Müpa Budapest Nonprofit Kft.

ADATVÉDELMI SZABÁLYZATA

2023.

Tartalomjegyzék

1. A SZABÁLYZAT bevezető rendelkezései 4

1.Alapelvek 4

2.Alapfogalmak 5

3.A Szabályzat célja 7

4.A Szabályzat személyi hatálya 7

5.A Szabályzat időbeli hatálya 7

6.A Szabályzat tárgyi hatálya 7

7.Feladat és felelősség 8

2. Az Adatkezelő adatvédelmi szervezeti felépítése és rendszere 8

8.Vezérigazgató 8

9.Adatvédelmi tisztviselő (DPO) 8

10. Belső adatvédelmi felelős (BAF) 10

3. Általános adatvédelmi szabályok 11

11. Az adatkezelés jogszerűségének biztosítása 11

12. Adatkezelés bevezetésével kapcsolatos feladatok 11

13. Dokumentálási kötelezettség 13

14. A személyes adatok kezelésének felülvizsgálata 13

15. Adatkezelő és a munkavállalók feladatai a megfelelő adatvédelem érdekében 13

16. Adatkezelési Nyilvántartások 14

17. Az érintetti jogok gyakorlásának általános szabályai 15

18. Az adatkezelési tevékenység nyilvánossága 21

19. Gyermekek adatkezelésére vonatkozó speciális szabályok 21

20. Közérdekű adatok megismerése iránti igényre vonatkozó általános szabályok 22

21. Harmadik országba irányuló adattovábbítás általános szabályai 22

22. Általános adatbiztonsági intézkedések (technikai és szervezési intézkedések) meghatározása és végrehajtása 22

23. Adatkezelés megszüntetésével kapcsolatos feladatok 23

4. Az Adatkezelő szerződéses partnereivel, és Munkavállalói val kapcsolatos adatkezelések szabályai 24

24. A közös adatkezelői megállapodások megkötésének és végrehajtása, ellenőrzésének szabályai 24

25. Adatfeldolgozói szerződések megkötésének és végrehajtása ellenőrzésének szabályai 26

26. A munkavállalók személyes adatainak kezelésére vonatkozó különleges szabályok 26

5. Az Adatkezelő szolgáltatásához kapcsolódó adatkezelések általános szabályai 27

27. A szolgáltatás nyújtása során kezelt személyes adatok 27

6. Az adatvédelmi incidensekre vonatkozó általános szabályok 28

28. Az adatvédelmi incidens minősítése 28
29. Az adatvédelmi incidens észlelése 29
30. Az adatvédelmi incidens kivizsgálása 30
31. Az érintett tájékoztatása a súlyos adatvédelmi incidensről 30
32. Az adatvédelmi incidens bejelentése a Felügyeleti Hatóságnak 33
33. Az adatvédelmi incidensek nyilvántartása 34
34. Jogkövetkezmények alkalmazása 34
7. Adatkezelés során alkalmazandó módszertanok 35
35. Az érdekmérlegelési teszt elvégzésének módszertana 35
36. Az adatvédelmi hatásvizsgálat elvégzésének módszertana 36
8. Záró rendelkezések 37

1. A SZABÁLYZAT BEVEZETŐ RENDELKEZÉSEI

1. Alapelvek

1. A **MÜPA Budapest Nonprofit Kft.** (a továbbiakban: **Adatkezelő**) jelen Adatvédelmi Szabályzatban (a továbbiakban: **Szabályzat**) határozza meg a természetes személyek személyes adatainak kezelésével és védelmével kapcsolatos szabályokat.

2. A Szabályzat hatálya alá tartozó személyek kötelesek a tevékenységük során az Adatkezelő kezelésében lévő személyes adatokat a mindenkori jogszabályi rendelkezéseknek megfelelően, így különösen a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016/679/EU európai parlamenti és tanácsi rendelet (a továbbiakban: **GDPR**), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: **Infotv.**), a Munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.), a Polgári Törvénykönyvről szóló 2013. évi V. törvény, a Büntető Törvénykönyvről szóló 2012. évi C. törvény, valamint az Adatkezelőre irányadó egyéb jogszabályok rendelkezései szerint kezelni. Az Adatkezelő a személyes adatok kezelésével járó tevékenysége során érvényre juttatja a GDPR alapelveit, így különösen:
   a/ jogszerűség, tisztességes eljárás és átláthatóság elvei: a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni;
   b/ célhoz kötöttség elve: a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történik, és azokat az Adatkezelő nem kezeli ezekkel a célokkal össze nem egyeztethető módon;
   c/ adattakarékosság elve: a kezelt személyes adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk;
   d/ pontosság elve: a kezelt személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék;
   e/ korlátozott tárolhatóság elve: a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé;
   f/ integritás és bizalmas jelleg: a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve;

g/ elszámoltathatóság elve: az adatkezelő felelős az adatkezelési elveknek való megfelelésért, továbbá képesnek kell lennie a megfelelés igazolására

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

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

3. A Szabályzat hatálya alá tartozó személyek kötelesek az olyan tevékenységük során, amely szükségszerűen együtt jár személyes adatok kezelésével, az adott tevékenységre és a személyes adatok kezelésére vonatkozó jogszabályi rendelkezések mellett a jelen Szabályzat rendelkezései szerint eljárni.

2. Alapfogalmak

4. Jelen Szabályzat alkalmazása során a GDPR 4. cikkében és az Infotv. 3. § 3., 4., 6., 11., 12., 13., 16., 17., 21., 23., 24. pontjaiban meghatározott fogalmakon kívül az alábbi fogalmakat kell alkalmazni:

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

b/ adatkezelési nyilvántartás: az Adatkezelő által a GDPR 30. cikkében rögzített tartalmi elemekkel folyamatosan aktualizált nyilvántartás

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

d/ adatvédelmi hatásvizsgálat: olyan vizsgálat, amelyet az adatkezelő köteles elvégezni, amennyiben valamely tervezett adatkezelés – figyelemmel annak jellegére, hatókörére, körülményeire és céljaira, ideértve különösen az új technológiák alkalmazásának esetét – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve,

és amelynek célja annak megállapítása, hogy a tervezett adatkezelés a személyes adatok védelmét hogyan érinti. Az adatvédelmi hatásvizsgálat egy olyan eljárás, amelynek során az adatkezelő a tervezett adatkezelési műveletet vagy műveleteket áttekinti, megvizsgálja az adatkezelés érintettekre gyakorolt esetleges hatását, felméri annak kockázatait, a kockázatok kezelésének módját, és mindezt megfelelően dokumentálja,

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

f/ belső adatvédelmi felelős (BAF): az adatvédelmi tisztviselő tevékenységét a jelen Szabályzat szerint támogató munkavállaló (Jogi vezető);

g/ adatvédelmi tisztviselő (DPO): a GDPR 39. cikkében meghatározott feladatokat az Adatkezelő részére szerződéses jogviszonyban ellátó személy.

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

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

j/ dolgozói személyes adat: az Adatkezelővel munkaviszonyban álló személyek adata,

k/ érdekmérlegelési teszt: adatkezelés tervezett bevezetése esetén annak írásbeli dokumentálása, hogy az adatkezelő számba vette az adatkezelést megalapozó érdekeket, érveket, valamint az érintettek személyes adatok védelméhez fűződő – a tervezett adatkezelés ellen ható – jogait és érdekeit, és ezen érdekek és érvek összevetésével megalapozza az adatkezelés bevezetését vagy a bevezetés elutasítását,

l/ informatikai szakterület: az informatikai rendszerek üzemeltetéséért, az informatikai biztonság ellátásáért felelős szervezeti egység vagy egységek, ideértve az Adatkezelő elektronikus információs rendszer biztonságáért felelős személyét is,

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

n/ törlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása a továbbiakban már nem lehetséges.

3. A Szabályzat célja

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

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

7. A Szabályzat további célja, hogy meghatározza az Adatkezelő által vezetett, személyes adatokat tartalmazó nyilvántartások vezetésének és az adatvédelmi auditok, illetve az adatvédelmi szervezet működtetésének jogszerű rendjét, valamint biztosítsa az adatvédelmi jogi elveinek és az adatbiztonság követelményeinek érvényesülését.

4. A Szabályzat személyi hatálya

8. Jelen Szabályzat személyi hatálya kiterjed az Adatkezelő munkavállalóira, valamint azon természetes személyekre, akik személyes adatait a jelen Szabályzat hatálya alá tartozó adatkezelések tartalmazzák (a továbbiakban: **érintett**), továbbá azon személyekre, akik jogait vagy jogos érdekeit az adatkezelés érinti. Az Adatkezelő megbízásából személyes adatok kezelését végző Adatfeldolgozók esetén az erre a jogviszonyra az Adatkezelővel kötött szerződésben a GDPR 28. cikkének megfelelően rendelkezni kell arról, hogy az Adatkezelő által megbízott Adatfeldolgozó a feladata ellátása során hogyan juttatja érvényre jelen Szabályzat rendelkezéseit.

5. A Szabályzat időbeli hatálya:

9. Jelen Szabályzat a hatálybalépése napjától a módosításáig vagy visszavonásáig hatályos. A Szabályzat felülvizsgálatára rendszeres időközönként, illetve soron kívül kerül soramennyiben jogszabályi, szakmai, strukturális vagy egyéb változások szükségessé teszik a felülvizsgálatot.

6. A Szabályzat tárgyi hatálya

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

a/ az Adatkezelő önálló adatkezelői minőségében saját szervezeti egységeinek működtetése érdekében végrehajtott adatkezelési műveletekhez köthetők,
b/ az Adatkezelő szerződéses partnereivel, hatóságokkal és felügyeleti szervekkel kapcsolatos adatkezelési műveletekhez köthetők,
c/ az Adatkezelő által nyújtott szolgáltatásokhoz köthetők.

