A HOSSZÚSÉTATÉRI ÓVODA ÉS A HOSSZÚSÉTATÉRI ÓVODA TÓVÁROSI TAGÓVODÁJÁNAK

ADATKEZELÉSI- ÉS ADATVÉDELMI SZABÁLYZATA

Hatályos: 2020. február 03. napjától
Az adatkezelési és adatvédelmi szabályzat a kihirdetést követő napon lép hatályba, ezzel egyidejűleg a 2018.05.25. napján kelt adatvédelmi szabályzat hatályát veszti. Jelen szabályzat kihirdetésének módja: kifüggesztés. A kifüggesztés helye: intézményvezetői iroda.

Adatkezelő: Hosszúsétatéri Óvoda
Székhely: 8000 Székesfehérvár, Hosszúsétatér 42.
E-mail cím: postmaster@hosszuovi.t-online.hu
Telefonszám: 22/313-807
Adószám: 16700091-2-07
Képviselő: Tóth Ildikó telefon: 22/313-807

Hosszúsétatéri Óvoda Tóvárosi Tagóvodája
Cím: 8000 Székesfehérvár, Tóvárosi lakónegyed 70.
E-mail cím: postmaster@tovarosiovoda.t-online.hu
Telefon: 22/506-223
Adószám: 16700091-2-07
Tagóvoda vezető: Rácz Beatrix telefon: 22/506-223
Képviselő: Tóth Ildikó telefon: 22/313-807 továbbiakban: intézmény

Adatvédelmi tisztviselő: dr. Kozma Gergely e.v. 52286010, www.adatorom.hu, info@adatorom.hu, 06-30-3889943

Székesfehérvár, 2020. január 31.

……
Tóth Ildikó óvodaigazgató
Hosszúsétatéri Óvoda

Tartalom

MELLÉKLETEK

PREAMBULUM

(1) A **Hosszúsétatéri Óvoda és a Hosszúsétatéri Óvoda Tóvárosi Tagóvodája** (továbbiakban: intézmény) tevékenysége során elkötelezett az adatvédelmi és adatbiztonsági előírások betartása iránt. 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 (a továbbiakban: GDPR), valamint az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: infotv.) mindenkor hatályos szabályain túl az intézmény vezetője kiadja jelen adatvédelmi és adatbiztonsági szabályzatot (továbbiakban: szabályzat). A szabályzat az elfogadást követő naptól hatályba lép, és az intézmény alkalmazottjaival, az intézménnyel szerződéses kapcsolatban állókkal az őket érintő terjedelemben meg kell ismertetni.

(2) Az adatkezelési- és adatvédelmi szabályzat (a továbbiakban: Szabályzat) előírásai az Intézménye egészére, minden szervezeti egységére, az adminisztratív és technikai ügyintéző szervezetének minden munkatársára, valamint az óvodai nevelési-gondozási feladatokat személyesen ellátókra is kötelezők.

(3) Az intézmény felügyeleti szerve: Székesfehérvár Megyei Jogú Város Önkormányzat Közgyűlése, mint fenntartó látja el az intézmény irányítását, jóváhagyja és ellenőrzi a költségvetést és annak végrehajtását, az óvodaigazgató esetében gyakorolja a foglalkoztatói jogokat.

(4) Az intézmény alaptevékenysége: a Nkt. szerint köznevelési feladatot ellátó intézmény.

(5) Az intézmény köznevelési feladatai:

a) Óvodai nevelés
b) A többi gyermekkel együtt nevelhető sajátos nevelési igényű gyermekek óvodai nevelése: akik a szakértői bizottság szakértői véleménye alapján beszédfogyatékos, vagy egyéb pszichés fejlődési zavarral (súlyos tanulási, figyelem-vagy magatartásszabályozási zavarral) küzdenek.
c) Azoknak a sajátos nevelési igényű gyermekeknek az óvodai ellátása, akik a többi gyermekkel nem foglalkoztathatók együtt: akik a szakértői bizottság szakértői véleménye alapján beszédfogyatékossággal küzdenek.

(6) Az intézmény szakágazati besorolása:
Óvodai nevelés

(7) Az intézmény szakfeladat szerinti tevékenysége:
Óvodai nevelés, ellátás
Sajátos nevelési igényű gyermekek óvodai nevelése, ellátása

Óvodai intézményi étkeztetés
Nem lakóingatlan bérbeadása, üzemeltetése

(8) A beszédfogyatékos gyermekek nevelése és oktatása az e célra létrehozott csoportban és integráltan is zajlik.

(9) Szabad kapacitás kihasználása érdekében végzett alaptevékenység:
Egyéb oktatást kiegészítő tevékenység

(12) Az intézmény informatikai eszközei, hálózatának üzemeltetésében esetileg megbízott informatikus teljesít feladatokat (szerverépítés, szoftvertelepítés, konfigurálás, hibaelhárítás, biztonsági ellenőrzés). Az intézmény gondoskodik megfelelő vírusvédelemről, tűzfalról, biztonsági mentésekről, szünetmentes működésről. Az informatikai eszközöket jelszó, az intézmény titkosított hordozható informatikai eszközöket alkalmaz.

(13) Az intézmény az ellátása alá tartozó gyermekeket, szüleiket, munkatársait, illetve a vele bármilyen jogviszonyban álló személyeket nem kategorizálja, nem minősíti, ilyen célból adatot nem kezel.

(14) Az adatvédelmi elveknek a GDPR 25. cikk alapján az intézmény valamennyi tevékenysége, döntése során érvényesülnie kell, az intézmény törekszik arra, hogy a lehetőségekhez képest olyan adatvédelmi informatikai megoldást, szervezeti szabályozást alkalmazzon, amely az adatok védelmét a tudomány és technika állása szerint a leghatékonyabban biztosítja.

(15) Az intézmény valamennyi adatvédelmi folyamatának szabályozottnak, átláthatónak, nyomon követhetőnek, konkrét munkakörhöz rendelhetőnek kell lennie.

(16) Az intézmény törekszik arra, hogy amennyiben meghatározott cél elérése személyes adat kezelése nélkül is elérhető, úgy ne kezeljen személyes adatot.

(17) Az intézmény az alkalmazotti tevékenységét úgy szervezi meg, hogy lehetőleg minél kevesebb alkalmazott kezeljen személyes adatokat, a személyes adatot kezelő alkalmazott pedig a személyes adatok egy csoportját kezelje (pl. személyügyi adatok, kifizetéshez kapcsolódó adatok, ügyfélkapcsolati adatok).

I. **RÉSZ**

Általános rendelkezések

1. A szabályozás célja

1. Az Intézmény tevékenységének ellátása során személyes adatokat kezel egyrészről: a közalkalmazottak, az alkalmazottak, ill. a szerződéses kapcsolatban együttműködő megbízottak/egyéb partnerek személyes adatait, az intézménybe beíratott kiskorú gyermekek és szüleik, nevelőik személyes adatait; másrészről: ügyfelek, partnerek, együttműködő óvodák, illetve oktatási intézmények és közintézmények képviseletében eljáró természetes személyek személyes adatait.

2. A Szabályzat célja, hogy az Intézmény a rá vonatkozó, a mindenkor hatályos jogszabályokkal, EU rendeletekkel összhangban, azok előírásai szerint vezesse nyilvántartásait, végezze esetleges statisztikai adatgyűjtési, adatfeldolgozási, információszolgáltatási tevékenységét; kezelje az Intézmény birtokában levő személyes adatokat. Az Intézmény az adatkezelése és feldolgozása során olyan fokozott gondossággal jár el, amely az adatvédelmi incidensek előfordulásának megelőzését szolgálja. A szabályzat célja továbbá, hogy az intézmény tevékenysége során a személyes adatok védelméhez fűződő adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározásra kerüljenek az adatvédelmi és adatbiztonsági előírások, továbbá az érintettek jogai megfelelően biztosítva legyenek.

3. A szabályzat célja azon belső szabályok megállapítása és intézkedések megalapozása, amelyek biztosítják, hogy az intézmény adatkezelő és adatfeldolgozó tevékenysége megfeleljen a következő jogszabályoknak:

– 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; angol megnevezése: GDPR (General Data Protection Regulation);
- Magyarország Alaptörvénye;
- 2011. évi CLXXXIX. törvény Magyarország helyi önkormányzatairól
- 2013. évi V. törvény – a Polgári Törvénykönyvről (Ptk.);
- 1992. évi XXXIII. törvény a közalkalmazottak jogállásáról (továbbiakban: Kjt.)
– 2011. évi CXII. törvény – az információs önrendelkezési jogról és az információszabadságról (a továbbiakban: Info tv.);
- 2012. évi I. törvény – a munka törvénykönyvéről (Mt.);
- 1997. évi CLV. törvény a fogyasztóvédelemről;
- 1997. évi LXXVIII. törvény az épített környezet alakításáról és védelméről;
- az Intézmény alapító okirata;
- a gyámhatóságokról, valamint a gyermekvédelmi és gyámügyi eljárásról szóló 149/1997. (IX. 10.) Korm. rendelet,
- A nemzeti köznevelésről szóló 2011. CXC. törvény
- Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997.évi XLVII. törvény.
- A fertőző betegségek és a járványok megelőzése érdekében szükséges járványügyi intézkedésekről szóló 18/1998. (VI. 3.) NM rendelet
- Az iskola-egészségügyi ellátásról szóló 26/1997 (VI.3) NM. rendelet.
- A pedagógiai szakszolgálati intézmények működéséről szóló 15/2013. (II. 26.) EMMI rendelet
- A személyes gondoskodást nyújtó gyermekjóléti alapellátások és gyermekvédelmi szakellátások térítési díjáról és az igénylésükhöz felhasználható bizonyítékokról szóló 328/2011. (XII. 29.) Kormány rendelet
- a nemzeti köznevelésről szóló törvény végrehajtásáról szóló 229/2012. (VIII. 28.) Korm. rendelet
- a 20/2012 (VIII. 31.) EMMI rendelet
- Óvodai Nevelés Országos Alapprogramjáról szóló (363/2012. (XII. 17.) Korm. rendelet;
- Polgári Törvénykönyvről szóló 2013. évi V. törvény

- Székesfehérvár Megyei Jogú Város Önkormányzat Közgyűlésének a személyes gondoskodást nyújtó ellátásokról, azok igénybevételéről, valamint a fizetendő térítési díjakról szóló önkormányzati rendelete,
- Székesfehérvár Megyei Jogú Város Önkormányzat Közgyűlésének a pénzbeli és természetben nyújtott szociális-, család- és gyermekvédelmi ellátások biztosításának szabályairól szóló önkormányzati rendelete,
- Székesfehérvár Megyei Jogú Város Önkormányzat Közgyűlésének Székesfehérvár Megyei Jogú Város vagyonáról és a vagyona feletti tulajdonosi jogok gyakorlásáról szóló önkormányzati rendelete.
- egyéb jogszabályok, kormányrendeletek, melyek az egyes tevékenységekhez kapcsolódnak (a folyamatok adatkezelésének leírásánál felsorolásra kerülnek).

4. Jelen szabályzatban nem szereplő kérdésekben a GDPR és az Infotv. szabályai szerint kell eljárni.

5. A Szabályzat hatálya természetes személyre vonatkozó személyes adatok Intézmény általi kezelésére terjed ki, egyéni vállalkozó, egyéni cég, őstermelő ügyfeleket, vevőket, szállítókat e szabályzat alkalmazásában természetes személynek kell tekinteni.

6. A Szabályzat hatálya nem terjed ki az olyan személyes adatkezelésre, amely jogi személyekre – nevükre, formájukra, elérhetőségükre – vonatkozik.

2. Értelmező rendelkezések

Jelen szabályzat alkalmazása során a GDPR 4. cikkben meghatározott fogalmakat kell érteni, a következő kiegészítésekkel:

7. **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;

8. **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;

9. **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;

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

11. **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;

12. **közös adatkezelő:** Ha az adatkezelés céljait és eszközeit két vagy több adatkezelő közösen határozza meg, azok közös adatkezelőnek minősülnek.

13. **adatfeldolgozó**: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;

14. **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. Azon közhatalmi szervek, amelyek egy 2016.5.4. L 119/33 Az Európai Unió Hivatalos Lapja HU egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;

15. **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;

16. **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;

17. **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;

18. **egészségügyi adat**: egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;

19. **személyes adatok határokon átnyúló adatkezelése**:

a) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel

összefüggésben kerül sor; vagy
b) személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket;

20. **adatbiztonság:** az adatvédelmi incidenst bekövetkezését megelőzni képes szervezési, technikai megoldások, valamint eljárási szabályok összessége; az adatkezelés azon állapota, amelyben a kockázati tényezőket – és ezáltal a fenyegetettséget – a szervezési, műszaki megoldások és intézkedések a minimálisra csökkentik.

