, így például álláspályázatra jelentkező, munkavállaló, felhasználó, ügyfél, vendég, partner kapcsolattartója) az alábbi jogai vannak az Adatkezelővel szemben:

1. **Hozzájárulás tetszőleges visszavonásának joga (GDPR 7. cikk)**
   Amennyiben az adatkezelés az Érintett hozzájárulása alapján történt, joga van annak visszavonására az így folytatott adatkezelés leállítása érdekében. A hozzájárulás visszavonása a visszavonást megelőzően folytatott adatkezelés törvényességét nem érinti.

2. **Előzetes tájékozódáshoz való jog (GDPR 60 preambulumbekezdés, valamint 13-14. cikk)**
   Az Érintett jogosult arra, hogy az adatkezeléssel összefüggő tényekről és információkról az adatkezelés megkezdését megelőzően tájékoztatást kapjon.

3. **Az Érintett hozzáférési joga (GDPR 15. cikk)**
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 a GDPR-ban meghatározott információhoz hozzáférést kapjon.

4. **A helyesbítéshez való jog (GDPR 16. cikk)**
Az Érintett jogosult arra, hogy kérésére az Adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat, és kérje a hiányos személyes adatainak kiegészítését.

5. **A törléshez való jog („az elfeledtetéshez való jog") (GDPR 17. cikk)**
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, ha a feltételek valamelyike fennáll.

6. **Adatkezelés korlátozásához való jog (GDPR 18. cikk)**
Az Érintett jogosult arra, hogy kérésére az Adatkezelő korlátozza az adatkezelést, ha meghatározott feltételek teljesülnek.

7. **Az adathordozhatósághoz való jog (GDPR 20. cikk)**
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 anélkül, hogy ezt akadályozná az az Adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta.

8. **A tiltakozáshoz való jog (GDPR 21. cikk)**
Az Érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak kezelése ellen.

9. **Az Érintett tájékoztatása az adatvédelmi incidensről (GDPR 34. cikk)**
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.

10. **A Felügyeleti Hatóságnál történő panasztételhez való jog (hatósági jogorvoslathoz való jog) (GDPR 77. cikk)**
Az Érintett a személyes adatainak védelméhez fűződő joga sérelme esetén jogorvoslatért fordulhat:

Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)
székhely: 1055 Budapest, Falk Miksa utca 9-11.
levelezési cím: 1363 Budapest, Pf. 9.
telefon: +36 (1) 391-1400
email: ugyfelszolgalat@naih.hu

honlap: www.naih.hu

11. **A Felügyeleti Hatósággal szembeni bírósági jogorvoslathoz való jog (GDPR 78. cikk)**
Minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a Felügyeleti Hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben, vagy ha a Felügyeleti Hatóság nem foglalkozik a panasszal, vagy ha nem tájékoztatja az Érintettet a benyújtott panasszal kapcsolatos eljárási fejleményekről vagy annak eredményéről.

12. **Az Adatkezelővel vagy az Adatfeldolgozóval szembeni bírósági jogorvoslathoz való jog (GDPR 79. cikk)**
Az Érintett jogosult bírósághoz fordulni az Adatkezelő vagy Adatfeldolgozó ellen, ha a személyes adatai kezelésének jogellenességét tapasztalja. A bíróság az ügyben soron kívül jár el. Ebben az esetben szabadon eldöntheti, hogy a lakóhelye vagy a tartózkodási helye szerint illetékes törvényszéknél nyújtja-e be a keresetét. A törvényszékek elérhetősége: https://birosag.hu/torvenyszekek.

Az Érintett kérelmét – függetlenül attól, hogy a szervezeten belül pontosan hová érkezik be elsőként – továbbítani kell az adatvédelmi tisztviselőhöz.

Az adatvédelmi tisztviselő értékeli a kérelmet, egyeztet a kérelem tárgyát képező adatkezelési tevékenységekben érintett részleggel, majd megteszi a szükséges intézkedést annak érdekében, hogy a kérelem a lehető legteljesebb mértékben megválaszolásra kerüljön.

Az Érintett kérelmére indokolatlan késedelem nélkül és általában legkésőbb a kérelem beérkezését követő 1 hónapon belül válaszolni kell, valamint tájékoztatni a jogai gyakorlására irányuló kérelme nyomán hozott intézkedésekről (GDPR 12. cikk (3)–(4) bekezdés). Ennek megfelelően az Érintett kérelmét azonnal fel kell dolgozni.