7. Feladat és felelősség

11. Az adatkezelés jogszerűsége érdekében az alábbi feladat és felelősségi köröket rendeli el az Adatkezelő:

Jelen Szabályzat **kidolgozásáért** felelős:	Belső Adatvédelmi Felelős (BAF)
Jelen Szabályzat **alkalmazásáért** felelős:	Belső Adatvédelmi Felelős (BAF)
Jelen Szabályzat **ellenőrzéséért** felelős:	Adatvédelmi Tisztviselő (DPO)

2. AZ ADATKEZELŐ ADATVÉDELMI SZERVEZETI FELÉPÍTÉSE ÉS RENDSZERE

8. Vezérigazgató

12. A Vezérigazgató az Adatkezelő hatályos adatvédelmi jogszabályoknak megfelelő működése érdekében:

a/ megbízza az adatvédelmi tisztviselőt (DPO);
b/ jelen szabályzat útján kijelöli a belső adatvédelmi felelőst (BAF);
c/ ellenőrzi az adatvédelmi tisztviselő (DPO) és a belső adatvédelmi felelős (BAF) tevékenységét;
d/ kiadja az Adatvédelmi Szabályzatot és gondoskodik annak betartatásáról;
e/ biztosítja az adatvédelmi tevékenység ellátásához, valamint az érintett jogai gyakorlásához szükséges személyi és tárgyi feltételeket.

9. Adatvédelmi tisztviselő (DPO)

13. Az adatvédelmi tisztviselőt a Vezérigazgató nevezi ki/bízza meg az olyan, jogi vagy természetes személyek közül, aki vagy amely ismeri az Adatkezelő működését, feladatait, munkafolyamatait és rendelkezik vagy jogi személy megbízása esetén annak alkalmazottja:

a/ lehetőleg jogi végzettséggel vagy informatikai főiskolai (BSc) vagy egyetemi (MSc) szintű végzettséggel;
b/ az európai és hazai adatvédelemmel kapcsolatos főbb szabályozók, hatósági és bírósági határozatok, iránymutatások ismeretével;
c/ alapvető adatkezelési és informatikai folyamatok ismeretével;
d/ legalább 2 év adatvédelmi területen szerzett gyakorlattal.

14. Az adatvédelmi tisztviselő a megbízatása során szorosan együttműködik az Adatkezelő belső adatvédelmi felelősével.

15. Az adatvédelmi tisztviselő független, függetlensége biztosítása érdekében szakmai feladatai ellátása során utasítást nem fogadhat el, szakmai feladatai ellátásával összefüggésben nem bocsátható el. Jelen Szabályzatban foglalt tevékenysége ellátása során autonóm, szakmai ügyekben kizárólag a Vezérigazgatónak tartozik felelősséggel.

16. Az Adatkezelő elősegíti az adatvédelmi tisztviselő megfelelő szakmai feladatellátását. Ennek érdekében az Adatkezelő biztosítja különösen az adatvédelmi tisztviselő feladatai végrehajtásához a személyes adatokhoz és az adatkezelési műveletekhez való hozzáférést, valamint a szakértői szintű ismereteinek fenntartásaihoz szükséges forrást, elegendő időt a feladatai ellátásához, a megfelelő technikai-, eljárási intézkedésekhez szükséges források meghatározása (költségvetési tervezés) során annak érdekében, hogy teljesüljenek az adatvédelem alapelvei a technikai vívmányok alkalmazása (beépített adatvédelem) és az adatvédelmet szolgáló megoldások (alapértelmezett adatvédelem) révén. A felügyeleti hatósággal történő együttműködés során az adatvédelmi tisztviselő – igény szerint a belső adatvédelmi felelős és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – tartja a kapcsolatot.

17. Az adatvédelmi tisztviselő véleményét – a jelen szabályzat rendelkezései szerint – ki kell kérni a személyes adatok kezelést érintő döntések, szerződés minták és belső szabályzatok előkészítése, módosítása esetén.

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

19. Az Adatkezelőben nem lehet adatvédelmi tisztviselő az a természetes személy, aki az Adatkezelőnél az adatkezelési tevékenység céljainak, kereteinek, eszközeinek meghatározásáról dönt, különösen a Vezérigazgató, a belső adatvédelmi felelős, illetve a belső ellenőr.

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

21. Az adatvédelmi tisztviselő nevét és elérhetőségeit az Adatkezelő honlapján, székhelyén, telephelyén a nyilvánosság részére mindenkor elérhetővé kell tenni.

22. Adatvédelmi tisztviselő feladatai:

    a/ ellenőrzi a GDPR, az Infotv., az ágazati jogszabályok és a jelen Szabályzat, illetve az Adatkezelő egyéb adatvédelmi vagy információszabadság tárgyú belső szabályzatainak alkalmazását és végrehajtását és ezek összhangját,

b/ tájékoztat, szakmai tanácsot ad és ellenőrzi az adatvédelemmel kapcsolatos jogszabálynak való megfelelést, különös tekintettel az egészségügyi adatok kezelésére vonatkozó szabályokra,
c/ közreműködik az Adatvédelmi Szabályzat elkészítésében, felülvizsgálatában,
d/ kivizsgálja – a belső adatvédelmi felelős és az érintett szakterületek bevonásával – a neki címzett panaszokat, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót,
e/ tanácsot ad az adatvédelmi hatásvizsgálatra és az érdekmérlegelési tesztekre vonatkozóan, valamint aktívan közreműködik ezek elvégzése során,
f/ együttműködik és kapcsolattartó pontként működik a Felügyeleti Hatóság felé az adatkezeléssel kapcsolatos ügyekben,
g/ adatvédelmi incidens esetén - amennyiben ez indokolt -, a tudomására jutástól számítva haladéktalanul, maximum 72 órán belül bejelentést tesz a Felügyeleti Hatóság (NAIH) felé,
h/ javaslatot tesz az adatvédelem, illetve az adatbiztonság területén a kifejlesztett új technológiák és eszközök alkalmazása előtt.

10. Belső adatvédelmi felelős (BAF)

23. A belső adatvédelmi felelős (BAF) feladatait a Jogi vezető látja el az alábbiak szerint:

a/ az adatvédelmi tisztviselő munkájának támogatása,
b/ aktív részvétel adatvédelmi incidensek azonosításában és kezelésében,
c/ intézményen belüli adatkezelés jogszerűségének, valamint a személyes adatok kezelésére vonatkozó jogszabályok és belső szabályozók betartásának ellenőrzése,
d/ az adatkezelésekhez esetlegesen szükséges érdekmérlegelési tesztek, illetve adatvédelmi hatásvizsgálatok elkészítése az adatvédelmi tisztviselő szakmai irányítása mellett,
e/ rendszeres időközönként áttekinti az adatvédelmi hatásvizsgálatban azonosított kockázatok alakulását, szükség esetén dokumentálja, illetve jelzi az adatvédelmi tisztviselőnek az adatkezeléssel járó kockázatok változását és az azok csökkentését célzó intézkedéseket, elvégzi, illetve közreműködik az adatvédelmi hatásvizsgálatok utóellenőrzésében és annak dokumentálásában [GDPR 35. cikk (11) bek.].
f/ adatvédelmi nyilvántartások naprakészségének felügyelete.

3. ÁLTALÁNOS ADATVÉDELMI SZABÁLYOK

11. Az adatkezelés jogszerűségének biztosítása

24. Személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak. Kizárólag olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig. Az adatokat megfelelő intézkedésekkel védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

25. Az Adatkezelő adatkezelői tevékenységét a jelen Szabályzatban foglalt okokból és célok elérése érdekében végzi. Az Adatkezelő az adatkezelés minden szakaszában biztosítja az adatok pontosságát, gondoskodik az érintett személyes adatainak védelméről jogosulatlan hozzáférés, megváltoztatás, továbbítás, törlés vagy megsemmisülés esetén.

26. A személyes adatoknak a gyűjtésük eredeti céljától eltérő egyéb célból történő kezelése csak akkor megengedett, ha az adatkezelés összeegyeztethető az adatkezelés eredeti céljaival, amelyekre a személyes adatokat eredetileg gyűjtötték. Ebben az esetben nincs szükség attól a jogalaptól eltérő, külön jogalapra, mint amely lehetővé tette a személyes adatok gyűjtését.

27. Adatkezelőnél tilos faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése. A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó személyes adatokat Adatkezelő nem kezelhet, azok kezelésére kizárólag közhatalmi szerv adatkezelésének keretében kerülhet sor.

28. Adatkezelő közhatalmi tevékenységet nem végez, a személyes adatok kezelése munkavállalókkal kapcsolatos, szerződéses partnerekkel kapcsolatos valamint szolgáltatás nyújtással kapcsolatos adatkezelés.

12. Adatkezelés bevezetésével kapcsolatos feladatok

29. Jogszabályban elrendelt vagy jogszabály rendelkezése miatt szükséges, vagy az Adatkezelő döntése alapján létrehozandó nyilvántartási rendszer (a továbbiakban együtt: **adatkezelés**) bevezetése esetén, amennyiben az a természetes személyek adatainak kezelésével (beleértve meglévő nyilvántartási rendszer adatainak új célú felhasználásával, új célú adatkezelés bevezetésével, nyilvántartási rendszerbe adatok felvételével, adatok tárolásával, harmadik személynek továbbításával stb.)

jár, az adatkezelés bevezetése során e fejezet rendelkezéseit figyelembe véve kell eljárni.

30. Új adatkezelés bevezetéséről döntéshozatalra az jogosult, aki a Szervezeti és Működési Szabályzat szerint az érintett adatkezelés alapjául szolgáló tevékenységgel kapcsolatban döntésre jogosult. A valamennyi munkavállalót és érintettett, vagy a munkavállalók és az érintettek széles körét érintő adatkezelésről döntéshozatalra az jogosult, aki az Adatkezelőnél képviseleti jogosultsággal rendelkezik.