21. **adatkezelési nyilvántartás:** a GDPR 30. cikke alapján vezetett, személyesadat-kezeléseket tartalmazó nyilvántartás, amely az érintett adatkezeléshez kapcsolódó minden lényeges információt tartalmaz, jelen szabályzat **1. számú melléklete**.

22. **adatvédelmi incidens nyilvántartás:** a GDPR 33. cikk (5) bekezdése alapján vezetett nyilvántartás, amely jelen szabályzat **2. számú melléklete**.

23. **dolgozói személyes adat**: az intézménnyel jogviszonyban, egyszerűsített foglalkoztatotti jogviszonyban álló személyek célhoz kötöttség elvének betartásával kezelt adata.

24. **nyilvántartási célú személyesadat-kezelés**: előre meghatározott szempontok alapján gyűjtött személyesadat-fajtákból adott szempontok szerint strukturált papíralapú vagy elektronikus adatállomány, amelyben az adatkezelés időtartama alatt biztosított az adatok különböző jellemzők alapján történő visszakereshetősége, lekérdezhetősége. Nyilvántartási célú adatkezelésnek minősül az is, amennyiben az adatok a nyilvántartás felvételét megelőző ügyfélkapcsolati adatkezelésből származnak, de az adatok kezelése az adatkezelési cél tekintetében elválik az alapeljárástól. Nyilvántartási célú adatkezelésnek is meg kell felelni a GDPR alapelveinek, rendelkezéseinek.

25. **ügyviteli célú személyesadat-kezelés:** az intézmény által a hatósági hatáskör gyakorlásához más adatkezelő által rendelkezésre bocsátott személyes adatok kezelése (tevékenységre vonatkozó engedély). Az ügyvitelhez kapcsolódó adatkezelés szorosan az ügy feldolgozásához kapcsolódik, alapvető célja az adott ügyhöz kapcsolódó eljárás lefolytatásához, az eljárás szereplőinek azonosításához és az ügy befejezéséhez szükséges adatok biztosítása. Az ügyviteli célú adatkezelés során a személyes adatok kizárólag az adott ügy irataiban szerepelnek, kezelésükre ezen célból csak az alapul szolgáló irat selejtezéséig van lehetőség.

3. Szabályzat hatálya

26. A Szabályzat előírásai az Intézmény egészére, minden szervezeti egységére, az ügyintő szervezetének minden munkatársára kötelező, valamint az Intézménnyel szerződéses vagy egyéb kapcsolatban álló személyes adatkezelést végző személyekre kötelező.

Fokozott felelősséggel tartozik az Intézmény eljáró ügyintéző szervezete, illetve az eljáró felelős személy.

27. A Szabályzat hatálya kiterjed továbbá az Adatkezelő által igénybe vett adatfeldolgozók, közös adatkezelőkkel közösen végzett adatkezelésekre a megállapodások szerint.

28. A Szabályzat tárgyi hatálya kiterjed az Adatkezelő szervezeti egységei által kezelt valamennyi személyes adatra, a rajtuk végzett adatkezelési műveletek teljes körére.

29. A Szabályzat az alkalmazottakkal való közléstől, visszavonásáig hatályos.

30. Jelen szabályzat kötelezően felülvizsgálandó:

a) jelentős szervezeti, vagy jogszabályi változásokat követően,

b) a hatályossá válását követő minden harmadik évben, így az első kötelező felülvizsgálat időpontja: 2022.;

c) az adatkezelések változása, új adatkezelés bevezetése esetén haladéktalanul.

II. **RÉSZ**

Adatvédelem felelősségi rendszere

4. Az adatkezelések szintjei

31. Az intézmény kapcsolatban áll közös adatkezelővel, adatfeldolgozókkal – informatikus, alvállalkozó, beszállítók – amelyek kiválasztása körében törekszik a lehető legmagasabb szintű adatvédelmi és adatbiztonsági megoldásokat nyújtó partnerek kiválasztására, ebből a célból előzetesen megismeri az adatfeldolgozók adatvédelmi és adatbiztonsági szabályzatát, illetve az adatfeldolgozói szerződésben rögzítik a vonatkozó szervezeti és informatikai biztonságra vonatkozó rendelkezéseket.

32. Az intézmény ügyel arra, hogy az adatfeldolgozók lehetőség szerint ne kerüljenek kapcsolatba az alkalmazottak, megbízók személyes adataival, amennyiben ez nem kerülhető el, úgy azok – elektronikus, vagy papír alapú – átadása megfelelő biztonsági intézkedések keretében történhet.

33. Az intézmény a Székesfehérvár Megyei Jogú Város Humán Szolgáltató Intézetével (továbbiakban: Humán Szolgálató Intézet) közös adatkezelést végez.

5. Az adatkezelő szerv vezetője felelősségi rendszere

34. Az adatvédelemre vonatkozó előírások alkalmazása során adatkezelő szerv vezetőjének kell tekinteni az intézmény vezetőjét.

35. Az adatkezelő szerv vezetője felelős:

a) az intézmény adatvédelmi és adatbiztonsági intézményrendszerének kiépítéséért és működtetéséért, ennek keretében a szerv által kezelt személyes

adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosítását célzó, hatáskörébe tartozó intézkedések megtételéért;
b) az alkalmazottak adatvédelmi oktatásáért és továbbképzéséért;
c) a vezetése vagy irányítása alá tartozó intézmény tevékenységének rendszeres adatvédelmi ellenőrzéséért, az ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért;
d) az érintettek jogainak gyakorlásához szükséges feltételek biztosításáért.
e) adatvédelmi tisztviselővel való együttműködésért.

36. Az adatkezelő szerv vezetőjének felelőssége nem zárja ki az intézménnyel kapcsolatban álló személyek akár kártérítési, akár büntetőjogi felelősségét.

37. Amennyiben a személyes adatokhoz való jog megsértése miatt az intézménynek sérelemdíj, kártérítés fizetési kötelezettsége keletkezik, a személyes adatokhoz fűződő jogsértést ténylegesen elkövető személy kilétének felderítésére mindent meg kell tenni, és amennyiben ez sikerrel jár, vele szemben kártérítési eljárást kell kezdeményezni.

6. Az adatkezelő szerv vezetőjének feladat- és hatásköre

38. Adatkezelő szerv vezetőjének feladat- és hatásköre:
a) az intézmény adatkezelési rendszerének (nyilvántartások, adattárak, munkafolyamatok, információáramlások és feldolgozások, jogosultságok) kialakítása és irányítása, rendeltetésszerű működtetése, melynek keretében teljes felelősséget visel a személyes adatok kezelésére vonatkozó törvények és az ezen alapuló rendelkezések érvényre juttatásáért.
b) gondoskodik a személyes adatok körében a jogosulatlan hozzáférés, közlés, megváltoztatás, vagy törlés megelőzéséről, a technikai védelemről, továbbá, hogy a személyes adatok védelmének biztosítása érdekében az érintett az adatkezelő által kezelt adataihoz – ha törvény kivételt nem tesz – hozzáférhessen, illetve gyakorolhassa az őt megillető jogokat.
c) az általa alkalmazott, vele szerződéses kapcsolatban állók tevékenységét, a törvényes és szakszerű működést, ezen belül az állomány adatkezelői tevékenységet irányítja, az adatvédelmi előírások, valamint a kapcsolódó ügyviteli szabályok betartását ellenőrzi.
d) a védelmi és biztonsági szabályok gyakorlati érvényesülését ellenőrzi, intézkedik a hiányosságok felszámolására;
e) kialakítja az adatkezelések szervezeti és működési feltételeit, gondoskodik a működési követelmények és az adatbiztonsági követelmények érvényre juttatásáról;
f) biztosítja az adatkezelések szabályozottságának, dokumentáltságának kialakítását, ellenőrzését;
g) gondoskodik az adatvédelmi kockázatok elemzéséről, szükség esetén kezdeményezi a hatásvizsgálat lefolytatását.
h) biztosítja az adatkezelési nyilvántartás, az adatvédelmi incidensek nyilvántartás vezetését, naprakészen tartását.
i) Gondoskodik a KIR rendszerben az intézmény működésével kapcsolatban rögzített adatok naprakészen tartásáról.

7. Az intézmény adatvédelmi tisztviselője

39. Mivel a gyermekek napközbeni ellátását biztosító intézmények - **az intézmény főtevékenységének államháztartási szakágazati besorolása:** 851020 Óvodai nevelés -közfeladatot látnak el, így az intézménye köteles adatvédelmi tisztviselő kijelöléséről gondoskodni. (GDPR 37. cikk (1) bek a) pontja). Az adatvédelmi tisztviselő szolgáltatási szerződés keretében áll kapcsolatban az intézménnyel, akit az intézmény a Nemzeti Adatvédelmi és Információszabadság Hatóság adatvédelmi tisztviselői rendszerében regisztrált.

40. Az Intézmény közfeladata az óvodai nevelés.

41. Az intézmény adatvédelmi tisztviselője, olyan szerződéssel megbízott vállalkozó, aki szakmai szempontból rátermett, az adatvédelmi jogot és gyakorlatot szakértői szinten ismeri, a feladatok ellátására alkalmas, könnyen elérhető.

42. Az intézmény az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el, szankcióval nem sújthatja. Az adatvédelmi tisztviselő közvetlenül az óvodaigazgatónak és a Humán Szolgáltató Intézetnek tartozik felelősséggel.

43. Az intézmény adatvédelmi tisztviselője feladatköre keretében:

a) közreműködik az intézmény adatvédelmi tevékenységének irányításában, tájékoztat, szakmai tanácsot, iránymutatást ad;
b) segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
c) felkérésre ellenőrzi az adatkezelésre vonatkozó jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzat rendelkezéseinek és az adatbiztonsági követelményeknek a megtartását;
d) kivizsgálja a hozzá érkezett bejelentéseket és adatvédelmi incidens észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót, indokolt esetben vizsgálat lefolytatását kezdeményezi az intézmény vezetőjénél, javaslatot tesz az incidens káros következményeinek elhárítására, a hasonló jövőbeni incidensek megelőzésére;
e) elkészíti az adatvédelem tárgyában kiadandó munkáltatói szabályzatok tervezetét, közreműködik az adatvédelmet érintő egyéb szabályzatok kidolgozásában. Segíti az óvodaigazgatót az adatkezelésekre vonatkozó jogszabályok és szabályzatok érvényre juttatásában, ennek során figyelemmel kíséri az adatvédelemmel összefüggő jogszabályváltozásokat és jelzi az intézmény vezetőjének a munkáltatói szabályzatok módosításának szükségességét;
f) közreműködik az intézménnyel jogviszonyban állók oktatásában és igény szerinti vizsgáztatásában;
g) egyedi ügyekben kidolgozott állásfoglalásával segíti az egységes gyakorlat kialakítását;
h) adatkezelési tevékenységét érintő ügyekben közreműködik az intézmény álláspontjának kialakításában, kapcsolatot tart a NAIH-hal, közreműködik a

NAIH vizsgálatainak lefolytatásában és az ezekkel összefüggő megkeresések megválaszolásában;

i) a kérelem tárgyában elkészíti az érintettnek a személyes adatai kezelésére vonatkozó kérelmére adandó válasziratokat;
j) gondoskodik az intézmény honlapján megjelenített adatvédelmi nyilatkozat, irányelvek és adatkezelési tájékoztató naprakészen tartásáról;
k) peres ügyekben az intézmény adatvédelemmel kapcsolatos álláspontját egyezteti a peres képviseletet ellátó személlyel. Az adatvédelemmel kapcsolatos perekben szakértőként vehet részt;
l) éves jelentést tesz a személyes adatok kezelése, feldolgozása esetén a tájékoztatáshoz kapcsolódóan elutasított kérelmekről;
m) az intézmény vezetője részére igény esetén éves jelentésben értékeli az intézmény adatvédelmi tevékenységét;
n) adatvédelmi szempontból véleményezi a személyes adatokat tartalmazó informatikai nyilvántartásokra, szoftverekre vonatkozó fejlesztési javaslatokat;
o) feladat- és hatáskörében – a célhoz kötöttség elvére figyelemmel – jogosult az intézménynél folytatott adatkezelésekbe betekinteni, az adatkezelőtől felvilágosítást kérni;
p) felkérésre ellenőrzi a GDPR-nak, valamint az egyéb uniós és tagállami adatvédelmi rendelkezéseknek, jelen belső szabályzatnak való megfelelést, képzést, auditokat;
q) közreműködik a betekintési és hozzáférési jogosultságok felügyeletében;
r) szakmai tanácsot ad a hatásvizsgálatra vonatkozóan, nyomon követi a hatásvizsgálat elvégzését.
s) felkérésre ellenőrzi az adatfeldolgozók adatfeldolgozói szerződésben vállalt kötelezettségeinek betartását, amennyiben szerződésbe ütköző gyakorlatot tapasztal, ezt jelzi az intézmény vezetőjének, javaslatot tesz a szerződéses kapcsolat megszüntetésére.
t) Az elutasított közérdekű adatigényekkel kapcsolatban évente tájékoztatást ad a NAIH részére.
u) előkészíti a közös adatkezelői szerződés tervezetét.