A választ az Érintett részére ingyenesen, tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva, valamint az általa használt kommunikációs csatornákon keresztül kell biztosítani (GDPR 12. cikk (1) bekezdés). Ha az Érintett kérelme egyértelműen megalapozatlan vagy – különösen annak ismétlődő jellege miatt – túlzó, az Adatkezelő megtagadhatja a kérelem alapján történő intézkedést. A kérelem egyértelműen megalapozatlan vagy túlzó jellegének bizonyítása az Adatkezelőt terheli.

Az Érintetti jog gyakorlása körében érkezett kérelemmel kapcsolatos eljárás folyamata:

1) **Kérelem beérkezése és továbbítása**
A kérelmet, amely érkezhet emailben, postai úton, telefonon vagy személyesen, haladéktalanul továbbítani kell az adatvédelmi tisztviselőhöz. Ilyen esetben az Adatkezelő által készített formanyomtatvány is használható (ld. Érintetti kérelem).
A telefonon vagy személyesen előterjesztett kérelmet annak a kollégának kell lejegyezni és az adatvédelmi tisztviselő részére emailen megküldeni, akinél a kérelem bejelentésre került.

2) **A kérelem megvizsgálása és minősítése**
Az adatvédelmi tisztviselő feladata az, hogy meghatározza a kérelem típusát, tehát azt, hogy az Érintetti jogok közül az Érintett melyiket kívánja érvényesíteni, azaz:
- milyen intézkedést kér
- milyen jogot érvényesít
- kire irányul a kérelem
- ki a kérelmező.

3) **Előzetes ellenőrzés**
Az adatvédelmi tisztviselő ellenőrzi, hogy a kérelmező által megadott adatok alapján egyértelműen beazonosítható-e a személy, akiről szó van, a megadott adatok alapján a kérdéses személy megtalálható-e az adatbázisban. Amennyiben nem áll rendelkezésre elegendő információ, akkor további adat szolgáltatását kell kérni a kérelmezőtől. Ezt követően az adatvédelmi tisztviselő a kérelem elfogadhatóságát értékeli, ugyanis a kérelmet el lehet utasítani vagy észszerű díj előzetes megfizetéséhez lehet kötni, ha az „egyértelműen megalapozatlan" (pl. túlzó és/vagy ismétlődő jellegű).

4) **Személyazonosság ellenőrzése és az adatbázisok átvizsgálása**
Amennyiben minden szükséges adat – akár hiánypótlás útján is – rendelkezésünkre áll, azt kell megvizsgálni, hogy az adott személyre nézve kezel-e az Adatkezelő személyes adatot, valamint az, aki e joggal élni kíván, az valóban a kérelem benyújtására jogosult személy-e.

5) **A kérelem érdemi értékelése**
E lépés során azt értékeljük, hogy az Érintett ténylegesen hivatkozhat-e arra a jogra, melyet érvényesít (jogalaponként eltérő az érvényesíthető jogok listája). Ezután elkészül a megfelelő válasz az Érintett részére az Adatkezelő által készített formanyomtatvány alapján (ld. Érintetti kérelemre válasz). Az adott eljárás az érvényesíteni kívánt jogtól függ.

6) **Kérelem megválaszolása, további intézkedések**
Az adatvédelmi tisztviselő megküldi az elkészített választ (ld. Érintetti kérelemre válasz) és tájékoztatja az Érintettet a megtett intézkedésekről. Amennyiben az Érintett olyan jog gyakorlását kérte, amely további intézkedést kíván, megteszi a szükséges lépéseket. Például törlési kérelem esetén gondoskodik az adat másik Adatkezelőnél történő törléséről is.

V. Adatkezelő kötelezettségei

1. Beépített és alapértelmezett adatvédelem

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 a GDPR-ban foglalt követelmények teljesítéséhez és az Érintett jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába.

Az Adatkezelő megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre. Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.

Az Adatkezelő már az adatkezelés tényleges megkezdése előtt – például már egy projekt előkészítés időszakában, vagy egy új technológia bevezetése előtt – is figyelemmel kíséri az adatvédelemmel kapcsolatos jogszabályok előírásait. A beépített adatvédelem az Adatkezelő saját, olyan belső eljárásainak az összessége, amivel igyekszik megfelelni annak, hogy az Érintett magánszféráját minél jobban védje.