31. A belső adatvédelmi felelőst és szükség esetén az adatvédelmi tisztviselőt az új adatkezelés bevezetésére vonatkozó igény megfogalmazásától kezdve be kell vonni az adatkezelés feltételeinek kidolgozása folyamatába.

32. Az adatkezelés feltételeinek kidolgozásában érintett szakterületek/szervezeti egységek vezetői kötelesek egymással, a belső adatvédelmi felelőssel és az adatvédelmi tisztviselővel együttműködni.

33. Az adatkezelés bevezetésével, az adatkezelés feltételeinek meghatározásával kapcsolatban
    a/ a leendő adatkezelésért a belső adatvédelmi felelős felelős, e körben:
        aa/ meghatározza az adatkezelés célját, az adatkezelés jogalapját, a kezelendő adatok körét, az adatkezelés egyéb feltételeit, és ilyen tartalmú javaslatot készít a döntésre jogosultnak [GDPR 4. cikk 7. és 16. pont];
        ab/ az aa/ alpontban meghatározott feladat részeként előterjesztést tesz a döntésre jogosultnak arról, hogy az eltérő célú adatkezelés összeegyeztethető-e az eredeti céllal, és így szolgálhat-e a tervezett adatkezelés új jogalapjául [GDPR 6. cikk (4) bek.];
        ac/ az aa/ pontban meghatározott feladat részeként, amennyiben az adatkezelés jogalapja a jogos érdek lehet, elkészíti az érdekmérlegelési tesztet és szükség esetén a hatásvizsgálatot [GDPR 6. cikk (1) bek. f) pont];
        ad/ az aa/ pontban meghatározott feladat részeként előterjesztést tesz a döntésre jogosultnak arról, hogy az adatkezelést közös adatkezelésként indokolt-e ellátni, illetve indokolt-e adatfeldolgozót bevonni;
        ae/ az aa/ pontban meghatározott feladat részeként megszövegezi a hozzájáruló nyilatkozatot [GDPR 7. cikk (2) bek.], illetve ha közös adatkezelés vagy adatfeldolgozó bevonása miatt szükséges, a megfelelő szerződéses rendelkezéseket;
        af/ megfogalmazza az új adatkezelésre, vagy a meglévő adatkezelés módosítására vonatkozó információkat és azzal kiegészíti az adatkezelésről szóló tájékoztatást [GDPR 13-14. cikk] és gondoskodik annak könnyen hozzáférhető módon való közzétételéről [GDPR 12. cikk (1) bek.];
        ag/ az adatkezelés bevezetéséről való döntést követően az Adatkezelési Nyilvántartásában rögzíti az új adatkezelést, illetve a nyilvántartott adatokban bekövetkezett valamennyi változást [GDPR 30. cikk (1) bek.].

34. A döntések, javaslatok véglegesítése előtt indokolt esetben ki kell kérni az adatvédelmi tisztviselő véleményét, úgy, hogy az adatvédelmi tisztviselőnek megelelő idő álljon rendelkezésére a vélemény adására.

35. Az adatvédelmi tisztviselő adatvédelmi jogi támogatást nyújt a belső adatvédelmi felelős által előkészített, megszövegezett, adatkezeléshez kapcsolódó dokumentumok elkészítésében és közreműködik azok véglegesítésében.

13. Dokumentálási kötelezettség

36. Az Adatkezelő felelős a személyes adatok kezelésére vonatkozó alapelvek [GDPR 5. cikk (1) bek.] betartásáért. Az Adatkezelőnek képesnek kell lennie a személyes adatok kezelésére vonatkozó alapelvek betartásának igazolására [GDPR 5. cikk (2) bek.]. A megfelelőség igazolása különösen az adatkezeléshez kapcsolódó döntéseket megalapozó körülmények és a döntések (pl. az adatkezelés feltételeit meghatározó döntéselőkészítő iratok), az érintetteknek szóló adatkezelési tájékoztatók, az érintettől származó nyilatkozatok (pl. hozzájáruló nyilatkozatok, az adatkezelési tájékoztató megismerését igazoló dokumentumok) dokumentálásával történik. Az Adatkezelő – a GDPR 30. cikkének megfelelően – adatkezelési nyilvántartást vezet.

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

14. A személyes adatok kezelésének felülvizsgálata

38. Annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, Adatkezelő a kezelt adatok körét rendszeresen felülvizsgálja.

39. A személyes adatok kezelése felülvizsgálatának koordinálása a Belső Adatvédelmi Felelős feladata.

15. Adatkezelő és a munkavállalók feladatai a megfelelő adatvédelem érdekében

Adatkezelő a megfelelő adatvédelmi tudatosság biztosítása érdekében gondoskodik a munkavállalók szakmai felkészítéséről, valamint a jelen szabályzat és a kapcsolódó dokumentumok megismertetéséről.

40. Adatkezelő mint munkáltató a jelen szabályzat rendelkezéseinek – akár súlyos gondatlansággal, akár szándékosan történő – megszegését a munkaviszonyból származó kötelezettség megszegésének tekinti.

16. Adatkezelési Nyilvántartások

41. Adatkezelési tevékenységekről adatkezelési célonként az Adatkezelő adatkezelési nyilvántartást vezet.

42. Az adatkezelési nyilvántartás valamennyi, az Adatkezelő általi adatkezelés esetén tartalmazza:
    a/ az adatkezelés célját,
    b/ az adatkezelés jogalapját,
    c/ az érintettek körét,
    d/ az érintettekre vonatkozó személyes adatok kategóriáit,
    e/ az adatok forrását (opcionális),
    f/ az adatok kezelésének időtartamát vagy az adattörlés ideje megállapításának szempontjait;
    g/ a továbbított adatok fajtáját, címzettjét és a továbbítás jogalapját, ideértve a harmadik országokba irányuló, valamint nemzetközi szervezethez történő adattovábbításokat és azok garanciáinak leírását is,
    h/ az adatfeldolgozó nevét és címét, a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét,
    i/ az alkalmazott adatfeldolgozási technológia jellegét (opcionális);
    j/ az adatkezelő, valamint közös adatkezelés esetén a közös adatkezelők megnevezését és elérhetőségét,
    k/ az adatkezelésért felelős szervezeti egység megnevezését, az adatokhoz hozzáférésre jogosult személyek körét (munkakör), (opcionális),
    l/ az adatvédelmi tisztviselő nevét és elérhetőségét,
    m/ az adatkezelés módszerét (manuális, számítógépes, vegyes),
    n/ ha lehetséges, az adatbiztonsági intézkedések általános leírását,
    o/ az archiválás módját, gyakoriságát (opcionális),
    p/ az adatbiztonsági kockázati besorolást (opcionális)
    q/ az érdekmérlegelési teszt és a hatásvizsgálati dokumentum elérhetőségét (opcionális).

43. Az adatkezelési nyilvántartás célja az Adatkezelő, mint adatkezelő adatkezelési tevékenysége átláthatóságának biztosítása, és ezzel az esetleges felesleges, párhuzamos adatkezelések elkerülése.

44. Az Adatkezelő adatkezelési nyilvántartásába való betekintést – a Felügyeleti Hatóság képviselőin kívül – az adatvédelmi tisztviselő, a belső adatvédelmi felelős, az érintett szakterület vezetői, továbbá a közös adatkezelést érintő rész tekintetében a közös adatkezelő részére biztosítja.

45. A nyilvántartásába bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezeléssel érintett szervezeti egység vezetője köteles megfelelő időn belül bejelenteni a belső adatvédelmi felelősnek, aki ennek megfelelően módosítja az adatkezelési nyilvántartás adatait.

17. Az érintetti jogok gyakorlásának általános szabályai

46. Az Adatkezelőnek elő kell segítenie az érintetti jogok gyakorlását. Adatkezelő, illetve munkavállalói gondoskodnak arról, hogy az érintett személy tájékoztatást kapjon az adatkezelés tényéről és céljairól. A tájékoztatást az adatkezelés megkezdése előtt kell megadni és a tájékoztatáshoz való jog az adatkezelés során annak megszűnéséig megilleti az érintettet.

47. Az Adatkezelőnek az érintett részére a személyes adatok kezelésére vonatkozó valamennyi információt és minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva kell nyújtania, 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. Amennyiben az adatkezelés az érintett hozzájárilásán alapul, kétség esetén az adatkezelőnek kell bizonyítania, hogy az adatkezeléshez az érintett hozzájárult.

48. Az Adatkezelő indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított 25 napon belül tájékoztatja az érintettet a jogai gyakorlására irányuló kérelme nyomán hozott intézkedésekről. E határidő a GDPR-ban írt feltételekkel további két hónappal meghosszabbítható, amelyről az érintettet tájékoztatni kell.

49. 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 Felügyeleti Hatóságnál, és élhet bírósági jogorvoslati jogával.

50. Az Adatkezelő az információkat és az érintett jogairól szóló tájékoztatást és intézkedést díjmentesen biztosítja, azonban a GDPR-ban írt esetekben díj számítható fel.

51. Az érintett jogosult arra, hogy az adatkezeléssel összefüggő tényekről és információkról az adatkezelés megkezdését megelőzően tájékoztatást kapjon [GDPR 13-14. cikk].

52. Ha az adatkezelő a személyes adatokon a megszerzésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatnia kell az érintettet erről az eltérő célról és minden releváns kiegészítő információról.