III. **RÉSZ**

A személyes adatok védelme az intézménynél

8. Az adatkezelés alapvető szabályai

44. Az intézménynél kezelt 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.

45. Az intézmény valamennyi adatkezelése vonatkozásában a személyes adatok biztonsága érdekében köteles érvényre juttatni a Szabályzatban és más belső szabályozóiban és más dokumentumokban (folyamatokban, munkaszerződésekben, munkaköri leírásokban) és vezetői intézkedésekben meghatározott technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek a GDPR és az Infotv., érvényre juttatásához szükségesek.

46. Az adatkezelő köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy biztosítsa az érintettek magánszférájának védelmét, jogaik gyakorlásának lehetőségét. Az intézmény a törvény alapján titoktartásra nem kötelezett, de személyes adatok kezelő személyekre vonatkozóan titoktartási kötelezettséget ír elő, amelyet a **10. sz. melléklet** tartalmaz.

47. A személyes adatokhoz való hozzáférést az intézmény, elektronikus úton (hálózati meghajtó, beléptető rendszer) jogosultsági szintek megadásával korlátozza.

48. A folyamatban levő munkavégzés, feldolgozás alatt levő iratokhoz csak az érintett alkalmazottak férhetnek hozzá, a bér- és munkaügyi, gyermekekre, szülőkre vonatkozó adatokat, illetve egyéb személyes adatokat tartalmazó iratokat biztonságosan elzárva – zárható irodákban és zárható szekrényekben – kell tartani.

49. Az adatkezelő, illetve tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról. Az intézmény a tudomány és technológia állása és a megvalósítás költségei, az adatkezelés jellege hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett kockázat figyelembevételével köteles megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adatvédelmi elvek, szabályok és az érintettek jogainak védelmére vonatkozó garanciák érvényre juttatásához szükségesek. Több lehetséges adatkezelési megoldás közül lehetőség szerint azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja.

50. A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok – kivéve, ha azt törvény lehetővé teszi – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

51. Amennyiben az intézmény személyes adatok automatizált feldolgozását végzi, az automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja:

a) az érintett tájékoztatását;
b) az eszköz pontosságát, rendeltetésszerű működését;
c) a jogosulatlan adatbevitel megakadályozását;
d) az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;
e) annak ellenőrizhetőségét és megállapíthatóságát, ha a személyes adatokat adatátviteli berendezés alkalmazásával továbbították vagy továbbíthatják;
f) annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;
g) a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát;
h) az automatizált feldolgozás során fellépő hibákról jelentés készítését;
i) az érintettnek biztosítani kell az emberi beavatkozás lehetőségét, lehetővé kell tenni, hogy álláspontját kifejthesse, és a döntéssel szembeni kifogást közölje.

9. Az adatbiztonság alapvető szabályai

52. A személyes adatok kezelésének helyszínéül szolgáló épület megfelelő fizikai, és tűzvédelméről gondoskodni kell. A személyes adatok kezelése zárható helyiségében történik, ahova csak az arra jogosultak léphetnek be.

53. Az intézmény indokolt esetben külön adatbiztonsági szabályzatot alkalmaz.

54. Az informatikai rendszerek tűzfalas védelméről, vírusvédelméről, az adattárolókon lévő személyes adatok biztonsági mentéséről, felhasználónév-jelszó védelméről, a mobil adathordozók titkosításáról, legalább féléves rendszerességű biztonsági mentéséről a vezető intézkedik.

55. A nem pedagógiai/gyermekfelügyeleti feladatot végző alkalmazott (pl. takarító, karbantartó) személyes adatokkal nem kerülhet kapcsolatba, ezért az ilyen tartalmú dokumentumokat zárható szekrényben kell őrizni, a monitorok rálátásvédelméről, az informatikai eszköz őrizetlenül hagyása esetén a kijelző zárolásáról és jelszavas védelméről gondoskodni kell.

56. Az intézmény az informatikai rendszerek frissítéséről havi szinten gondoskodik, tesztelését nem valós adatokkal végezheti. Az informatikus programok telepítését, frissítését megelőzően, megfelelő időben értesíti az intézményt, annak érdekében, hogy a személyes adatokhoz való hozzáférés folyamatosan biztosított legyen.

57. Az intézmény azon alkalmazottai, akik személyes adat meghatározott csoportját nem kezelik (pl. alkalmazotti adatok, alkalmazottak pénzügyi adatai, gyermekre, szülőkre vonatkozó adatok, egészségügyi adatok) azokhoz nem férhetnek hozzá.

58. A rendszergazdai jogosultsággal rendelkezők esetén is nyomon követhetővé teszi azt, hogy személyhez rendelhető legyen valamennyi adatkezelési művelet (pl. admin1, admin2, admin3 felhasználónévvel).

59. Az intézmény elektronikus adatfeldolgozásra, nyilvántartásra alkalmazott szoftvere lehetővé teszi a rendszer naplózhatóságát, hogy azonosítható legyen, mely felhasználó, mikor, mit rögzített, vagy törölt. Az intézmény, csak eredeti szoftvereket alkalmaz, beszerzi az alkalmazott szoftverekre vonatkozó hatásvizsgálati dokumentációt, amely igazolja a GDPR rendeletnek való megfelelést.

60. Az intézmény a hardverek esetén a garanciális időszakot követően új adathordozókat szerez be, és a garanciális időszakot meghaladott adathordozókat megsemmisíti.

61. Az intézmény gondoskodik mind az elektronikus, mind a papír alapú bejövő és kimenő kommunikáció ellenőrzéséről.

62. A jelszavak használata esetén ügyelni kell arra, hogy több személynek nem lehet azonos jelszava, egymás jelszavát nem ismerhetik meg a felhasználók.

63. A szkennelésnél ügyelni kell arra, hogy minden felhasználó a saját mappájába tudja menteni a személyes adatokat tartalmazó dokumentumokat.

64. A dokumentumok nyomtatásánál alkalmazni kell a titkos nyomtatás funkciót, amennyiben több személy közös nyomtatót használ.

65. Informatikai eszköz elvesztése esetén gondoskodni kell az alkalmazásokhoz való hozzáférések visszavonásáról, az adatok távoli törléséről.

66. Az informatikai rendszerek, alkalmazások sérülékenységi vizsgálatát bevezetését megelőzően el kell végezni.

67. Az intézmény felhőszolgáltatás igénybe vétele esetén olyan szolgáltatót választ, amelynek tárhelye az Európai Unió valamely országában található.

68. A tárasaság eszközein a felhasználónevek, jelszavak megjegyzése nem állítható be. Jelszó papír alapon nem tárolható.

69. Személyes adatot tartalmazó papír alapú dokumentumot az intézmény épületéből kivinni, az 1. sz. mellékletben megjelölt helyről más helyre áthelyezni, csak vezetői engedéllyel lehet. Az irat mozgás dokumentálása érdekében a **8. sz. mellékletet** kell kitölteni.

10. Az intézmény adatkezelési tájékoztatója

70. Az intézmény általános adatkezelési tájékoztatóját a **3. sz. melléklet** tartalmazza.

71. Amennyiben az intézmény eseti adatkezelést végez (pl. rendezvény szervezése, álláshirdetés) úgy a vonatkozó tájékoztató kidolgozásáról és az érintettek részére elérhetővé tételéről megfelelően gondoskodik. Az intézmény az eseti adatkezelést megelőzően az adatvédelmi tisztviselő véleményét beszerzi.

IV. RÉSZ
AZ ADATKEZELÉS LEHETSÉGES JOGALAPJAI

72. Az intézmény valamennyi adatkezelése során biztosítja az érintett jogainak főszabály szerint díj- és költségmentes gyakorlását.

11. Az érintett hozzájárulása

73. Amennyiben a személyes adatok kezelése hozzájáruláson alapul, az érintett hozzájárulását főszabály szerint a **4. számú melléklet** szerinti adatkérő lap szerinti tájékoztatással és tartalommal kell beszerezni. A hozzájárulás önkéntességét biztosítani kell.

74. A hozzájárulásnak mindig önkéntesnek, konkrétnak, megfelelő tájékoztatáson alapulónak és egyértelműnek kell lennie. Az intézmény, mint adatkezelő a hozzájárulást valamennyi adatkezelési célhoz egyenként szerzi be, egyúttal felhívja az érintett figyelmét azon jogára, hogy a hozzájárulást bármikor egyszerű módon visszavonhatja, amely visszavonás azonban nem érinti a megelőzően végzett adatkezelés jogszerűségét.

75. A hozzájárulás az ugyanazon cél vagy célok érdekében történő összes adatkezelési tevékenységre kiterjed.

76. Ha az érintett hozzájárulása más ügyekre is vonatkozik – így különösen értékesítési, szolgáltatási szerződés megkötése - a hozzájárulást ezektől a más ügyektől egyértelműen megkülönböztethető módon kell kifejezni, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel. Az érintett hozzájárulását tartalmazó nyilatkozat bármely olyan része, amely a GDPR-ba ütközik, kötelező erővel nem bír.

77. Az intézmény nem kötheti szerződés megkötését, teljesítését olyan személyes adatok szolgáltatása feltételéül, amelyek nem szükségesek a szerződés teljesítéséhez.

78. Ha a személyes adat felvételére az érintett hozzájárulásával került sor, az adatkezelő a rá vonatkozó jogi kötelezettség teljesítése céljából, törvény eltérő rendelkezésének hiányában további külön hozzájárulás nélkül, valamint a hozzájárulás visszavonását követően is kezelheti.

79. Az intézménynek bármikor igazolnia kell tudni azt, hogy az adatkezelési művelethez az érintett hozzájárult.

12. Szerződés, mint jogalap

80. A szerződés, mint jogalap akkor alkalmazandó, ha a szerződés tárgya alapján a közérdekű tevékenység gyakorlásához nem szükséges a szerződés megkötése.

81. A szerződés előkészítése során, a tervezet kidolgozásakor, véleményezésre megküldése során – amennyiben nem titkosított csatornán történik – személyes adat feltüntetésére nem kerülhet sor.

82. A szerződésben csak a szerződés érvényességéhez és a teljesítéséhez szükséges személyes adatok kezelhetőek.

83. A szerződésekben külön adatvédelmi záradékot kell feltüntetni, amiben rögzíteni kell az adatkezelés jogalapját és a tájékoztatás megadására vonatkozó információt, a szerződésben szereplő személyes adatok (jellemzően kapcsolattartói adatok) védelme érdekében.

84. A szerződésben szereplő személyes adatok kezelésére a szerződés hatálya ideje alatt történhet. A szerződés teljesítését, megszűnését követően 5 évig az esetlegesen szerződésen alapuló követelések kölcsönös bizonyítása, érvényesítése érdekében is sor kerülhet. Amennyiben a szerződésben nyújtott jótállás a szerződés teljesítését követő 5 éven túli időre kiterjed, úgy a jótállási idő leteltét követő 5 évig jogszerűen kezelhetők a szerződésben szereplő személyes adatok.

85. Az intézmény a szerződést kötő partnerét tájékoztatja jelen szabályzatban meghatározott, szerződéskötéshez kapcsolódóan lényeges adatkezelési, adatvédelmi feltételekről.

13. Jogi kötelezettség teljesítése

86. A jogi kötelezettségen alapuló adatkezelés szabályaira – adatkezelés célja, kezelhető adatok köre, tárolás időtartama, címzettek – a vonatkozó jogszabály rendelkezései irányadók.