2. Adatfeldolgozók

A munkavállalónak jeleznie kell az illetékes szervezeti egységnek egy új beszállító, egy új megbízó (továbbiakban: Partner) megjelenését annak érdekében, hogy megállapításra kerüljön:

- történik-e a Partner részéről adatkezelés az Adatkezelő felhasználójának, partnerének vagy munkavállalójának személyes adatainak vonatkozásában
- a Partner Adatfeldolgozónak vagy közös/önálló Adatkezelőnek minősül-e
- szükséges-e „Adatfeldolgozási szerződést” vagy más típusú szerződést kötni ezzel a Partnerrel.

Az Adatkezelő az Adatfeldolgozói tevékenységet végző természetes vagy jogi személlyel, illetve jogi személyiséggel nem rendelkező szervezettel az adatvédelmi kötelezettségek teljesítése érdekében „Adatfeldolgozási szerződést” köt. Az Adatfeldolgozási szerződés szabályozza az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az Érintettek kategóriáit, az Adatkezelő és Adatfeldolgozó kötelezettségeit és jogait, valamint a technikai és szervezési intézkedéseket általános leírását (ld. Adatfeldolgozási szerződés).

3. Adatkezelési tevékenységek nyilvántartása

Az Adatkezelő vezet(het)i az adatkezelési tevékenységek nyilvántartását, amely az alábbi adatokat tartalmazza (ld. Adatkezelési tevékenységek nyilvántartása):

- az Adatkezelő neve és elérhetősége
- az Adatvédelmi tisztviselő neve és elérhetősége
- adatkezelés céljai
- adatkezelés jogalapjai (opcionális)

- Érintettek kategóriái
- személyes adatok kategóriái
- adatkezelés időtartama (opcionális)
- címzettek kategóriái
- harmadik országba vagy nemzetközi szervezet részére történő adattovábbítás
- technikai és szervezési intézkedések általános leírása (opcionális).

VI. Adatvédelmi incidens

1. Adatvédelmi incidens esetén alkalmazandó eljárás

A munkavállaló bármilyen személyes adat biztonságával kapcsolatban észlelt történést haladéktalanul jelenteni köteles az adatvédelmi tisztviselő részére.

Az adatvédelmi incidens gyanúja esetén, az adatvédelmi tisztviselőt legalább az alábbiakról tájékoztatni kell (ld. Adatvédelmi incidens bejelentő lap):

- incidens tárgya
- bejelentés időpontja
- incidens bekövetkezésének időpontja
- incidens bekövetkezésének helye
- észlelő (neve, beosztása, szervezeti egysége, telefonszáma, email címe)
- bejelentő (neve, beosztása, szervezeti egysége, telefonszáma, email címe)
- informatikai rendszer érintettsége
- incidens külső partneri érintettsége
- incidens jellege
- incidens rövid leírása
- az incidensben érintett természetes személyek kategóriája[1] és hozzávetőleges száma
- az incidensben érintett személyes adatok kategóriái[2] és hozzávetőleges száma
- az incidensből eredő, valószínűsíthető következmények
- az incidens orvoslására tett vagy tervezett intézkedések
- az incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedések
- az incidenssel kapcsolatos egyéb információk
- bejelentő aláírása

Az adatvédelmi tisztviselő a hozzá érkezett gyanús esetet késedelem nélkül kivizsgálja. A vizsgálatnak tartalmaznia kell, hogy az eset adatvédelmi incidensnek minősül-e, az magas kockázattal jár-e az Érintett jogaira és kötelezettségeire, milyen jellegű kockázatról van szó és szükséges-e a Felügyeleti Hatóság vagy az Érintett tájékoztatása az incidensről. A vizsgálatot legkésőbb a bejelentéstől számított 72 órán belül be kell fejezni és a vizsgálat eredményéről tájékoztatni kell az Adatkezelő vezető tisztségviselőjét.

[1] pl. munkavállaló, vendég, ügyfél, felhasználó

[2] pl. személyazonosító adatok (név, születési, hely, idő, anyja neve), elérhetőségi adatok (telefonszám, email cím, lakcím, levelezési cím), felhasználói adatok (felhasználónév, email cím), egyéb személyes adatok (pénzügyi adatok, egészségügyi adatok stb.).