53. Az előzőekben leírtakat nem kell alkalmazni, ha és amilyen mértékben:

a/ az érintett már rendelkezik az információkkal;

b/ a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne, különösen a Rendelet 89. cikk (1) bekezdésében foglalt feltételek és garanciák figyelembevételével végzett

adatkezelés esetében, vagy amennyiben a GDPR 14. cikk (1) bekezdésében említett kötelezettség valószínűsíthetően lehetetlenné tenné vagy komolyan veszélyeztetné ezen adatkezelés céljainak elérését. Ilyen esetekben az adatkezelőnek megfelelő intézkedéseket kell hoznia – az információk nyilvánosan elérhetővé tételét is ideértve – az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében;

c/ az adat megszerzését vagy közlését kifejezetten előírja az adatkezelőre alkalmazandó uniós vagy tagállami jog, amely az érintett jogos érdekeinek védelmét szolgáló megfelelő intézkedésekről rendelkezik; vagy

d/ a személyes adatoknak valamely uniós vagy tagállami jogban előírt szakmai titoktartási kötelezettség alapján, ideértve a jogszabályon alapuló titoktartási kötelezettséget is, bizalmasnak kell maradnia

54. 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 hozzáférést kapjon (GDPR 15. cikk).

55. Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére történő továbbítására kerül sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan a GDPR 46. cikk szerinti megfelelő garanciákról.

56. Az Adatkezelőnek az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére kell bocsátania. 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 kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri. A másolat igénylésére vonatkozó jog nem érintheti hátrányosan mások jogait és szabadságait [GDPR 15. cikk].

57. Az érintett jogosult arra, hogy kérésére az Adatkezelő indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat.

58. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését is [GDPR 16. cikk].

59. 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. [GDPR 17. cikk]:

60. Ha az Adatkezelő nyilvánosságra hozta a személyes adatot, és az előbbi pont értelmében azt törölni köteles, az elérhető technológia és a megvalósítás költségeinek figyelembevételével megteszi az észszerűen elvárható lépéseket – ideértve technikai intézkedéseket – annak érdekében, hogy tájékoztassa az adatokat kezelő adatkezelőket, adatfeldolgozókat, hogy az érintett kérelmezte tőlük

a szóban forgó személyes adatokra mutató linkek vagy e személyes adatok másolatának, illetve másodpéldányának törlését.

61. Az előző két pont nem alkalmazandó, amennyiben az adatkezelés szükséges:

a/ a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;

b/ 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;

c/ a GDPR 9. cikk (2) bekezdése h) és i) pontjának, valamint a GDPR 9. cikk (3) bekezdésének megfelelően a népegészségügy területét érintő közérdek alapján;

d/ jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez [GDPR 17. cikk[.

62. Az érintett jogosult arra, hogy az Adatkezelő korlátozza az adatkezelést, ha a jogszabályban meghatározott feltételek teljesülnek [GDPR 18. cikk].

63. Az érintett jogosult arra, hogy kérésére az Adatkezelő korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:

a/ 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;

b/ az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;

c/ az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez; vagy

d/ az érintett a GDPR 21. cikk (1) bekezdése szerint tiltakozott az adatkezelés ellen; ez esetben a korlátozás arra az időtartamra vonatkozik, amíg megállapításra nem kerül, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.

64. Az adatkezelő minden olyan címzettet tájékoztat valamennyi helyesbítésről, törlésről vagy adatkezelés-korlátozásról, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az érintettet kérésére az adatkezelő tájékoztatja e címzettekről. a [GDPR 19. cikk]:

65. 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, ha

a/ az adatkezelés a GDPR 6. cikk (1) bekezdésének a) pontja vagy a GDPR 9. cikk (2) bekezdésének a) pontja szerinti hozzájáruláson, vagy a GDPR 6. cikk (1) bekezdésének b) pontja szerinti szerződésen alapul és

b/ az adatkezelés automatizált módon történik.

66. A fenti esetekben az érintett kérheti a személyes adatok adatkezelők közötti közvetlen továbbítását is.

67. Az adathordozhatóságra és továbbításra irányuló kéréseket Az Adatkezelő Vezérigazgatójának címzett kérelemben kell megfogalmazni.

68. Az adathordozhatósághoz való jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű feladat végrehajtásához szükséges. E jog nem érintheti hátrányosan mások jogait és szabadságait. [GDPR 30. cikk]:

69. Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak [GDPR 6. cikk (1) bekezdés e) pont] közérdeken, közfeladat végrehajtásán, vagy jogos érdeken alapuló kezelése ellen, ideértve az említett rendelkezéseken alapuló profilalkotást is. Ebben az esetben az adatkezelő a személyes adatokat nem kezelheti tovább, kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

70. Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett jogosult arra, hogy bármikor tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen, ideértve a profilalkotást is, amennyiben az a közvetlen üzletszerzéshez kapcsolódik. Ha az érintett tiltakozik a személyes adatok közvetlen üzletszerzés érdekében történő kezelése ellen, akkor a személyes adatok a továbbiakban e célból nem kezelhetők.

71. Ezen jogokra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni annak figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

72. Az érintett a tiltakozáshoz való jogot műszaki előírásokon alapuló automatizált eszközökkel is gyakorolhatja.

73. Ha a személyes adatok kezelésére a GDPR 89. cikk (1) bekezdésének megfelelően tudományos és történelmi kutatási célból vagy statisztikai célból kerül sor, az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozhasson a rá vonatkozó személyes adatok kezelése ellen, kivéve, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség [GDPR 21. cikk].

74. Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené [GDPR 22. cikk].

75. Ez a jogosultság nem alkalmazandó abban az esetben, ha a döntés:

a/ az érintett és az Adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges;

b/ meghozatalát az adatkezelőre alkalmazandó olyan uniós vagy tagállami jog teszi lehetővé, amely az érintett jogainak és szabadságainak, valamint jogos érdekeinek védelmét szolgáló megfelelő intézkedéseket is megállapít; vagy

c/ az érintett kifejezett hozzájárulásán alapul.

76. Az Adatkezelő köteles megfelelő intézkedéseket tenni az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, ideértve az érintettnek legalább azt a jogát, hogy az adatkezelő részéről emberi beavatkozást kérjen, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.

77. Az Adatkezelőre vagy adatfeldolgozójára alkalmazandó uniós vagy tagállami jog jogalkotási intézkedésekkel korlátozhatja jogok és kötelezettségek (GDPR 12-22. cikk, 34. cikk, 5. cikk) hatályát, ha a korlátozás tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát.

78. Az Adatkezelőre vagy adatfeldolgozójára alkalmazandó uniós vagy tagállami jog jogalkotási intézkedésekkel korlátozhatja a GDPR 12–22. cikkben és a 34. cikkben foglalt, valamint a 12–22. cikkben meghatározott jogokkal és kötelezettségekkel összhangban lévő rendelkezései tekintetében az 5. cikkben foglalt jogok és kötelezettségek hatályát, ha a korlátozás tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát, valamint az alábbiak védelméhez szükséges és arányos intézkedés egy demokratikus társadalomban:

a/ nemzetbiztonság;

b/ honvédelem;

c/ közbiztonság;

d/ bűncselekmények megelőzése, nyomozása, felderítése vagy a vádeljárás lefolytatása, illetve büntetőjogi szankciók végrehajtása, beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését;

e/ az Unió vagy valamely tagállam egyéb fontos, általános közérdekű célkitűzései, különösen az Unió vagy valamely tagállam fontos gazdasági vagy pénzügyi érdeke, beleértve a monetáris, a költségvetési és az adózási kérdéseket, a népegészségügyet és a szociális biztonságot;

f/ a bírói függetlenség és a bírósági eljárások védelme;

g/ a szabályozott foglalkozások esetében az etikai vétségek megelőzése, kivizsgálása, felderítése és az ezekkel kapcsolatos eljárások lefolytatása;

h/ az a)–e) és a g) pontban említett esetekben – akár alkalmanként – a közhatalmi feladatok ellátásához kapcsolódó ellenőrzési, vizsgálati vagy szabályozási tevékenység;

i/ az érintett védelme vagy mások jogainak és szabadságainak védelme;

j/ polgári jogi követelések érvényesítése.

79. Az előző bekezdésben említett jogalkotási intézkedések adott esetben részletes rendelkezéseket tartalmaznak legalább:

a/ az adatkezelés céljaira vagy az adatkezelés kategóriáira,

b/ a személyes adatok kategóriáira,

c/ a bevezetett korlátozások hatályára,

d/ a visszaélésre, illetve a jogosulatlan hozzáférésre vagy továbbítás megakadályozását célzó garanciákra,

e/ az Adatkezelő meghatározására vagy az Adatkezelők kategóriáinak meghatározására,

f/ az adattárolás időtartamára, valamint az alkalmazandó garanciákra, figyelembe véve az adatkezelés vagy az adatkezelési kategóriák jellegét, hatályát és céljait,

g/ az érintettek jogait és szabadságait érintő kockázatokra, és

h/ az érintettek arra vonatkozó jogára, hogy tájékoztatást kapjanak a korlátozásról, kivéve, ha ez hátrányosan befolyásolhatja a korlátozás célját [GDPR 23. cikk].

80. Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja, kivéve a jogi kötelezettség teljesítésére vonatkozó igényét. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét,

81. Az érintett jogosult arra, hogy panaszt tegyen a Felügyeleti Hatóságnál a **https://naih.hu** internetes oldalon közzétett elérhetőségeken – illetve a szokásos tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerinti tagállam Felügyeleti Hatóságnál –, ha az érintett megítélése szerint a rá vonatkozó személyes adatok kezelése jogsértő [GDPR 77. cikk].

82. A rendelkezésre álló közigazgatási vagy nem bírósági útra tartozó jogorvoslatok – köztük a Felügyeleti Hatóságnál történő panasztételhez való jog – sérelme nélkül, minden érintett hatékony bírósági jogorvoslatra jogosult, ha megítélése szerint a személyes adatainak nem a GDPR rendelkezéseinek megfelelő kezelése következtében megsértették a GDPR szerinti jogait [GDPR 79. cikk].