87. Amennyiben a jogszabályi előírás a közérdekű tevékenység gyakorlására vonatkozik, úgy ezen jogalap nem alkalmazható.

88. Az intézmény a bérszámfejtés, illetőleg az adó- és járulék fizetés, valamint a Magyar Államkincstár által az intézménybe beíratott gyermekek után járó normatíva folyósítása, illetve ezen adatszolgáltatási kötelezettsége érdekében kezel személyes adatokat, ezen kötelezettségek teljesítéséhez szükséges mértékben.

89. A jogi kötelezettség teljesítésén alapuló adatkezelés az érintett hozzájárulásától független. Az érintettel az adatkezelés megkezdése előtt ez esetben közölni kell, hogy az adatkezelés kötelező, továbbá az érintettet az adatkezelés megkezdése előtt egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, arról, ha az érintett személyes adatait az adatkezelő a rá vonatkozó jogi kötelezettség alapján kezeli, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is. Kötelező adatkezelés esetén a tájékoztatás megtörténhet az előbbi információkat tartalmazó jogszabályi rendelkezésekre való utalás nyilvánosságra hozatalával is.

14. Közérdekű tevékenység gyakorlásához szükséges adatkezelés

90. Az intézmény jellemzően közérdekű tevékenység gyakorlásához szükséges jogalap alapján adatkezelést végez a köznevelésről szóló jogszabályok által ráruházott pedagógiai nevelő munka, mint óvodás korú gyermekek nevelése közérdekű feladatellátás gyakorlása keretében végzett feladatok végrehajtásához szükséges mértékben. Ilyenek például a főtevékenységhez kapcsolódó rendezvényszervezésre, valamint az egészségügyi, pedagógiai és nevelési feladatokra, a neveléshez szükséges körülmények biztosítására vonatkozó kapcsolódó adatkezelések.

15. Intézmény jogos érdeke

91. Az intézmény a számára, vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges jogalapot nem alkalmazza.

16. Személyes adatok gyűjtési céltól eltérő kezelése

92. Személyes adatok gyűjtési céljuktól eltérő kezelése csak akkor megengedett, ha az adatkezelés összeegyeztethető az adatkezelés eredeti céljával. A további adatkezelés megkezdése előtt indokolt kikérni az adatvédelmi tisztviselő állásfoglalását.

93. A közérdekű archiválási, tudományos, történelmi kutatási célból, vagy statisztikai célból történő további adatkezelés megengedett.

V. RÉSZ

ALKALMAZOTTI ADATKEZELÉSEK

17. Személyügyi nyilvántartás

94. A Személyi irat minden – bármilyen anyagon, alakban és bármilyen eszköz felhasználásával keletkezett – adathordozó, amely a közalkalmazotti jogviszony létesítésekor, fennállása alatt, megszűnésekor, valamint azt követően keletkezik, és a természetes személy alkalmazott személyével összefüggésben adatot, megállapítást tartalmaz.

95. A foglalkoztatottakról csak a közalkalmazotti jogviszonyukkal összefüggő adat tárolható. Az érintettől csak olyan nyilatkozat, vagy adatlap kitöltése kérhető, amely személyiségi jogait nem sérti.

96. A közalkalmazotti jogviszonnyal összefüggésben az Intézmény alkalmazásában álló személyekről nyilvántartásokat vezet, különösen személyi anyagok, egészségbiztosítási ellátások nyilvántartása, magán-nyugdíjpénztári nyilvántartás, fizetési jegyzékek, járulék-nyilvántartások, számfejtési anyagok, bérfeladások, bérátutalások, statisztikai jelentések, személyi jövedelemadó nyilvántartások, OEP elszámolások, adó- és járulékbevallások, kiküldetési rendelvények nyilvántartása, hivatali célra saját gépkocsi használat nyilvántartása.

97. A Székesfehérvár MJV Önkormányzat fenntartásában működő székesfehérvári székhelyű bölcsődékbe járó kiskorú gyermekekről az intézmények vezetnek személyi nyilvántartást, azonban a normatívák, illetve a védőnői és házi gyermekorvosi szolgálatok tekintetében közös adatkezelőként a Humán Szolgáltató Intézet is kezel adatokat a gazdasági-pénzügyi-műszaki célú felhasználásra, valamint egészségügyi alap-és szakellátással összefüggő célra. Ezen adatkezelés jogi kötelezettség teljesítése céljából valósul meg; itt az adatkezelés jogalapja jogi kötelezettség teljesítése (GDPR 6. cikk (1) bekezdés c./ pontja, illetve e./ pontja).

98. A személyi iratokat és a személyi adatokat védeni kell, különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen. A személyi iratokat, egyéb papír alapú nyilvántartásokat az Intézmény hivatalos helyiségében, zárható szekrényben kell tárolni, megakadályozandó, hogy illetéktelenek hozzáférjenek.

Az elektronikusan tárolt adatok esetén is külön szabályzat szerint gondoskodni kell az adatvédelemről.

99. A személyi iratokat az erre munkaköri leírásban felhatalmazott alkalmazott a munkavégzéshez szükséges mértékben használhatja. Az iratokba a foglalkoztatói jogkör gyakorlójának is joga van betekinteni.

100. A foglalkoztatásra irányuló jogviszonnyal kapcsolatos személyi irat, dokumentum kizárólag személyesen, vagy meghatalmazott útján vehető át, illetve tértivevényes ajánlott küldeményként az érintett lakcímére postázandó.

101. Az Intézményéhez bármilyen formában álláskeresési céllal (hirdetésre, spontán módon) eljuttatott önéletrajzokban lévő személyes adatok kezeléséhez az érintett hozzájárulását kell kérni tárolás céljára. Alkalmazás hiányában a személyes adatokat törölni kell.

102. Az intézménybe beíratott kiskorú gyermekek és szüleik, nevelőik személyes adatai tekintetében titoktartási kötelezettség áll fenn.

103. Az Intézmény nyilvántartásában szereplő adatok kizárólag a kiskorú gyermekek gondozása, nevelése és a családi kapcsolataik szükségszerű megismeréséhez kapcsolódó feladatok teljesítéseként használhatók fel, oly módon, hogy az adat célhoz kötött felhasználása ellenőrizhető legyen.

104. Az Intézmény alkalmazottjai - a titoktartási nyilatkozatuk szerinti körben és feltételek mellett - kötelesek az ügykörükben tudomásukra jutott személyes jellegű szociális, egészségügyi és más érzékeny információkat titokként megőrizni.

105. A szenzitív adatok körébe tartozó információk kezelése az érintettek kifejezett hozzájárulása esetén kezelhetőek; adatkezelés során fokozott körültekintéssel kell eljárni. A kiskorú gyermek, sajátos nevelési igényére, beilleszkedési zavarára, magatartási rendellenességére vonatkozó adatai az egészségügyi intézmények között szükség esetén a szülői hozzájárulás beszerzését követően továbbíthatók.

106. Az intézmény megnevezés alatt jelen részben írtak esetén, a munkáltatót is érteni kell a munka törvénykönyvéről szóló 2012. évi I. törvény szerint (a továbbiakban: Mt.).

107. Az alkalmazottól csak olyan nyilatkozat megtétele vagy adat közlése kérhető, amely személyiségi jogát nem sérti, és a jogviszony létesítése, teljesítése vagy megszűnése szempontjából lényeges.

108. Az intézmény köteles az alkalmazottat tájékoztatni személyes adatainak kezeléséről. Az intézmény az alkalmazottra vonatkozó tényt, adatot, véleményt harmadik személlyel csak törvényben meghatározott esetben vagy az alkalmazott hozzájárulásával közölhet.

109. A jogviszonyból származó kötelezettségek teljesítése céljából az intézmény az alkalmazott személyes adatait - az adatszolgáltatás céljának megjelölésével, törvényben meghatározottak szerint – közös adatkezelő, illetve adatfeldolgozó számára átadhatja. Erről az alkalmazottat előzetesen tájékoztatni kell.

110. Az alkalmazott csak a jogviszonnyal összefüggő magatartása körében ellenőrizheti. Az intézmény ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. Az alkalmazott magánélete nem ellenőrizhető. Az intézmény előzetesen tájékoztatja az alkalmazottt azoknak a technikai eszközöknek az alkalmazásáról, amelyek az alkalmazott ellenőrzésére szolgálnak.

111. Az intézmény nem jogosult az alkalmazotti okmányainak másolására, amennyiben erre jogszabály nem hatalmazza fel. Erre való tekintettel az okmányazonosító rögzítésére a személyi ügyekkel foglalkozó alkalmazott jogosult, amely rögzítés helyességét a vezetője igazolja.

112. Az intézmény a Polgári Törvénykönyvben rögzített, illetve a közalkalmazott **5. számú mellékletek** szerinti törzslapon meghatározott adatait kezeli.

113. Az adatok pontosságának garantálása érdekében az alkalmazott a fenti adatokban bekövetkezett változást, 8 napon belül írásban köteles bejelenteni az intézmény vezetője részére.

114. A személyes adatok címzettjei, a munkáltató vezetője, munkáltatói jogkör gyakorlója, az intézmény munkaügyi feladatokat ellátó alkalmazottja, közös adatkezelője és adatfeldolgozója.

115. A személyi anyagba csak az arra jogosultak tekinthetnek be.

116. Az alkalmazott köteles a munkája során tudomására jutott titkot megőrizni. Ezen túlmenően sem közölhet illetéktelen személlyel olyan adatot, amely munkaköre betöltésével összefüggésben jutott a tudomására, és amelynek közlése az intézményre vagy más személyre hátrányos következménnyel járhat.

117. Az intézmény a jelen szabályzat **6. számú melléklete** szerinti Tájékoztató kihirdetésével és az intézményvezető irodájában papír alapon történő elhelyezésével tájékoztatja az alkalmazottat személyes adatainak kezeléséről és a személyhez fűződő jogokról.

18. Alkalmassági vizsgálatokra vonatkozó adatkezelés

118. Az alkalmazottal szemben csak olyan alkalmassági vizsgálat alkalmazható, amelyet jogviszonyra vonatkozó szabály ír elő, vagy amely jogviszonyra vonatkozó szabályban meghatározott jog gyakorlása, kötelezettség teljesítése érdekében szükséges.

119. Az alkalmazottat előzetesen tájékoztatni kell, hogy az adott munkakör betöltésére csak megfelelő készség, képesség esetén van lehetőség.

120. A vizsgálat előtt részletesen tájékoztatni kell az alkalmazottakat arról is, hogy az alkalmassági vizsgálat milyen készség, képesség felmérésére irányul, a vizsgálat milyen eszközzel, módszerrel, gyakorisággal történik, ki végezheti, eredménye milyen hatással lesz jogaikra, a személyes beavatkozás lehetősége fennáll-e, automatikus

döntéshozatalra, profilalkotásra sor kerül-e. Amennyiben jogszabály írja elő a vizsgálat elvégzését, akkor tájékoztatni kell az alkalmazottakat a jogszabályi rendelkezésről is. E Tájékoztatáshoz kapcsolódó adatkezelési tájékoztató mintáját jelen szabályzat **7. számú melléklete** tartalmazza.

121. A kezelhető személyes adatok köre a munkaköri alkalmasság ténye, és az ehhez szükséges feltételek megállapítása. Az adatkezelés jogalapja: a munkáltató jogos érdeke. A személyes adatok kezelésének célja jogviszony létesítése, fenntartása, munkakör betöltése.

122. A vizsgálati eredményt az érintett alkalmazottak, illetve a vizsgálatot végző, titoktartási kötelezettség alá eső szakember ismerheti meg. A munkáltató csak azt az információt kaphatja meg, hogy a vizsgált személy a munkára alkalmas-e vagy sem, illetve milyen feltételek biztosítandók ehhez. A vizsgálat részleteit, illetve annak teljes dokumentációját a munkáltató nem ismerheti meg.

19. Önéletrajzok kezelése

123. Annak érdekében, hogy a nem pályázati kiírás eredményeként érkező önéletrajz benyújtója, illetve a pályázat keretében benyújtott önéletrajzok további tárolása érdekében személyes adatok védelméhez fűződő joga ne sérüljön, az érintettnek a beküldött önéletrajzához csatolnia kell egy nyilatkozatot, amelyben hozzájárul önéletrajzának lefeljebb 1 évig tartó megőrzéséhez. Hozzájárulás hiányában az intézmény kizárólag annak vizsgálatára jogosult, hogy a pályázati anyagnak megfelelő betöltetlen álláshellyel rendelkezik-e, amennyiben ilyen álláshely nem áll rendelkezésre, az anyagot a benyújtójának vissza kell küldeni vagy meg kell semmisíteni.