A magas kockázattal járó adatvédelmi incidens esetén az Adatkezelő indokolatlan késedelem nélkül és a tudomásszerzést követő legfeljebb 72 órán belül köteles tájékoztatni az adatvédelmi incidensről a GDPR 55. cikke alapján létrehozott Felügyeleti Hatóságot. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

2. Adatvédelmi incidens nyilvántartás

Az adatvédelmi incidensről nyilvántartást kell vezetni, amely tartalmazza (ld. Adatvédelmi incidens nyilvántartás):

- incidens tárgya
- bejelentés időpontja
- incidens bekövetkezésének időpontja
- incidens bekövetkezésének helye
- bejelentő (neve, beosztása, szervezeti egysége, telefonszáma, email címe)
- informatikai rendszer érintettsége
- incidens külső partneri érintettsége
- incidens jellege
- incidens rövid leírása
- az incidensben érintett természetes személyek kategóriája[3] és hozzávetőleges száma
- az incidensben érintett személyes adatok kategóriái[4] és hozzávetőleges száma
- az incidensből eredő, valószínűsíthető következmények
- az incidens orvoslására tett vagy tervezett intézkedések
- az incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedések
- az incidenssel kapcsolatos egyéb információk
- a Nemzeti Adatvédelmi és Információszabadság Hatósághoz történő bejelentés időpontja(i)
- Érintett tájékoztatásának időpontja
- Érintett tájékoztatásának módja.

3. Az adatvédelmi incidens bejelentése a Felügyeleti Hatóság részére

Ha a vizsgálat eredményeként megállapítást nyer, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve, akkor azt indokolatlan késedelem nélkül, legkésőbb 72 órán belül be kell jelenteni a Felügyeleti Hatóságnak.

A bejelentésnek tartalmaznia kell:

- ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az Érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát

[3] Pl. munkavállaló, vendég, ügyfél, felhasználó

[4] Pl. személyazonosító adatok (név, születési, hely, idő, anyja neve), elérhetőségi adatok (telefonszám, email cím, lakcím, levelezési cím), felhasználói adatok (felhasználónév, email cím), egyéb személyes adatok (pénzügyi adatok, egészségügyi adatok stb.).

- közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket
- ismertetni kell az Adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

A Felügyeleti Hatóság e célra rendszeresített formanyomtatványa, amelyen a bejelentés megtehető: https://naih.hu/adatvedelmi-incidensbejelent--rendszer.html.

4. Az Érintett tájékoztatása az adatvédelmi incidensről

Ha a vizsgálat eredményeként megállapítást nyer, hogy az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságára nézve, akkor arról indokolatlan késedelem nélkül értesíteni kell az Érintettet. Nem kell az Érintettet tájékoztatni, ha:

- az Adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták
- az Adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az Érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé.

5. Adatvédelmi hatásvizsgálat

Amennyiben valamely új adatkezelési folyamat – annak jellegére, hatókörére, körülményeire, céljaira tekintettel – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelés megkezdését megelőzően az Adatkezelő hatásvizsgálatot folytat le arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.

A hatásvizsgálat kiterjed legalább:

- a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére
- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára
- az Érintett jogait és szabadságait érintő kockázatok vizsgálatára és
- a kockázatok kezelését célzó intézkedések bemutatására (garanciák, biztonsági intézkedések és mechanizmusok).

6. Előzetes konzultáció

Amennyiben az elvégzett hatásvizsgálat azt állapítja meg, hogy az adatkezelés valószínűsíthetően magas kockázattal jár, akkor az Adatkezelő a személyes adatok kezelését megelőzően konzultációt kezdeményez a Felügyeleti Hatóságnál.

VII. Adatvédelmi ellenőrzés

A Szabályzat rendelkezéseit az uniós vagy magyar, adatkezelést érintő jogszabályok változásakor, de legalább 2 évente egyszer felül kell vizsgálni.

Az adatvédelmi ellenőrzés az ütemtervben meghatározottakon túl szúrópróbaszerűen, vagy az adatvédelmi incidens kivizsgálása során tett megállapítás (pl. adatkezelésre vonatkozó előírás be nem tartása vezetett az incidens bekövetkezéséhez) következményeként is végezhető.

Amennyiben az adatbiztonsági szabályok és intézkedések megtartásának ellenőrzése információbiztonsági szakértelmet is megkíván, az adatvédelmi ellenőrzésbe információbiztonsági szakértőt is be kell vonni.

Az adatvédelmi tisztviselő az adatvédelmi ellenőrzés tapasztalatairól és javaslatairól írásos jelentést készít az Adatkezelő vezető tisztségviselőjének, aki meghozza a szükséges intézkedéseket.

VIII. Záró rendelkezések

Ez a szabályzat **2021. március 1. napján** lép hatályba.

A szabályzat rendelkezéseit a munkavállalóval ismertetni kell.