83. Az adatkezelővel vagy az adatfeldolgozóval szembeni eljárást az adatkezelő vagy az adatfeldolgozó tevékenységi helye szerinti tagállam bírósága előtt kell

megindítani. Az ilyen eljárás megindítható az érintett szokásos tartózkodási helye szerinti tagállam bírósága előtt is, kivéve, ha az adatkezelő vagy az adatfeldolgozó valamely tagállamnak a közhatalmi jogkörében eljáró közhatalmi szerve.

84. 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.

85. Az adatfeldolgozó abban az esetben 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.

86. 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, illetve az adatfeldolgozó mentesül a felelősség alól, ha bizonyítja, hogy a kárt előidéző eseményért őt nem terheli felelősség.

18. Az adatkezelési tevékenység nyilvánossága

87. Az Adatkezelő a honlapján egy olyan, „Adatvédelem" nevű oldalt tart fenn a **https://mupa.hu/adatvedelem** internetes címen, amely közvetlenül elérhető és nyilvános. Az „Adatvédelem" oldalon közzé kell tenni:
    a/ az Adatkezelő adatvédelmi tisztviselőjének nevét és elérhetőségeit
    b/ az Adatkezelő előzetes adatkezelési tájékoztatóját;
    c/ az általános adatvédelmi feltételeket.

88. Az Adatkezelő honlapján el kell helyezni az internetes oldalra vonatkozó
    a/ impresszumot
    b/ adatkezelési tájékoztatót
    c/ süti tájékoztatót
    d/ egyéb releváns dokumentumot

19. Gyermekek adatkezelésére vonatkozó speciális szabályok

89. Az Adatkezelő szervezeti egységeinek vezetői a belső adatvédelmi felelős közreműködésével gondoskodnak arról, hogy az Adatkezelővel kapcsolatba kerülő gyermekek az adataik kezelésével kapcsolatos tájékoztatást a gyermek számára világos és elérhető módon megkapják. A tájékoztatás az alábbi módokon történhet:
    a/ a gyermek törvényes képviselője útján: a gyermeket érintő adatkezelésről a gyermekkel kapcsolatba lépő munkavállaló írásban tájékoztatja a gyermek törvényes képviselőjét, és írásban nyilatkoztatja arra vonatkozóan, hogy a tájékoztatást közli a gyermekkel;
    b/ a gyermek vagy a törvényes képviselő kifejezett kérésére a gyermekkel kapcsolatba lépő munkavállaló – a fentieken túlmenően – biztosítja a gyermek részére a rövid, szóbeli tájékoztatást is az adatai kezelésével kapcsolatban;

c/ amennyiben a gyermek életkora és érettsége lehetővé teszi, a gyermekkel kapcsolatba lépő munkavállaló írásban közvetlenül a gyermeket is tájékoztatja az adatkezelésről. A speciális, gyermekeknek szóló tájékoztató dokumentumot az adatvédelmi tisztviselő készíti el az Adatkezelő belső adatvédelmi felelősének bevonásával. A különböző életkorú gyermekek számára a gyerekek életkorához igazodó tartalmú tájékoztató anyagot kell készíteni.

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

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

20. Közérdekű adatok megismerése iránti igényre vonatkozó általános szabályok

92. Az Adatkezelő az Infotv. 28-31.§ rendelkezéseinek megfelelően jár el a közérdekű adatok megismerése iránti igények esetében.

93. Az Adatkezelő adatvédelmi nyilvántartást vezet a közérdekű adatok megismerése iránti igényekről.

94. Az Adatkezelő az elutasított közérdekű adatigénylésekről éves jelentést készít a Felügyeleti Hatóság számára, amelyben megjelöli az elutasítás pontos indokát és körülményeit.

21. Harmadik országba irányuló adattovábbítás általános szabályai

95. Amennyiben személyes adatnak harmadik országba történő továbbításának lehetősége, vagy szükségessége merül fel, az érintett szervezeti egység köteles a belső adatvédelmi felelős és az adatvédelmi tisztviselő véleményét kérni az adattovábbítás megengedhetőségéről, illetve az adattovábbítás lehetséges módjáról.

96. A belső adatvédelmi felelős vagy az adatvédelmi tisztviselő javaslatot tesz az adattovábbítás módjára, az adatátadás során alkalmazandó biztosítékok körére.

22. Általános adatbiztonsági intézkedések (technikai és szervezési intézkedések) meghatározása és végrehajtása

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

98. Az adatbiztonsági intézkedések mindennapi működésben történő betartására az Adatkezelő minden alkalmazottja, valamint az Adatkezelő informatikai rendszereihez hozzáférő személy köteles.

99. Az Adatkezelő rendelkezik a mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási, jogi, ügyrendi intézkedések megtételéhez azon eszközökkel, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

100. A dokumentum kezelési és gazdasági rendszerekben csak az arra jogosult személy dolgozhat. Az Adatkezelő belső adatállományaihoz, valamint a géppark távmenedzseléséhez külső hozzáférést csak VPN kapcsolaton és nagyon indokolt esetben lehetséges, függetlenül a hozzáférés fizikai voltától (Internet, betárcsázás, stb). A belső hálózat védelmét tűzfalrendszer használatával kell biztosítani; valamint az Internethez történő hozzáférés csak ezen a kapcsolaton keresztül valósulhat meg a belső hálózatot használó számítógépek esetén; a programnak rendelkeznie kell a belülről kifelé és a kívülről befelé irányuló adatforgalom típusonkénti és felhasználónkénti szabályozásának tulajdonságával, valamint szét kell tudnia választani a belső és külső adatforgalmat.

101. Az Adatkezelő minden számítógépén vírusellenőrző program telepítve van, ugyanígy a szerverek és a tűzfalrendszer vírusellenőrző programmal van ellátva. A vírustámadások veszélyének minimalizálása érdekében a vírusvédelmi rendszer napi többszöri frissítése biztosítva van. Az egyes felhasználók saját felhasználónévvel és jelszóval rendelkeznek. A jelszavakat vagy a jelszófájlokat a hálózaton nyílt, olvasható formában továbbítani tilos.

102. Az Adatkezelő hálózatára számítógépet, illetve egyéb gyengeáramú berendezést kizárólag az Adatkezelő munkatársai csatlakoztathatnak. A szabályzatnak megfelelően a nem használt végpontokat, illetve aktív eszköz portokat inaktív állapotba kell helyezni.

103. A számítógépes adatállományról rendszeresen elosztottan automatikus mentés történik külső adattárolóra.

104. Az Adatkezelőben működtetett számítástechnikai rendszert folyamatosan ellenőrizni és szükség szerint bővíteni kell. A rendszer működési műszaki megbízhatóságának alapja a működéssel kapcsolatos visszajelzések és problémák hatékony kezelése.

23. Adatkezelés megszüntetésével kapcsolatos feladatok

105. Amennyiben a kezelt adatokra a továbbiakban nincs szükség (az adatkezelési cél megvalósult vagy a kezelt adatokra vonatkozó megőrzési idő letelt), vagy jogszabályi változások miatt, vagy az adatvédelmi Felügyeleti Hatóság vagy bíróság döntése értelmében az adatok kezelését meg kell szüntetni, a belső adatvédelmi felelős javaslatot tesz a döntésre jogosultnak:

a/ az adatkezelés egészének vagy egyes adatfajták nyilvántartásának megszüntetésére (az adatok archiválására a megőrzési idő leteltéig),
b/ nyilvántartási rendszer egészének vagy egyes adatfajták, illetve adatok törlésére.

4. AZ ADATKEZELŐ SZERZŐDÉSES PARTNEREIVEL, ÉS MUNKAVÁLLALÓI VAL KAPCSOLATOS ADATKEZELÉSEK SZABÁLYAI

24. A közös adatkezelői megállapodások megkötésének és végrehajtása, ellenőrzésének szabályai

106. Közös adatkezelésnek minősül, ha az adatkezelés céljait és eszközeit az Adatkezelő egy vagy több másik adatkezelővel közösen határozza meg a GDPR 26. cikk értelmében.

107. A közös adatkezelésről szóló megállapodásban meg kell határozni különösen

a/ az adatkezelés célját, a kezelendő adatok körét, az adatkezelés időtartamát, az alkalmazandó adatbiztonsági intézkedéseket, az adatkezelés egyéb feltételeit,
b/ azt, hogy a közös adatkezelésben érintett egyes adatkezelők
ba/ mely adatkezelési műveleteket (pl. hozzájáruló nyilatkozatok felvétele, adatok tárolása, adatok felhasználása stb.) végzik,
bb/ az érintett tájékoztatását hogyan végzik (pl. melyik adatkezelő készíti el az adatkezelési tájékoztatót és bocsátja az érintettek rendelkezésére stb.),
bc/ az érintett jogai gyakorlását hogyan biztosítják (pl. egyesített vagy elkülönített ügyfélszolgálat stb.),
bd/ az esetleges jogellenes adatkezelés következményeit milyen arányban viselik;
c/ az adatvédelmi incidens észlelése esetén követendő eljárást, különösen azt, hogy
ca/ az adatvédelmi incidens tudomásra jutása esetén a másik adatkezelő adatvédelmi tisztviselőjét (adatvédelmi tisztviselő hiányában a kijelölt kapcsolattartót) haladéktalanul kötelesek értesíteni az adatvédelmi rendellenességről vagy incidensről,
cb/ egymással kötelesek együttműködni az adatvédelmi rendellenesség vagy incidens okának kiderítésében és következményeinek felszámolásában,
cc/ az egyes adatkezelőket mely adatvédelmi incidensek tekintetében terheli a bejelentési kötelezettség;
d/ kijelölnek-e kapcsolattartót az érintettek számára, és ha igen, a kapcsolattartó személyét és elérhetőségét naprakészen kell tartani,
e/ a megállapodásról az érintett rendelkezésére bocsátandó összefoglalót, aminek – a GDPR 13-14. cikkeiben írtakon túl – tartalmaznia kell az adatkezelők által végzett adatkezelési műveleteket, és azt, hogy az érintett hogyan gyakorolhatja jogait a közös adatkezelés tekintetében.