124. Az állásfelhívás feladása során jelezni kell, hogy az önéletrajzok tárolási ideje az adott pályázat lezárulásától, amennyiben a jelentkezés pályázattól függetlenül érkezett, a jelentkezés benyújtásától számított 3 hónap. A fel nem vett személyek önéletrajza a felvett, azonban próbaidő alatt megüresedő munkakör betöltése céljából kezelhető.

125. Az adattárolási határidő lejártát, vagy az érintett hozzájárulásának visszavonását követően a pályázati anyagokat meg kell semmisíteni és az érintettet erről elektronikus úton tájékoztatni szükséges. Amennyiben a pályázati anyagra a jelentkező külön igényt tart, részére vissza kell küldeni.

126. A kezelhető személyes adatok köre, a természetes személy neve, születési ideje, helye, anyja neve, lakcím, képesítési adatok, fénykép, telefonszám, e-mail cím, korábbi munkáltatói értékelés (ha van).

127. A személyes adatok kezelésének célja, a megfelelő munkaerő kiválasztása. Az érintettet tájékoztatni kell arról, ha a munkáltató nem őt választotta az adott állásra.

128. Az adatkezelés jogalapja a hozzájárulás.

129. Az önéletrajzokat az intézménynél munkáltatói jogok gyakorlására jogosult vezető, személyügyi feladatokat ellátó alkalmazottak kezelhetik.

130. Amennyiben az intézmény képviselője az állásinterjú során jegyzetet vesz fel, előzetesen az érintett hozzájárulását kell kérni és lehetővé kell tenni a jegyzet megismerését, amelyhez észrevételt tehet. Az állásinterjú végén az érintett amennyiben a jegyzet tartalmával egyet ért, azt aláírja, aláírás megtagadása esetén a jegyzetet meg kell semmisíteni.

131. Az álláspályázathoz kapcsolódóan az intézmény nem jogosult korábbi munkáltatók megkeresésére.

132. Az intézmény a munkaerő kiválasztása során előzetes tájékoztatást követően jogosult a jelentkező közösségi oldalon közzétett profiloldalának megtekintésére és a munkakör betöltéséhez szükséges adatok kezelésére. Az intézmény a pályázó közösségi oldal zárt csoporthoz kapcsolódó tevékenységet nem ellenőrizhet.

133. A 118/2001. (VI. 30.) Korm. rendelet 10. § (1) bekezdés e) pontja meghatározza, hogy milyen adatokat nem lehet kezelni magán-munkaközvetítés során. A jogszabály értelmében tilos olyan személyes adatokat kezelni, amelyekre a munkát keresők alkalmasságának a megítéléséhez nincs szükség, illetve amelyek a keresett munkával nincsenek közvetlen összefüggésben.

134. Az álláspályázat részenként a közalkalmazott, a Kjt-ben meghatározott hatósági erkölcsi bizonyítvány bemutatására köteles.

20. Elektronikus levelezőrendszer ellenőrzéséhez kapcsolódó adatkezelés

135. Az intézmény alkalmazottjait azért ellenőrizheti, hogy megbizonyosodjon róla, hogy üzleti, személyes adatokra vonatkozó titoktartási kötelezettségüknek eleget tesznek, munkaköri feladatuk ellátásáról, azok minőségéről, az alkalmazottak, készségéről, képességéről meggyőződjön.

136. Az intézmény az intézmény ügyeinek intézése céljából közös, intézményi e-mail fiókot alkalmaz, amelyhez az intézményvezető, helyettese, tagintézményvezető, óvodatitkár férhetnek hozzá. Az e-mail fiókot az intézmény működésével kapcsolatos célra használhatja, hogy a munkáltató képviseletében levelezzenek az ügyfelekkel, más személyekkel, szervezetekkel. Az elektronikus levelezőrendszer magán célra nem használható, a fiókban személyes leveleket nem kezelhet, amely tilalomra az intézmény félévente emlékezteti az érintett alkalmazottjait.

137. Az adatkezelés jogalapja, hogy az ellenőrzés a közérdekű jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, célja, a jogviszonyra vonatkozó kötelezettségek megtartásának ellenőrzése, a megfelelő munkavégzés biztosítása.

138. Az intézmény elektronikus levelezőrendszerének informatikai védelméről, így annak rendelkezésre állásáról, sértetlenségéről, bizalmasságáról a vezető gondoskodik. A levelezés biztonsági mentéséről a szolgáltató a szerződési feltételek szerint gondoskodik.

139. Az elektronikus levelezőrendszer használata során az érintett alkalmazott köteles megfelelő körültekintéssel eljárni, mind a címzettek megadása, titkos másolatok alkalmazása, mind a dokumentumok csatolása során. Ügyelni kell arra, hogy a címzettek és másolatot kapó személyhez kapcsolódó elektronikus levelezési cím is személyes adat.

140. Az elektronikus levelezés során törekedni kell a személyes adatok titkosítására. A dokumentumok tervezeteit személyes adatok feltüntetése nélkül kell egyeztetésre küldeni.

141. A munkahelyi levelezőrendszer használata kizárólag munkahelyi eszközökön engedélyezett.

142. A munkáltató jogosult az e-mail fiók tartalmát és használatát rendszeresen ellenőrizni. Az ellenőrzés célja az e-mail fiók használatára vonatkozó munkáltatói rendelkezés betartásának ellenőrzése, továbbá az alkalmazotti kötelezettségek teljesítésének ellenőrzése, jogalapja a közérdekű jogosítvány gyakorlásának keretében végzett feladat végrehajtásának szükségessége.

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

144. Lehetőség szerint biztosítani kell, hogy az alkalmazott jelen lehessen az ellenőrzés során, távollétében két személy jelenlétében jegyzőkönyvet kell felvenni a tapasztaltakról, jogszabályba, vagy jelen szabályzatba ütközés esetén.

145. Az ellenőrzés megkezdése előtt tájékoztatni kell az alkalmazottat arról, hogy milyen munkáltatói érdek miatt kerül sor az ellenőrzésre, munkáltató részéről, ki végezheti az ellenőrzést, - milyen szabályok szerint kerülhet sor és mi az eljárás menete, - milyen jogai és jogorvoslati lehetőségei vannak az ellenőrzés eredményével kapcsolatban.

146. Az ellenőrzés során a fokozatosság elvét kell érvényesíteni, így elsődlegesen levél címéből és tárgyából kell következtetést levonni arra vonatkozóan, hogy az az alkalmazott munkaköri feladatával kapcsolatos, és nem személyes célú. A nem személyes célú e-mailek tartalmát az intézmény korlátozás nélkül vizsgálhatja.

147. Amennyiben megállapítható, hogy az alkalmazott az elektronikus levelezőrendszert személyes célra használta, fel kell szólítani, hogy a személyes adatokat haladéktalanul törölje, vagy mentse le. Az alkalmazott távolléte, vagy együttműködésének hiánya esetén a személyes adatokat az ellenőrzéskor a munkáltató törli.

148. Az elektronikus levelező rendszer jelen szabályzatba ütköző használata miatt az intézmény az alkalmazottval szemben, az Mt. 56. § alapján, a munkaszerződésben rögzített jogkövetkezményeket alkalmazhat.

149. Az alkalmazott az elektronikus levelezőrendszer ellenőrzésével együtt járó adatkezeléssel kapcsolatban jelen szabályzatnak az érintett jogairól szóló részében írt jogokat gyakorolhatják.

150. A jogviszony megszűnését megelőzően az alkalmazott gondoskodik arról, hogy az esetleges magáncélú leveleit törölje. A jogviszony megszűnését követően az intézmény az elektronikus levelezőrendszerben tárolt személyes adatokat megsemmisíti.

151. Az alkalmazott munkahelyi levelezőrendszer GDPR-nak való megfelelősségére vonatkozó hatásvizsgálat eredményét az intézmény a szolgáltatótó beszerzi, amennyiben annak eredménye (a GDPR rendelkezéseinek való megfelelősség) nem nyilvános.

152. Az az alkalmazott, aki a levelezőrendszer működésében rendellenességet észlel, vagy olyan személyes adat válik számára hozzáférhetővé, amelynek megismerésére nem jogosult, köteles azonnal jelezni az intézmény vezetője felé.

21. Az informatikai eszközök ellenőrzésével kapcsolatos adatkezelés

153. Az intézmény jelen szabályzattal előírja, hogy az általa biztosított számítástechnikai vagy elektronikus eszközt így különösen számítógépet, laptopot, tabletet, mobiltelefont, pendrive-t az alkalmazott kizárólag a munkavégzéshez használhatja, ezek magáncélú használatát az intézmény megtiltja, ezen eszközökön az alkalmazott semmilyen személyes adatot, levelezését nem kezelhet és nem tárolhat.

154. Az elektronikai eszközök időszakos – félévente – biztonsági mentéséről gondoskodni kell, megelőzően az érintetteket fel kell hívni, hogy esetleges személyes adataikat távolítsák el az adathordozókról.

155. Az intézmény által biztosított mobil adathordozókon kívül egyéb eszköz nem csatlakoztatható az intézmény informatikai eszközeihez, amelyről végpontvédelmi beállításokkal is gondoskodni szükséges.

156. Az informatikai eszköz javítására az intézmény által megbízott vállalkozó intézkedik, amennyiben helyben nem javítható, úgy a javítás idején az intézmény képviselőjének jelen kell lennie, hogy személyes adat jogosulatlanul ne kerülhessen ki az informatikai eszköz adathordozójáról. A harmadik személy által végzett javítás idején akkor lehet az intézmény képviselője távol, ha adathordozót (winchestert) nem ad át, vagy a harmadik személy igazolja, hogy az általa folytatott tevékenység a GDPR rendeletnek megfelel, és titoktartási nyilatkozatot tesz.

157. Az informatikai eszköz selejtezését, értékesítését megelőzően gondoskodni kell az adathordozó fizikai megsemmisítéséről, vagy az adatok biztonságos elektronikus törléséről.

158. Az adatkezelés jogalapja, a közérdekű jogosítvány gyakorlásának keretében végzett feladat végrehajtásának szükségessége, célja, a jogviszonyra vonatkozó kötelezettségek megtartásának ellenőrzése, a megfelelő munkavégzés biztosítása.

159. A jogviszony megszűnését megelőzően az alkalmazott gondoskodik arról, hogy az esetlegesen informatikai eszközön lévő magáncélú adatait törölje. A jogviszony megszűnését követően az intézmény az informatikai eszközön tárolt személyes adatokat megsemmisíti.

160. A munkáltató az informatikai eszközökön tárolt adatokat ellenőrizheti. Az informatikai eszközök munkáltató általi ellenőrzésére és jogkövetkezményire egyebekben a 20. cím rendelkezései irányadók.

161. Az alkalmazott köteles 24 órán belül bejelenteni az intézmény vezetője részére, ha informatikai eszközét elvesztette és közölni, hogy az eszközön megközelítőleg hány, és milyen jellegű személyes adat volt.

162. Az informatikai eszközök védelméről az intézményvezető gondoskodik, amelynek során megfelelő intézkedéseket tesz annak érdekében, hogy az eszköz elvesztése esetén a tárolt személyes adatokhoz ne lehessen hozzáférni.

22. A munkahelyi internethasználat ellenőrzésére vonatkozó adatkezelés

163. Az alkalmazott csak a munkaköri feladatával összefüggő honlapokat tekintheti meg, a személyes célú munkahelyi internethasználatot a munkáltató megtiltja.

164. Az intézmény informatikai eszközeire interneten elérhető szoftver csak intézményvezetői engedéllyel telepíthető, amit szükség esetén megbízott vállalkozóval teljesít. A szoftver telepítését személyesen, vagy rendszergazdai felhasználónév és jelszó megadása alapján engedélyezett. A külső forrásból kapott vagy letöltött, nem engedélyezett programok használata tiltott!

165. A fájl letöltő-, játék-, csevegő-, szexuális szolgáltatásokat kínáló oldalak látogatása szigorúan tilos.

166. Az adatkezelés jogalapja, a közérdekű jogosítvány gyakorlásának keretében végzett feladat végrehajtásának szükségessége, célja, a jogviszonyra vonatkozó kötelezettségek megtartásának ellenőrzése, a megfelelő munkavégzés biztosítása.

167. A munkaköri feladatként az intézmény nevében elvégzett internetes regisztrációk jogosultja az intézmény. A személyes adatok megadása is szükséges a regisztrációhoz, a jogviszony megszűnésekor azok törlését kezdeményezi az intézmény. Az intézmény informatikai eszközein nem megengedett a felhasználónév, jelszó megjegyzésének engedélyezése. Az intézmény nem jogosult megismerni az alkalmazott által alkalmazott jelszót.

168. Az alkalmazott munkahelyi internethasználatát az intézmény 20. cím rendelkezései szerint ellenőrizheti és az ott meghatározott jogkövetkezményeket alkalmazhatja.

23. A hivatali mobiltelefon használatának ellenőrzésével kapcsolatos adatkezelés

169. Az intézmény vezetője és távollétében helyettese, valamint a tagintézmény vezetője hivatali mobiltelefon használatára jogosult, amelynek használatára és ellenőrzésére vonatkozó szabályokat és tájékoztatást a fenntartó adja meg.

24. A munkahelyi be- és kiléptetéssel kapcsolatos adatkezelés

170. Az Intézmény kulcsát az arra vezető által feljogosított személy, külön szabályzat szerint veheti fel, adhatja le, tarthatja magánál. A kulcs elvesztése esetén gondoskodni kell a zárcseréről.

171. Az alkalmazottak jelenléti íven dokumentálják az intézménybe érkezés és távozás tényét, időpontját.

172. A munkaköri leírásban meghatározott munkaidőt követően, az intézmény vezetőjének engedélye hiányában a munkahelyen jogszerűen nem lehet tartózkodni.

173. A jelenléti ívhez kapcsolódóan kezelhető személyes adatok köre, a természetes személy neve, aláírása, belépés, kilépés ideje. Az adatkezelés jogalapja, közérdekű jogosítvány gyakorlásának keretében végzett feladat végrehajtásának szükségessége.

174. A személyes adatok kezelésének célja, az alkalmazotti kötelezettségek teljesítésének ellenőrzése, épület és a benne elhelyezett vagyontárgyak, dokumentumok védelme.

175. Az adatok a foglalkoztatottak részére hozzáférhetők, a közös adatkezelő részére továbbítható.

176. Az adatkezelés jogalapja, a közérdekű jogosítvány gyakorlásának keretében végzett feladat végrehajtásának szükségessége, célja, a jogviszonyra vonatkozó kötelezettségek megtartásának ellenőrzése, a megfelelő munkavégzés biztosítása.

177. A személyes adatok kezelésének időtartama, 3 év.

25. A szerződéses kapcsolattartói megjelölésre és a névjegykártya használatra vonatkozó adatkezelés

178. Az intézmény szerződéses kapcsolatai során kapcsolattartót jelöl meg. A kapcsolattartó elérhetőségi adatai név, e-mail cím, mobiltelefonszám a szerződésekben, illetve az intézmény által biztosított névjegykártyán feltüntethető.

179. Az adatkezelés jogalapja, a közérdekű jogosítvány gyakorlásának keretében végzett feladat végrehajtásának szükségessége, célja az alkalmazott munkaszerződésben, illetve munkaköri leírásában meghatározott feladatainak teljesítése.

180. Az adatkezelési idő a szerződés megszűnését követő 5 évig, illetve a kapcsolattartásban bekövetkezett változásig lehetséges.

26. A bélyegző nyilvántartáshoz kapcsolódó adatkezelés

181. Az intézmény az iratkezelési szabályzatban meghatározott személyek részére bélyegzőt ad ki, akik a meghatározott bélyegző lenyomatot aláírásukkal egyidejűleg elhelyezik a képviseleti jogkörükhöz tartozó dokumentumokon.

182. Az adatkezelés jogalapja, a közérdekű jogosítvány gyakorlásának keretében végzett feladat végrehajtásának szükségessége, célja, az intézmény megfelelő, hiteles képviseletének biztosítása.

183. Az adatkezelési idő a bélyegzőn feltüntetett, illetve a jogosult személyében bekövetkezett változásig hatályos.

VI. RÉSZ

HOZZÁJÁRULÁS, MINT AZ ADATKEZELÉS JOGALAPJA

27. Rendezvényeken készült képfelvételekkel kapcsolatos adatkezelés

184. Rendezvény (családi nap, mikulás, nyugdíjas találkozó, jubileumi ünnepség, pedagógus rendezvény) szervezése esetén az intézmény részéről a rendezvényen kép-, vagy kép- és hangfelvétel készülhet. Az adatkezelés jogalapja: az érintett alkalmazott, gyermek szülőjének, törvényes képviselőjének hozzájárulása.

185. A kép- vagy kép- és hangfelvételeken történő részvétel kapcsán a képmásnak, mint személyes adatnak kezelésére – törvényi felhatalmazás hiányában – kizárólag az érintett előzetes hozzájárulásával kerülhet sor. Az érintettek hozzájárulását a **4. sz. melléklet** szerinti nyilatkozat kitöltésével kell megszerezni, kivéve, ha a felvétel:

a) nyilvános közéleti szereplés során készült felvételnek minősül,
b) tömegfelvételnek minősül, vagy
c) közérdeklődésre számot tartó tudósítás, a jelenkor eseményeiről való szabad tájékoztatás esetén.

186. A hozzájáruló nyilatkozat aláírása önkéntes. Akik nem kívánnak a felvételeken szerepelni, e joguk érvényesítése érdekében – nevet, munkakört megjelölve – nyilvántartásba kell venni.

187. A hozzájáruló nyilatkozatokat a rendezvény szervezésre kijelölt személy összegyűjti, a nyilvántartást elkészíti és elzárva tárolja. A nyilvántartott neveket kizárólag a felvételekkel kapcsolatos adatkezelést végző személyek, valamint az adatvédelmi tisztviselő ismerheti meg.

188. A rendezvényen történő kép- és hangfelvétel készítése esetén a rendezvényért felelős feladata a rendezvény megkezdése előtt felhívni az érintettek figyelmét arra, hogy amennyiben a képfelvétel készítéséhez – ide nem értve a tömegfelvételt és a nyilvános közéleti szereplést – nem járulnak hozzá, úgy azt jelezzék a jelenlévő fotós részére.

189. A jelenléti vagy regisztrációs ív alkalmazásával járó események esetén az adatkezelési tájékoztatót jól látható helyen elérhetővé kell tenni, és a jelenléti íven vagy regisztrációs adatlapon az adatkezelési hozzájárulásnak külön rubrikát kell kialakítani, és alkalmazni amennyiben az érintettől még nem áll rendelkezésre a hozzájárulással kapcsolatos nyilatkozat.

190. A személyes adatok kezelésének célja az intézményi kohézió növelése, megfelelő munkahelyi légkör kialakítása.

191. A személyes adatok a hozzájárulás visszavonásáig tárolhatók, 1 év után archiválásra kerül sor.

192. A Polgári Törvénykönyvről szóló 2013. évi V. Törvény 2:43. § külön kiemeli a képmáshoz való jog védelmét: a személyiségi jogok megsértését jelenti különösen a képmáshoz és a hangfelvételhez való jog megsértése. Az intézmény az adatkezelése során elkerüli mindazon jogsértő magatartásokat, illetve tartózkodik mindazon jogellenes mulasztástól, amelyeket a Ptk. a képmáshoz és a hangfelvételhez való jog megsértése esetén szankcionál, vagyis amelyekhez joghátrány fűződik.

193. A hatályos jogszabályok alapján egy személy arca, képmása személyes adatnak, a fényképfelvétel készítése és felhasználása pedig adatkezelésnek minősül, amihez – külön törvényi felhatalmazás hiányában – az érintett hozzájárulása szükséges. Alapvetően olyan esetben van szükség hozzájárulásra, ha a képen szereplő személy felismerhető, különösen, ha a felvétel az illető egyéni ábrázolására alkalmas.

194. Nincs szükség az érintett hozzájárulására a felvétel elkészítéséhez és az elkészített felvétel felhasználásához tömegfelvétel és nyilvános közéleti szereplésről készült felvétel esetén, tehát ha az érintettet egy tömeg részeként ábrázolják. Ide tartoznak különösen az olyan eseményeken készült felvételek, ahol megszokott a felvételek készítése, például rendezvényeken, tréningeken. Ilyen esetben hozzájárulás akkor sem szükséges, ha az érintettet a tömegben, de egyénileg kiemelve ábrázolja a felvétel. A külön hozzájárulás nélkül készíthető fényképfelvételek hozzájárulás nélkül csak olyan körben használhatók fel, amelyet az elkészítés körülményei indokolnak, például az esemény megörökítése, tájékoztatás céljából.

195. Felhasználás (nyilvánosságra hozatal) az intézmény esetében: a képfelvételnek az intézmény által használt online felületek, pl a Fehérvár Médiacentum (Helyi Tv, rádió, online felületek) kezelésében álló online felületeken rendezvények alkalmával közzétett megjelentetések.

196. A gyermekek személyes adatainak kezeléséhez szükséges a gyermek szülőjének, törvényes képviselőjének felhatalmazása.

197. Különélő vagy elvált szülők esetében csak az a szülő adhat érvényes adatkezelési nyilatkozatot, aki a szülői felügyeleti jogok gyakorlására jogosult – az adatkezelőnek azonban nem feladata, hogy ezt a kérdést mélységében vizsgálja, el kell fogadnia az erről szóló szülői tájékoztatást azzal, hogy vita esetén az ellentmondást az erre jogosult hatóságnak (gyámhatóság, bíróság) kell feloldania és ezen jogkérdésben határozatot hoznia.

198. Az általános felhatalmazás (hozzájáruló nyilatkozat) azonban nem azt jelenti, hogy az egyes fotózásokról előzetesen ne kellene tájékoztatást adni és amennyiben valamelyik fénykép feltétele kifejezetten zavarja az érintett gyermeket vagy szülőt, törlési (vagy szöveg esetén helyesbítési) kérelmének haladéktalanul eleget kell tenni.

VII. RÉSZ

SZERZŐDÉS, MINT AZ ADATKEZELÉS JOGALAPJA

28. A szerződő felek adatainak kezelése

199. Az intézmény szerződés teljesítése jogcímén a szerződés megkötése, teljesítése, megszűnése, szerződési kedvezmény nyújtása céljából kezeli a vele vevőként, szállítóként szerződött természetes személy nevét, születési nevét, születési idejét, anyja nevét, lakcímét, adóazonosító jelét, adószámát, egyéni vállalkozói, őstermelői igazolvány számát, személyi igazolvány számát, lakcímét, székhely, telephely címét, telefonszámát, e-mail címét, honlap-címét, bankszámlaszámát, vevőszámát (ügyfélszámát, rendelésszámát), online azonosítóját (vevők, szállítók listája, törzsvásárlási listák), Ezen adatkezelés jogszerűnek minősül akkor is, ha az adatkezelés a szerződéskötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges.

200. A szerződés, mint jogalap abban az esetben alkalmazható, ha a szerződés tárgya alapján a közérdekű jogosítvány gyakorlásának keretében végzett feladat végrehajtásának szükségessége nem merül fel.

201. A személyes adatokat, az intézmény vezetője által feljogosított alkalmazottja, illetve a közös adatkezelő kezelheti.

202. A személyes adatok kezelésének időtartama: a szerződés megszűnését követő 8 év a számviteli iratok megőrzése céljából.

203. Az érintett természetes személlyel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a szerződésen alapul, amely tájékoztatás történhet a szerződésben is. Az érintettet személyes adatai adatfeldolgozó részére átadható, amelyről a szerződésben tájékoztatni kell. A természetes személlyel kötött szerződéshez kapcsolódó adatkezelési tájékoztató szövegét a **11. számú melléklet** tartalmazza.

29. A jogi személy partnerek kapcsolattartóinak elérhetőségi adatai

204. Az intézmény, az érintett természetes személy nevét, címét, telefonszámát, e-mail címét, online azonosítóját kezeli, jogalapja, a közérdekű jogosítvány gyakorlásának keretében végzett feladat végrehajtásának szükségesség, célja, a megfelelő beszállítók, partnerek kiválasztása, biztosítása, az intézmény jogi személy partnerével kötött szerződés teljesítése, üzleti kapcsolattartás.

205. Az adatkezelők a szerződésben **11. számú mellékletben** nyilatkoznak arról, hogy olyan személyt jelölnek meg kapcsolattartónak, akinek ez munkaköri feladatainak ellátásához tartozik, és akit tájékoztattak arról, hogy az adatkezelő tevékenységével kapcsolatban más adatkezelők a munkáltató által biztosított eszközön, munkaidőben megkereshetik.