108. A közös adatkezelés szükségességét a belső adatvédelmi felelős az adatkezelés bevezetéséről való döntés előkészítése részeként vizsgálja meg.

109. Amennyiben a közös adatkezelésben érintett másik adatkezelő harmadik országbeli adatkezelő, először abban a kérdésben kell dönteni, hogy a harmadik országbeli adatkezelő képes-e a GDPR-nak megfelelő adatbiztonsági követelmények teljesítésére. Amennyiben a harmadik országbeli adatkezelő nem képes a GDPR által elvárt adatbiztonsági követelmények érvényesítésére, illetve nem tud a GDPR szerinti garanciákat nyújtani a személyes adatok kezelésére, az adatkezelővel nem köthető megállapodás közös adatkezelésre.

110. Amennyiben döntés születik a közös adatkezelés bevezetéséről, a belső adatvédelmi felelős az adatvédelmi jogi megfelelőség biztosítása érdekében szükség esetén az adatvédelmi tisztviselő közreműködésével elkészíti a közös adatkezelésről szóló megállapodás tervezetét (benne a közös adatkezelőknek az érintettek számára kijelölendő kapcsolattartójának kijelölésével kapcsolatos döntést, valamint a közös adatkezelésre vonatkozó megállapodásnak az érintettek rendelkezésére bocsátható lényegi elemeit) és azt felterjeszti a szerződés megkötésére jogosult személynek.

111. A belső adatvédelmi felelős a közös adatkezelői megállapodás megkötését követően – az adatkezelések nyilvántartására vonatkozó szabályok szerint – e tényt és a további adatkezelő(k) adatait (név és cím, kapcsolattartó neve és elérhetősége) rögzíti az adatvédelmi nyilvántartásban.

25. Adatfeldolgozói szerződések megkötésének és végrehajtása ellenőrzésének szabályai

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

113. Az adatfeldolgozóval kötendő szerződésben

a/ a kellő részletességgel (pl. szabályzatra vagy szabványokra utalással) meg kell határozni az adatfeldolgozó, vagy az adatfeldolgozó által igénybe veendő további adatfeldolgozó által betartandó adatbiztonsági szabályokat, amelyek nem lehetnek kevésbé szigorúak, mint az Adatkezelő által alkalmazott adatbiztonsági intézkedések, és az adatfeldolgozónak az adatbiztonsági intézkedések végrehajtásával kapcsolatos feladatait;

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

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

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

cb/ köteles együttműködni az Adatkezelő adatvédelmi tisztviselőjével és más közreműködő szervezeti egységgel az adatvédelmi incidens okának feltárásban és következményeinek felszámolásában,

cc/ köteles együttműködni az adatvédelmi incidens bejelentésének teljesítésében,

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

114. Az adatfeldolgozó igénybevételének szükségességét a belső adatvédelmi felelős az adatkezelés bevezetéséről való döntés előkészítése részeként vizsgálja meg. Ezt a szabályt kell alkalmazni akkor is, ha az adatfeldolgozó igénybevételéről az adatkezelés folyamán születik döntés.

115. Amennyiben döntés születik az adatfeldolgozó igénybevételéről, a belső adatvédelmi felelős az adatvédelmi jogi megfelelőség biztosítása tekintetében szükség esetén az adatvédelmi tisztviselő közreműködésével előkészíti az adatfeldolgozóval kötendő szerződés tervezetét és azt felterjeszti a szerződés megkötésére jogosult személynek.

116. A belső adatvédelmi felelős az adatfeldolgozói szerződés megkötését követően – az adatkezelések nyilvántartására vonatkozó szabályok szerint – az adatfeldolgozó adatait (név és cím, kapcsolattartó neve és elérhetősége) rögzíti az adatvédelmi nyilvántartásban.

26. A munkavállalók személyes adatainak kezelésére vonatkozó különleges szabályok

117. A munkaviszony létesítését megelőzően csak olyan személyes adatok kezelésére kerül sor, amelyek az érintettnek az adott munkakörre való alkalmassága vonatkozásában lényeges információkat tartalmaz.

118. Amennyiben döntés született arról, hogy munkaviszony létesítésére nem kerül sor, az Adatkezelő az érintett személyes adatait törli.

119. Adatkezelő a munkaviszonnyal összefüggő adatokat a szerződés teljesítése érdekében törvény felhatalmazása, a nem jogszabály előírása alapján kezelt személyes adatokat az érintett hozzájárulása alapján kezeli.

120. A munkavállalótól csak olyan nyilatkozat megtétele vagy adat közlése kérhető, amely a személyiségi jogait nem sérti, és a munkaviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges.

121. Adatkezelő a munkavállaló számára csak munkaviszonyra vonatkozó jogszabályban előírt alkalmassági vizsgálatot ír elő.

122. Adatkezelő a munkaviszony megszűnése után a jogszabályban meghatározott adatokat az ott meghatározott ideig tárolja.

123. A munkaviszony megszűnésével összefüggésben Adatkezelő kizárólag jogszabályban előírt igazolásokat és minősítéseket készít. A fentieken túlmenően az érintettre vonatkozó további értékelést, minősítést Adatkezelő kizárólag az érintett erre irányuló kifejezett kérése esetén készít.

124. Adatkezelő a munkaviszonyból származó vagy azzal összefüggő igények elévülésének időtartamáig kezeli azokat az adatokat, amelyek felhasználása egy esetleges későbbi jogvitában szükséges lehet.

5. AZ ADATKEZELŐ SZOLGÁLTATÁSÁHOZ KAPCSOLÓDÓ ADATKEZELÉSEK ÁLTALÁNOS SZABÁLYAI

27. A szolgáltatás nyújtása során kezelt személyes adatok

125. Az Adatkezelő az alapító okiratának rendelkezésein alapuló szolgáltatás biztosítása érdekében és annak során kezel érintetti személyes adatokat.

126. A Szabályzat ezen fejezetének célja az Adatkezelő közfeladatainak ellátása, működése során kezelt valamennyi személyes adat, illetve különleges személyes adat védelme, kiemelten a rendezvények szervezése és lebonyolítása, illetve az ezzel kapcsolatos iratkezelés során.

127. Az Adatkezelő a GDPR 6. cikk szerinti jogalapokra hivatkozva pontosan meghatározott adatkezelési célok elérése érdekében kezel személyes adatokat. Az önkéntes hozzájáruláson alapuló adatkezelések esetében az érintettek e hozzájárulásukat az adatkezelés bármely szakában visszavonhatják, kivéve amennyiben a jogszabály, vagy a vonatkozó érdekmérlegelési tesztek alapján az Adatkezelő ezt megtagadhatja. Bizonyos esetekben a megadott adatok egy körének kezelését, tárolását, továbbítását jogszabályok teszik kötelezővé.

128. Az Adatkezelőnél végzett adatkezelés célja az Adatkezelő alapító okiratában közfeladatként megjelölt **előadó-művészet**, **múzeumi tevékenység** és **kultúrális tevékenység** biztosítása.

129. Az Adatkezelő által kezelt szerződések és egyéb a működés során keletkezett, dokumentumok tárolásának, megsemmisítésének és archiválásának részletes szabályaitaz Adatkezelő hatályos Iratkezelési Szabályzata határozza meg, függetlenül azok formátumától.

130. Az Adatkezelő tevékenységének gyakorlása során felvett adatokat nyilván kell tartani. A nyilvántartás eszköze lehet minden olyan eszköz, vagy módszer, amely biztosítja az adatok megfelelő védelmét.

131. Az Adatkezelő tevékenysége során keletkező egyéb érintetti adatok (jegyvásárlók adatai, regisztrált felhasználók, Müpa+ hűségprogram tagok adtai, stb.) felvételére, kezelésére, törlésére vonatkozó részletes szabályokat, a jelen Szabályzattal összhangban, az Adatkezelő Adatkezelési Tájékoztatója tartalmazza. Az Adatkezelési Tájékoztató elérhető az Adatkezelő saját honlapján

működtetett aloldalán a **https://www.mupa.hu/adatvedelem** internet címen. Az Adatkezelő az adkezeléssel kapcsolatos igényeket, illetve észrevételeket elsődlegesen az **adatvedelem@mupa.hu** e-mail címen keresztül fogadja.

132. Az Adatkezelő feladata, hogy a dokumentum kezelési és informatikai rendszer fejlesztése és működtetése során biztosítsa az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát; meghatározza az egyes folyamatok tekintetében az egyes szereplők kötelezettségeit, valamint az ellenőrzésre jogosultak körét.

6. AZ ADATVÉDELMI INCIDENSEKRE VONATKOZÓ ÁLTALÁNOS SZABÁLYOK

28. Az adatvédelmi incidens minősítése

133. Adatvédelmi incidens csak akkor következik be, ha az adatbiztonság – akár vétlen, akár szándékos – sérülésével jár és bekövetkezik a személyes adatok véletlen vagy jogellenes megsemmisítése, elvesztése, megváltoztatása, jogosulatlan közlése vagy az azokhoz való jogosulatlan hozzáférés.

134. Az adatvédelmi incidensre vonatkozó szabályokat kell alkalmazni az Adatkezelő elektronikus információs rendszereiben vagy tulajdonát képező adathordozón, mobiltelefonon, laptopon, egyéb számítástechnikai eszközön tárolt adatokra, továbbá az Adatkezelő alkalmazottainak olyan saját tulajdonú eszközein (adathordozó, mobiltelefon, laptop, egyéb számítástechnikai eszköz) tárolt adatokra, amely eszközöket munkavégzéshez, munkaköri feladatok ellátásához, munkavégzés céljából használhat. Az adatvédelmi incidensre vonatkozó szabályokat az Adatkezelő birtokában lévő papíralapú adathordozón lévő adatokra is alkalmazni kell.

135. Az adatvédelmi incidenseket az Adatkezelő három kategóriába sorolja

- 1. kategória: valószínűsíthetően kockázattal nem járó incidens
- 2. kategória: valószínűsíthetően alacsony kockázattal járó incidens
- 3. kategória: valószínűsíthetően magas kockázattal járó incidens.

136. Az adatvédelmi incidens értékelésének szempontjai:

- az incidens típusa (bizalmassági, sértetlenségi-integritási vagy elérhetőségi-rendelkezésre állási),
- a személyes adatok jellege (személyes adat / különleges kategória),
- az érintett személyek száma,
- a személyes adatok száma,
- az érintett természetes személyek kategóriái,
- az érintett természetes személyek azonosíthatósága,

- a természetes személyre nézve fennálló következmények valószínűsége és súlyossága;
- az érintett adatkezelés jogalapja.

137. Az incidens értékelése során az alábbi konkrét szempontokat kell figyelembe venni:

- az incidensben érintett adatok között találhatóak a személyes adatok különleges kategóriáiba eső adatok,
- az incidensben érintett természetes személyek száma meghaladja a 100 főt,
- az incidensben érintett személyes adatok száma meghaladja a 100 darabot,
- az incidensben érintett természetes személyek között találhatóak 16. életévüket be nem töltött természetes személyek,
- az incidensben érintett személyes adatok alkalmasak az érintettel történő közvetlen kapcsolatfelvételre (így különösen lakcím, telefonszám, e-mail cím),
- az incidensben érintett adatkezelés jogalapja az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme,
- az incidensben érintett adatkezelés jogalapja közérdekű vagy közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtása,
- az incidensben érintett adatkezelés jogalapja az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítése,
- a személyes adatok alkalmasak az érintett természetes személy személyazonosságának ellopására vagy a személyazonosságával való visszaélésre,
- az incidensben érintett személyes adatok alkalmasak arra, hogy pénzügyi veszteséget okozzanak az érintettjüknek.

138. Az incidenst az „1. kategória: valószínűsíthetően kockázattal nem járó incidens"-nek kell minősíteni, ha:

- a fenti pontban felsorolt feltételek közül legfeljebb egy áll fenn és
- az adatkezelő képes annak bizonyítására, hogy az érintett személyes adatokat megfelelő adminisztratív és/vagy fizikai és/vagy logikai védelemmel látta el, ,
- a védelem sérülése helyreállítható azonnal és
- az érintetettekre, az érintett személyes adatokra vonatkozóan az incidens nem jár kockázattal.

139. Az incidenst a „2. kategória: valószínűsíthetően alacsony kockázattal járó incidens"-nek kell minősíteni, ha:

- a fenti pontban felsorolt feltételek közül legfeljebb kettő áll fenn és
- az adatkezelő képes annak bizonyítására, hogy az érintett személyes adatokat megfelelő adminisztratív és/vagy fizikai és/vagy logikai védelemmel látta el, ,
- a védelem sérülése helyreállítható rövid időn belül és
- az érintetettekre, az érintett személyes adatokra vonatkozóan az incidens alacsony kockázattal jár.

140. Az incidens a „3. kategória: valószínűsíthetően magas kockázattal járó incidens"-nek kell minősíteni, ha:

- a fenti pontban felsorolt feltételek közül legalább kettő áll fenn és
- az adatkezelő nem képes annak bizonyítására, hogy az érintett személyes adatokat megfelelő adminisztratív és/vagy fizikai és/vagy logikai védelemmel látta el,
- a védelem sérülése nem állítható helyre rövid időn belül és
- az érintetettekre, az érintett személyes adatokra vonatkozóan az incidens magas kockázattal jár.

Abban az esetben, ha a kockázat besorolására az Európai Adatvédelmi Testület útmutatást ad ki, az adatkezelő a kockázati besorolást módosítja.

29. Az adatvédelmi incidens észlelése

141. Az a munkavállaló, aki az Adatkezelő által kezelt vagy feldolgozott személyes adatokkal kapcsolatban, vagy az Adatkezelő szerződéses partnere által kezelt vagy feldolgozott személyes adataival kapcsolatban adatvédelmi incidenst vagy annak gyanúját észleli, köteles azt haladéktalanul bejelenteni a belső adatvédelmi felelősnek, aki értesíti az adatvédelmi tisztviselőt.

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

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

144. Amennyiben a bejelentő nevének elhallgatását kéri, úgy az eljárás folyamatában biztosítani kell adatainak a zárt kezelését, amelyet csak irányítási jogköre alapján a Vezérigazgató, valamint a belső adatvédelmi felelős és az adatvédelmi tisztviselő ismerhet meg.

145. A bejelentést tevő személlyel szemben nem alkalmazható semmiféle hátrányos elbánás, jelentéséért – kivéve a szándékosan valótlan tartalommal megtett jelentést – felelősségre nem vonható.

146. Külső ellenőrzési szerv által észlelt szabálytalanságra vonatkozó megállapításait az általa készített dokumentáció tartalmazza.

147. Amennyiben külső személy jelzi az adatvédelmet sértő eseményt, a bejelentést az azt rögtzítő szervezeti egység vezetőjének és a belső adatvédelmi felelősnek az adatvédelmi tisztviselő bevonásával érdemben kell megvizsgálnia.

148. Amennyiben az adatvédelmi incidens érinti az informatikai rendszert is, akkor az adatvédelmi tisztviselő az adatvédelmi incidens kivizsgálásába bevonja az Informatikai vezetőt is.

149. A bejelentés érkezését követően az adatvédelmi tisztviselő – a belső adatvédelmi felelős és az érintett szervezeti egységek bevonásával – haladéktalanul megkezdi az adatvédelmi incidens kivizsgálását és értékelését. A kivizsgálásban és értékelésben valamennyi érintett szervezeti egység együttműködni köteles.

30. Az adatvédelmi incidens kivizsgálása

150. Az adatvédelmi tisztviselő a Belső adatvédelmi felelőssel együttműködve megvizsgálja a jelentést és amennyiben szükséges, a bejelentőtől, lletve az érintett szervezeti egységek vezetőitől, munkatársaitól további adatokat kér az incidensre vonatkozóan.

151. Az adatvédelmi tisztviselő az alábbi információkat (amennyiben azok a jelentésből nem derülnek ki) lehetőségéhez mérten köteles felderíteni:

- az adatvédelmi incidens bekövetkezésének időpontja és helye,
- az adatvédelmi incidens által érintett adatok köre,
- az adatvédelmi incidenssel érintett személyek köre és száma.

152. Ezen adatokból az adatvédelmi tisztviselő összegzést készít az adatvédelmi incidens várható hatásairól és cselekvési tervet készít a következményeinek enyhítése érdekében, az érintett szakterületek szakmai véleményei és javaslatai figyelembe vételével.

153. Az adatvédelmi tisztviselő jogosult munkájába bevonni az adatvédelmi incidenssel érintett szervezeti egységek vezetőit és munkatársait, akik kötelesek együttműködni az adatvédelmi tisztviselővel.

154. A vizsgálatot legkésőbb az adatvédelmi tisztviselőhöz érkezéstől számított 48 órán belül be kell fejezni. A vizsgálat eredményéről és a tervezett további feladatokról az adatvédelmi tisztviselő a vizsgálat befejezésével egyidejűleg tájékoztatja az adatkezelő vezérigazgatóját.

155. A vizsgálattal kapcsolatos eseményekről emlékeztetőt, a döntésekről indoklást is tartalmazó jegyzőkönyvet, vizsgálat alapján intézkedési javaslatokat is tartalmazó jelentést kell készíteni. A vizsgálat során keletkezett dokumentumok kezelésére az Adatkezelő mindenkori iratkezelési szabályai az irányadók.

156. Az adatvédelmi incidensről a belső adatvédelmi felelős haladéktalanul értesíti az Adatkezelő Vezérigazgatóját.

157. A bejelentés vizsgálata során az alábbi szempontokat kell figyelembe venni:

a) a bejelentés személyes adatot érint-e,
b) amennyiben a bejelentés személyes adatot érint, megállapítható-e a személyes adatok köre,
c) megállapítható-e az incidensben érintett személyek köre,
d) a hatályos jogszabályok és belső szabályok alapján megállapítható-e, hogy személyes adat jogellenes kezelése vagy feldolgozása (beleértve a törlést/megsemmisítést is) történt,
e) melyek az adatvédelmi incidensből eredő, valószínűsíthető következmények,
f) az Adatkezelő által alkalmazott technikai és szervezési védelmi intézkedések az incidensben érintett személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik-e az adatokat.

158. Ha a bejelentés vizsgálata azzal az eredménnyel jár, hogy az adatvédelmi incidens nem érintett személyes adatokat, akkor a vizsgálatot le kell zárni.

159. Az adatvédelmi tisztviselő és a Belső Adatvédelmi felelős javaslata alapján a Vezérigazgató legkésőbb annak kézhezvételét követően haladéktalanul dönt a GDPR 33. cikkében írt adatvédelmi Felügyeleti Hatósági bejelentés szükségességéről. A Vezérigazgató döntéséről haladéktalanul értesíti az adatvédelmi tisztviselőt.