206. A személyes adatok címzettjei, az intézmény munkaköri leírásban meghatározott alkalmazottai.

207. A személyes adatok tárolásának időtartama: az üzleti kapcsolat, illetve az érintett képviselői minőségének fennállását követő 5 évig.

VIII. RÉSZ

JOGI KÖTELEZETTSÉG TELJESÍTÉSÉN ALAPULÓ ADATKEZELÉSEK

30. Adó-, járulék- és számviteli kötelezettségek teljesítése céljából

208. Az intézmény jogi kötelezettség teljesítése alapján, törvényben előírt adó-, járulék és számviteli kötelezettségek teljesítése (könyvelés, adózás) céljából kezeli a vevőként, szállítóként vele üzleti kapcsolatba lépő természetes személyek törvényben meghatározott adatait.

209. A kezelt adatok az általános forgalmi adóról szóló 2017. évi CXXVII. tv. 169. §, és 202. §-a alapján különösen: adószám, név, cím, adózási státusz, a számvitelről szóló 2000. évi C. törvény 167. §-a alapján: név, cím, a gazdasági műveletet elrendelő

személy vagy szervezet megjelölése, az utalványozó és a rendelkezés végrehajtását igazoló személy, valamint a szervezettől függően az ellenőr aláírása; a készletmozgások bizonylatain és a pénzkezelési bizonylatokon az átvevő, az ellennyugtákon a befizető aláírása, a személyi jövedelemadóról szóló 1995. évi CXVII. törvény (továbbiakban: Szjatv.) alapján: vállalkozói igazolvány száma, őstermelői igazolvány száma, adóazonosító jel.

210. A személyes adatok tárolásának időtartama a jogalapot adó jogviszony megszűnését követő 8 év.

211. A jelen címhez kapcsolódó személyes adatokat az intézmény adózási, könyvviteli, bérszámfejtési, társadalombiztosítási feladatait ellátó alkalmazotti és adatfeldolgozói kezelhetik.

31. Közalkalmazotti jogviszonyra vonatkozó adatkezelések

212. Az intézmény a közérdekű jogosítvány gyakorlásának keretében végzett feladat végrehajtásának szükségessége alapján, törvényben előírt közalkalmazotti jogviszony szabályszerű teljesítése céljából kezeli az alkalmazottak törvényben meghatározott adatait a 6. számú mellékletben meghatározott alkalmazotti tájékoztató szerint.

213. A jelen címhez kapcsolódó személyes adatokat az intézmény személyzeti feladatait ellátó alkalmazottjai, illetve a közös adatkezelő, adatfeldolgozók kezelhetik.

32. Kifizetői adatkezelés

214. Az intézmény a törvényben előírt adó- és járulékkötelezettségek teljesítése (adó-, adóelőleg, járulékok megállapítása, bérszámfejtés, társadalombiztosítási, nyugdíj ügyintézés) céljából kezeli azon érintettek – alkalmazottak, családtagjaik, foglalkoztatottak, egyéb juttatásban részesülők – adótörvényekben előírt személyes adatait, akikkel kifizetői (az adózás rendjéről szóló 2017. évi CL. törvény (Art.) 7. § 31. pontja) kapcsolatban áll. A kezelt adatok körét az Art. 50. §-a határozza meg, kiemelve ebből: a természetes személy természetes személyazonosító adatait (ideértve az előző nevet és a titulust is), nemét, állampolgárságát, a természetes személy adóazonosító jelét, társadalombiztosítási azonosító jelét (TAJ szám). Amennyiben az adótörvények ehhez jogkövetkezményt fűznek, az intézmény kezelheti az alkalmazottak egészségügyi (Szjatv. 40. §) és szakszervezeti (Szjatv. 47. § (2) bekezdés b) pontja) tagságra vonatkozó adatokat adó és járulékkötelezettségek teljesítés (bérszámfejtés, társadalombiztosítási ügyintézés) céljából.

215. A személyes adatok tárolásának időtartama a jogalapot adó jogviszony megszűnését követő 8 év, a szolgálati időről vagy a nyugellátás megállapítása során figyelembevételre kerülő keresetről, jövedelemről adatot tartalmazó munkaügyi iratokat az intézmény a biztosítottra, volt biztosítottra irányadó öregségi nyugdíjkorhatár betöltését követő öt évig köteles megőrizni.

216. A személyes adatokat az intézmény adózási, bérszámfejtési, társadalombiztosítási (kifizetői) feladatait ellátó alkalmazottjai, közös adatkezelő és adatfeldolgozói kezelhetik.

33. A maradandó értékű iratokra vonatkozó adatkezelés

217. Az intézmény kezeli a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény szerint maradandó értékűnek minősülő iratait abból a célból, hogy irattári anyagának maradandó értékű része épségben és használható állapotban a jövő nemzedékei számára is fennmaradjon. Az adattárolás ideje: a közlevéltár részére történő átadásig.

218. A személyes adatokat az intézmény vezetője, iratkezelést, irattározást végző alkalmazottja, a közlevéltár munkatársa kezelheti.

219. Az irattározásra, selejtezésre, levéltárba adásra vonatkozóan külön szabályzat tartalmaz rendelkezést.

IX. RÉSZ
ADATFELDOLGOZÓVAL, KÖZÖS ADATKEZELŐVEL VALÓ KAPCSOLAT TEVÉKENYSÉG

34. Közös adatkezelői tevékenységek

220. Az intézmény az alábbi tevékenység kapcsán közös adatkezelőt vesz igénybe:
-személyzeti anyagok tárolása, személyi ügyintézés: Humán Szolgáltató Intézet
-bérszámfejtés előkészítése: Humán Szolgáltató Intézet
-gyermekek, alkalmazottak nyilvántartása: KIR

221. Az intézmény a közös adatkezelővel egyedi megállapodást köt, amennyiben jogszabály nem rendezi a közös adatkezelés feltételeit.

35. Adatfeldolgozói tevékenységek

222. Az intézmény az alábbi tevékenység kapcsán adatfeldolgozót vesz igénybe:
-bérszámfejtés: Magyar Államkincstár
-e-mail szolgáltató
-honlap tárhely szolgáltató
-informatikai eszközök, szoftver beszállítók, karbantartók
-Magyar Posta

36. Adatfeldolgozói garancianyújtás

223. Az intézmény részére az adatfeldolgozó garantálja – különösen a szakértelem, a megbízhatóság és az erőforrások tekintetében – hogy a GDPR követelményeinek teljesülését, az adatkezelés biztonságát biztosító technikai és szervezési intézkedéseket végrehajtja.

224. Az intézmény részére az adatfeldolgozó biztosítja, hogy az érintett személyes adatokhoz való hozzáférésre feljogosított személyek – ha jogszabályon alapuló megfelelő titoktartási kötelezettség hatálya alatt egyébként nem állnak – az általuk megismert személyes adatok vonatkozásában titoktartási kötelezettséget vállaljanak. Az alkalmazandó titoktartási nyilatkozat szövegét a **10. sz. melléklet** tartalmazza.

225. Az adatfeldolgozó megfelelő hardver és szoftver eszközökkel rendelkezik, az adatkezelés jogszerűségének és az érintettek jogai védelmének biztosítására alkalmas műszaki és szervezési intézkedések végrehajtására kötelezettséget vállal, amelyekről tájékoztatja az intézményt.

226. Az intézmény az állami szervekkel való elektronikus kapcsolattartás jogi és technikai feltételeivel rendelkezik. Az intézmény a saját neve alatt tartja a kapcsolatot az állami szervekkel, a megbízó adatkezelő felhasználónevét, jelszavát nem kezeli.

227. Az intézmény a megbízó adatkezelő rendelkezésére bocsát minden olyan adatot, amely az adatfeldolgozó igénybevételére vonatkozó megfelelés igazolásához szükséges.

37. Az adatkezelő kötelezettségei és jogai

228. Az adatfeldolgozásra vonatkozó előzetes tájékoztatás megadása az adatkezelő felelőssége.

229. Amennyiben az érintett a jelen szerződés tárgyát képező adatkezelési műveletekkel érintett személyes adatok tekintetében az érintetti jogok gyakorlása érdekében kérelmét az adatfeldolgozóhoz nyújtja be, az érintetti jogok gyakorlását minden esetben az adatkezelő jogosult és köteles biztosítani és az érintett értesítését teljesíteni.

230. A megbízó adatkezelő jogosult ellenőrizni az adatfeldolgozónál a szerződés szerinti tevékenység végrehajtását.

231. Az adatkezelőnek a szerződésben meghatározott feladatokkal kapcsolatos utasításai jogszerűségéért az adatkezelő felel, ugyanakkor az adatfeldolgozó köteles haladéktalanul jelezni az adatkezelőnek, amennyiben az utasítás vagy annak végrehajtása jogszabályba ütközne.

232. Az adatkezelő kötelezettsége, hogy az érintett természetes személyeket jelen szabályzat szerinti adatfeldolgozásról tájékoztassa, ha jogszabály előírja, hozzájárulásukat beszerezze.

233. Amennyiben az adatvédelmi incidensekre vonatkozó értesítéshez szükséges kapcsolattartáshoz az adatkezelő új elérhetőségeket határoz meg, vagy a meglévőket módosítja, arról haladéktalanul tájékoztatja az adatfeldolgozót.

38. Az adatfeldolgozó kötelezettségei és jogai

234. Az adatfeldolgozó tevékenységét az adatkezelő írásbeli utasítása és érdeke szerint teljesíti. Az adatfeldolgozó az adatkezelő utasításaitól csak halaszthatatlan esetekben, az adatkezelő érdekében és késedelem nélküli értesítése mellett térhet el.

235. Az adatfeldolgozó biztosítja, hogy az érintett személyes adatokhoz hozzáférő személyek – ha jogszabályon alapuló titoktartási kötelezettség hatálya alatt egyébként nem állnak – titoktartási kötelezettséget vállaljanak.

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

237. Az adatfeldolgozó intézkedéseket hoz annak biztosítására, hogy az irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az adatkezelő utasításának megfelelően kezelhessék az említett adatokat, kivéve, ha az eltérésre uniós vagy tagállami jog kötelezi őket.

238. Az adatfeldolgozó gondoskodik arról, hogy a tárolt adatokhoz belső rendszeren keresztül vagy közvetlen hozzáférés útján kizárólag az arra feljogosított személyek, és kizárólag az adatkezelés céljával összefüggésben férjenek hozzá.

239. Az adatfeldolgozó gondoskodik a felhasznált eszközök szükséges, rendszeres karbantartásáról, fejlesztéséről. Az adatokat tároló eszközt megfelelő fizikai védelemmel ellátott zárt helyiségben helyezi el, gondoskodik annak fizikai védelméről is.

240. Az adatfeldolgozó a szerződésben meghatározott feladatok ellátása érdekében megfelelő ismerettel és gyakorlattal rendelkező személyeket köteles igénybe venni. Köteles továbbá gondoskodni az általa igénybe vett személyek felkészítéséről a betartandó adatvédelmi jogszabályi rendelkezések, kötelezettségek, valamint az adatfelvétel célja és módja tekintetében.

241. Az érintettől származó, érintetti jogok gyakorlása érdekében benyújtott kérelmeket, amennyiben azok az adatfeldolgozóhoz érkeznek, az adatfeldolgozó köteles az adatkezelő részére 3 munkanapon belül elektronikus úton továbbítani.

242. Amennyiben az adatfeldolgozó számára a szerződés teljesítése során bármikor olyan körülmény áll elő, mely akadályozza az időben történő teljesítést, úgy az adatfeldolgozónak haladéktalanul, de legkésőbb 3 munkanapon belül írásban értesítenie kell az adatkezelőt a késedelemről, annak várható elhúzódásáról és okairól.

243. Az adatfeldolgozó vállalja, hogy további adatfeldolgozót csak a GDPR-ben és az Infotv-ben meghatározott feltételek teljesítése mellett vesz igénybe. Az adatfeldolgozó kizárólag az adatkezelő előzetes írásbeli felhatalmazása esetén vehet igénybe további adatfeldolgozót.