160. Amennyiben az adatvédelmi tisztviselő a vizsgálat során úgy ítéli meg, hogy azonnali intézkedések szükségesek annak biztosítására, hogy az adatvédelmi incidenssel azonos problémaforrásból eredő incidens a jövőben ne valósuljon meg, úgy a szükséges intézkedések megtétele érdekében haladéktalanul tájékoztatja a Vezérigazgatót és az érintett szervezeti egységek vezetőit.

161. A vizsgálatról szóló jelentést az Adatkezelő Vezérigazgatójának kell megküldeni.

162. A jelentés alapján a vizsgálatban érintett szervezeti egységek vezetői 5 munkanapon belül a megvalósításhoz szükséges határidőre tett javaslatot is tartalmazó intézkedési tervet készítenek, és azt megküldik a belső adatvédelmi felelős útján az adatvédelmi tisztviselőnek.

163. Az intézkedési tervet és a megvalósításhoz szükséges határidőt tartalmazó javaslatot az adatvédelmi tisztviselő a belső adatvédelmi felelőssel együttműködve a kézhezvételtől számított 3 munkanapon belül véleményezi, majd jóváhagyásra megküldi a Vezérigazgató részére.

164. Az adatvédelmi incidens elhárítása és a további incidensek megelőzése céljából megvalósított egyes intézkedésekről az incidenssel érintett szervezeti egység vezetője tájékoztatást küld a belső adatvédelmi felelős és az adatvédelmi tisztviselő, valamint a Vezérigazgató részére részére.

31. Az érintett tájékoztatása a súlyos adatvédelmi incidensről

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

166. Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább az alábbi információkat és intézkedéseket:

a) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
b) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
c) az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

167. Az érintettet nem kell tájékoztatni, amennyiben az incidens nem jár magas kockázattal, és a következő feltételek bármelyike teljesül:

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

168. Az Adatkezelő Vezérigazgatójának döntése alapján az Adatkezelő az érintetteket az Adatkezelő honlapján vagy országos lefedettségű sajtótermékben közzétett hirdetmény útján is értesítheti.

32. Az adatvédelmi incidens bejelentése a Felügyeleti Hatóságnak

169. Az adatvédelmi incidensről elsősorban a Felügyeleti Hatóság által a **https://naih.hu/adatvedelmi-incidensbejelento-rendszer** internetes oldalon működtetett elektronikus adatvédelmi incidens bejelentő rendszeren - üzemzavar esetén a bejelentő űrlap elektronikus levél formájában történő elküldésével - kell a bejelentést megtennie az adatvédelmi tisztviselőnek, ennek akadályoztatása

esetén a bejelentés elküldését és átvételét bizonyítható módon kell a Felügyeleti Hatóságrészére az incidens észlelését követő legkésőbb 72 órán belül megküldeni.

170. Amennyiben nem lehetséges az összes információt egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

171. Az adatvédelmi incidensről szóló bejelentéshez szükséges információkat az adatvédelmi tisztviselő rendelkezésére kell bocsátani.

172. Az adatvédelmi incidensről szóló bejelentéshez a Felügyeleti Hatóság elektronikus űrlapját kell használni, különös tekintettel az alábbiakra:

a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
d) ismertetni kell az Adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.
e) Ha nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

33. Az adatvédelmi incidensek nyilvántartása

173. Az adatvédelmi incidensekről az adatvédelmi tisztviselő a belső adatvédelmi felelőssel együttműködve adatvédelmi nyilvántartást vezet.

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

34. Jogkövetkezmények alkalmazása

175. A jogkövetkezményekről való döntés a Vezérigazgató feladata.

176. A jogkövetkezmény jellege szerint lehet:

a) jogi jellegű (kártérítési eljárás megindítása, szabálysértési vagy büntetőeljárás kezdeményezése az arra hatáskörrel rendelkező hatóságnál),
b) munkajogi (figyelmeztetés, munkaviszony felmondással, azonnali hatállyal történő megszüntetése),
c) pénzügyi jellegű (pénzbeli juttatás, kifizetés részben vagy egészben történő felfüggesztése, visszakövetelése, behajtása),

d) szakmai jellegű (belső szabályozás módosítása, szigorításának kezdeményezése, betartásának fokozott ellenőrzése stb.).

177. Amennyiben büntető- vagy szabálysértési eljárás kezdeményezésének szükségessége merül fel, a szükséges intézkedések meghozatala az arra illetékes szervek értesítését is jelenti annak érdekében, hogy megalapozottság esetén az illetékes szerv a megfelelő eljárásokat megindítsa. Az eljárások megindításának kezdeményezésére a Vezérigazgató jogosult.

178. Ha nyilvánvalóvá vált, hogy az adatvédelmet sértő eseményt bejelentő rosszhiszeműen járt el és alaposan feltehető, hogy ezzel bűncselekményt vagy szabálysértést követett el, másnak kárt vagy egyéb jogsérelmet okozott, adatai az eljárás kezdeményezésére, valamint lefolytatására jogosult részére átadhatók.

7. ADATKEZELÉS SORÁN ALKALMAZANDÓ MÓDSZERTANOK

35. Az érdekmérlegelési teszt elvégzésének módszertana

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

180. Az érdekmérlegelési tesztet a belső adatvédelmi felelős végzi el. Az érdekmérlegelési tesztet írásban kell elvégezni. Az elkészült dokumentumot az adatvédelmi tisztviselőnek kell megküldeni, aki azt szakmai szempontból véleményezi. A jogos érdeken alapuló adatkezelés kizárólag az érdekmérlegelési teszt elvégzését és az adatvédelmi tisztviselő véleményének beszerzését követően kezdhető meg.

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

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

f/ a személyes adatok védelme biztosítékainak leírása, garanciák beépítése az adatkezelés folyamatába
g/ az érdekmérlegelési teszt eredménye.

36. Az adatvédelmi hatásvizsgálat elvégzésének módszertana

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

184. A hatásvizsgálat elvégzésének szükségességéről a belső adatvédelmi felelős szükség esetén kikéri az adatvédelmi tisztviselő véleményét.

185. A hatásvizsgálat elvégzését a belső adatvédelmi felelős koordinálja. A hatásvizsgálat megállapításait írásban kell rögzíteni. Az elkészült hatásvizsgálati dokumentációt szükség esetén az adatvédelmi tisztviselőnek kell megküldeni, amely azt 8 munkanapon belül szakmai szempontból véleményezi. Ha a belső adatvédelmi felelős úgy ítéli meg, hogy az adatkezelés nem jár magas kockázattal a természetes személyek jogaira, úgy ezt meg kell indokolnia és – ha ez lehetséges – dokumentumokkal igazolnia a mellőzés okait. A bevezetendő adatkezelés kizárólag a hatásvizsgálat elvégzését követően kezdhető meg.

186. Adatvédelmi hatásvizsgálatot a GDPR 35. cikk (3) bekezdésében, illetve a Nemzeti Adatvédelmi és Információszabadság Hatóság által közzétett jegyzékben[1] szereplő adatkezelések, adatkezelési műveletek esetén kell végezni.

187. A fenti eseteken túl minden olyan bevezetésre kerülő – különösen az új technológiákat alkalmazó – adatkezelés esetén is hatásvizsgálatot kell végezni, mely adatkezelés az ügyfélre tekintettel jelentős joghatással bír/az ügyfelet (jogait) jelentős mértékben érinti.

188. A hatásvizsgálat módszertanát minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani. Egy lehetséges módszertant alkalmazó szoftver található a Nemzeti Adatvédelmi és Információszabadság Hatóság honlapján (https://naih.hu/adatvedelmi-hatasvizsgalati-szoftver.html).

189. A hatásvizsgálat első részében összefoglalóan le kell írni a tervezett adatkezelést, különösen:
a/ az adatkezelésért felelős szervezeti egységet és a tervezett közös adatkezelő vagy adatfeldolgozó megjelölését;
b/ az adatkezelés jogalapját, célját (az adatkezeléstől várt előnyöket, az adatkezelés szükségességét), terjedelmét (időben és a kezelt adatok volumenében);

[1] https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf

c/ az adatkezeléssel érintettek körét, a kezelendő adatok körét, az adatok megőrzésének tervezett idejét,
d/ azon adatkezelők megjelölését, akiknek az adatot továbbítani tervezik, és különösen, ha harmadik országba vagy nemzetközi szervezet felé tervezik az adattovábbítást;
e/ az adatkezelésre vonatkozó követelmények (jogszabályi követelmények vagy magatartási kódexből, szabványból eredő követelmények);
f/ az adatkezelés folyamatának a leírását.

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

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

192. A hatásvizsgálat negyedik része tartalmazza a tervezett adatkezelés értékelését:
a/ a fentiekben meghatározott szempontok értékelését a tekintetben, hogy azok egyenként megfelelőek, további intézkedésekkel megfelelőek lehetnek, illetve nem megfelelőek;
b/ a tervezett kiegészítő intézkedések végrehajtásának ütemtervét;
c/ annak egyértelmű rögzítését, hogy a tervezett adatkezelés valószínűsíthetően magas kockázattal jár-e a természetes személyek jogaira nézve, és ennek alapján az adatkezelés megkezdhető-e, illetve szükség van-e az adatvédelmi felügyeleti hatósággal való konzultációra.

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

8. ZÁRÓ RENDELKEZÉSEK

194. Jelen Szabályzat a kiadásának napján lép hatályba.

195. Jelen Szabályzat hatálybalépésével ***hatályát veszti a 2018. május 25-én hatályba lépett Adatvédelmi Szabályzat***.

196. Jelen Szabályzattal együtt értelmezendő és alkalmazandó azok a mindenkori dokumentumok és további szabályzatok és utasítások, amelyek az adatkezeléshez hozzájáruló írásbeli nyilatkozatot tartalmazzák, illetve a kötelező adatkezelési tájékoztatót írják le.

Budapest, 2023. május 8.

Müpa Budapest Nonprofit Kft.