244. Az adatfeldolgozó a további adatfeldolgozó igénybe vételét megelőzően tájékoztatja az adatkezelőt a további adatfeldolgozó személyéről, valamint a további adatfeldolgozó által végzendő tervezett feladatokról. Ha az adatkezelő ezen tájékoztatás alapján a további adatfeldolgozó igénybe vételével szemben kifogást emel, a további adatfeldolgozó igénybevételére az adatfeldolgozó kizárólag a kifogásban megjelölt feltételek teljesítése esetén jogosult. Ha az adatfeldolgozó további adatfeldolgozó szolgáltatásait igénybe veszi, erre köteles szerződést kötni, és a további adatfeldolgozóra is ugyanazokat az adatvédelmi kötelezettségeket telepíteni, mint amelyek az adatkezelő és az adatfeldolgozó között létrejött szerződésben szerepelnek. A további adatfeldolgozónak megfelelő garanciákat kell nyújtania a megfelelő technikai és szervezési intézkedések végrehajtására, és ezáltal biztosítania kell, hogy az adatkezelés megfeleljen a GDPR és az infotv. követelményeinek. Ha a további adatfeldolgozó nem teljesíti az adatvédelmi kötelezettségeit, az őt megbízó adatfeldolgozó teljes felelősséggel tartozik az adatkezelő felé a további adatfeldolgozó kötelezettségeinek a teljesítéséért.

245. Az adatfeldolgozó tudomására jutott minden adat, információ kizárólag az adatkezelő részére hasznosítható.

246. Amennyiben az adatfeldolgozó számára a szerződés teljesítése során bármikor olyan körülmény áll elő, mely akadályozza az időben történő teljesítést, úgy az adatfeldolgozónak haladéktalanul, de legkésőbb 3 munkanapon belül írásban értesítenie kell az adatkezelőt a késedelemről, annak várható elhúzódásáról és okairól.

247. Amennyiben az adatkezelő megítélése szerint szükséges, az adatfeldolgozó az adatkezelő külön megkeresését követően részt vesz az adatkezelő által lefolytatott adatkezelési kockázatelemzésekben és adatvédelmi hatásvizsgálatban.

248. Amennyiben az adatfeldolgozónál az adatkezelő részére feldolgozott adatok tekintetében adatvédelmi incidens következik be, az adatfeldolgozó az adatkezelő adatvédelmi tisztviselőjét haladéktalanul értesíti a **11. sz. mellékletét** szerinti incidens-bejelentési lap megküldésével.

249. Az adatvédelmi incidens felderítése, a bekövetkezett hatások feltárása, az érintettekre gyakorolt következmények elhárítása, orvoslása érdekében, továbbá a felügyeleti hatóság (NAIH) esetleges eljárása esetén az adatfeldolgozó az adatkezelővel együttműködik, a szükséges dokumentációkat rendelkezésre bocsátja.

250. Az adatfeldolgozó az adatkezelő rendelkezésére bocsát minden olyan információt, amely a GDPR 28. cikkében meghatározott kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is. Az adatfeldolgozó haladéktalanul tájékoztatja az adatkezelőt, ha úgy véli, hogy annak

valamely utasítása sérti a GDPR-t, vagy a tagállami vagy uniós adatvédelmi rendelkezéseket.

251. Az adatfeldolgozó, az adatok kezeléséhez használt adatkezelési rendszer biztonsági kockázatait – így különösen a személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből eredő – elemezte, az általa a rendszerhez rendelt technikai és szervezési intézkedések a megállapított kockázatok kezelésére alkalmasak, a kockázatok elemzését tartalmazó dokumentáció rendelkezésre áll.

252. Az adatkezelő, illetőleg a szerződésből eredő feladatai tekintetében az adatfeldolgozó köteles megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek. Ennek keretében az adatfeldolgozó szavatolja, hogy a személyes adatokat kizárólag titoktartási nyilatkozatot tett és adatvédelmi oktatásban részesített, megfelelő szaktudással rendelkező személyek végzik.

253. A titoktartási kötelezettség az Adatfeldolgozót a szerződés teljesítésére, illetőleg megszűnésére tekintet nélkül, határidő nélkül terheli.

39. Az adatfeldolgozás általános szerződési feltételei

254. Az intézmény az adatfeldolgozási tevékenységre a megbízó adatkezelővel írásbeli szerződést köt.

255. Az intézmény adatfeldolgozási tevékenységének általános szerződési feltételeit a **11. sz. melléklet** tartalmazza.

256. Az általános szerződési feltétel tartalmát a másik féllel a szerződéskötést megelőzően meg kell ismertetni, és azt a másik félnek el kell fogadnia.

X. RÉSZ

ADATVÉDELMI INCIDENSEK KEZELÉSE

40. Az adatvédelmi incidens fogalma

257. Az adatvédelmi incidens fogalmát a GDPR 4. cikk 12. pontja tartalmazza. Adatvédelmi incidens lehet például: a pendrive, laptop vagy mobil telefon elvesztése, személyes adatok elvesztése, nem biztonságos tárolása (pl. szemetesbe dobott fizetési papírok); adatok nem biztonságos továbbítása (tévesen küldött email), ügyfél- és vevő-partnerlisták illetéktelen másolása, továbbítása, szerver elleni támadások, honlap

feltörése, személyes adatot kezelő informatikai rendszer elérhetetlenné válása, személyes adat nyilvánosságra hozatala.

258. Az intézmény az adatvédelmi incidensek kezelésére vonatkozóan külön szabályzatot alkalmaz.

41. Adatvédelmi incidensek kezelés, orvoslása

259. Az adatvédelmi incidensek megelőzése, kezelése, a vonatkozó jogi előírások betartása, ellenőrzése az intézmény vezetőjének feladata.

260. Az informatikai rendszereken naplózni kell a hozzáféréseket és hozzáférési kísérleteket, és ezeket folyamatosan elemezni szükséges.

261. Amennyiben az intézmény ellenőrzésre jogosult alkalmazottjai adatvédelmi incidenst észlelnek, haladéktalanul értesíteniük kell az intézmény vezetőjét.

262. Az intézmény alkalmazottjai kötelesek írásban jelezni a vezetőnek, vagy a munkáltatói jogok gyakorlójának, ha adatvédelmi incidenst, vagy arra utaló eseményt észlelnek.

263. Az adatvédelmi incidens bejelenthető az intézmény központi e-mail címén, telefonszámán.

264. Adatvédelmi incidens bejelentése esetén az intézmény vezetője, az adatvédelmi tisztviselő – és szükség esetén a közös adatkezelő, illetve adatfeldolgozók – bevonásával haladéktalanul megvizsgálja a bejelentést.

265. Az előzetes vizsgálat során el kell dönteni, hogy valódi incidensről, vagy téves jelzésről van szó.

266. A kivizsgálás eredményéről a társság vezetője részére összefoglaló és döntési javaslat készül, valamint a feltárt hibák, hiányosságok orvoslására haladéktalanul intézkedni kell.

267. Meg kell vizsgálni és meg kell állapítani:
a) az incidens fajtáját
b) a bekövetkezésének időpontját és helyét,
c) az incidens körülményeit, hatásait,
d) az incidens során kompromittálódott adatok körét, számosságát,
e) a kompromittálódott adatokkal érintett személyek körét,
f) az incidens elhárítása érdekében tett intézkedések leírását,
g) a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.

268. Amennyiben az adatvédelmi incidenst be kell jelenteni a felügyeleti hatóság részére (NAIH), úgy erről az intézmény vezetője dönt, és felkéri az adatvédelmi tisztviselőt az online rendszerben való rögzítésre.

269. Adatvédelmi incidens bekövetkezése esetén az érintett rendszereket, személyeket, adatokat be kell határolni, el kell különíteni és gondoskodni kell az incidens bekövetkezését alátámasztó bizonyítékok begyűjtéséről és megőrzéséről. Ezt követően lehet megkezdeni a károk helyreállítását és a jogszerű működés visszaállítását.

270. Amennyiben az adatvédelmi incidens kapcsán bűncselekmény gyanúja merül fel, úgy az intézmény büntetőfeljelentést tesz.

271. Az adatvédelmi incidensek megfelelő kezelését erre irányuló vezetői döntés esetén évente gyakorolni indokolt.

42. Adatvédelmi incidensek nyilvántartása

272. Az adatvédelmi incidensekről a **2. sz. melléklet** szerinti nyilvántartást kell vezetni, amely tartalmazza:

a) az incidens jellegét,
b) az érintett személyes adatok kategóriáit, számát,
c) az adatvédelmi incidenssel érintettek körét és számát,
d) az adatvédelmi incidensről történt tudomásszerzés időpontját, körülményeit,
e) az adatvédelmi incidens körülményeit, hatásait,
f) az adatvédelmi incidens orvoslására megtett intézkedéseket,
g) a bejelentés időpontját,
h) az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

273. A nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatokat 5 évig meg kell őrizni.

43. Adatvédelmi incidens bejelentése a NAIH részére, illetve az érintettek tájékoztatása

274. Az adatvédelmi incidenseket nyilván kell tartani és amennyiben kockázatot jelentenek az érintettekre vonatkozóan, úgy a NAIH részére is be kell jelenteni. Az intézmény a NAIH honlapján elérhető online incindensbejelentő felületen regisztrál.

275. Az adatszolgáltatásnak tartalmaznia kell:

a) az incidens bekövetkezésének időpontját és helyét,
b) az incidens leírását, körülményeit, hatásait,
c) az incidens során kompromittálódott adatok körét, számosságát,
d) a kompromittálódott adatokkal érintett személyek körét,
e) az incidens elhárítása érdekében tett intézkedések leírását,
f) a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.

276. Az intézmény indokolatlan késedelem nélkül tájékoztatja az érintetteket valamennyi olyan adatvédelmi incidensről, ami olyan személyes adatokat érint, amely tekintetében az intézmény Adatkezelőként jár el, és amely valószínűsíthetően magas kockázattal jár a természetes személye jogaira és szabadságaira nézve. Az intézmény az adatvédelmi

incidensre vonatkozó tájékoztatásban világosan és közérthetően nyújt tájékoztatást az alábbiakról:

a) az adatvédelmi incidens jellege;
b) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó neve és elérhetőségei;
c) az adatvédelmi incidensből eredő, valószínűsíthető következmények;
d) az általa az adatvédelmi incidens orvoslására tett vagy tervezett intézkedések, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

277. Nem kell azonban az érintetteket tájékoztatni, ha

a) az intézmény megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták;
b) az intézmény 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; vagy
c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé (ez esetben nyilvánosan közzétett információk útján tájékoztat)

44. Nem belső adatvédelmi incidens

278. Amennyiben az intézmény elérhetőségeinek bármelyikén olyan információkhoz jut, megkeresések érkeznek hozzá, amely során egyértelmű, hogy a személyes adatokkal kapcsolatban nem merül fel adatkezelési tevékenysége (pl. rossz címre küldött csomag, boríték, elektronikus levél, stb.), úgy ezen incidenseket során az alábbiak szerint jár el:

a) az adatvédelmi incidensről nyilvántartást vezet, ezt a szabályzat **2. számú melléklete** képezi
b) haladéktalanul megteszi a szükséges lépéseket az incidens elhárítására (pl. csomag visszaküldése, feladónak visszajelzés jelzés),
c) az érintettet erről tájékoztatja;
d) a birtokába jutott személyes adatokat semmilyen célból nem kezeli.

XI. RÉSZ

ADATVÉDELMI HATÁSVIZSGÁLAT

45. Adatvédelmi hatásvizsgálat és előzetes konzultáció

279. Ha az adatkezelés a NAIH honlapján közzétett hatásvizsgálati jegyzékben szerepel, illetve 29. cikk szerinti munkacsoport WP 248. számú állásfoglalása alapján hatásvizsgálat köteles, mivel – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetők.

280. Nem kell adatvédelmi hatásvizsgálatot végezni, ha az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges vagy közérdekű jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges, és az adatkezelést jogszabály írja elő, amennyiben a jogalkotó a jogszabály-előkészítés során adatvédelmi hatásvizsgálatot végzett.

281. Az adatvédelmi hatásvizsgálat szükségességének megállapításához az intézmény vezetője az adatvédelmi tisztviselővel, illetve szükség esetén külső szakember közreműködésével megválaszolja az **1. függelékben** foglalt kérdéseket.

282. Ha a tervezett adatkezelés annak körülményeire, így különösen céljára, az érintettek körére, az adatkezelési műveletek során alkalmazott technológiára tekintettel – az adatkezeléssel várhatóan érintett személyek jogaira és szabadságaira nézve – valószínűsíthetően magas kockázatot nem azonosít, vagy megállapítást nyer, hogy az adatkezelés az adatvédelmi jogszabályban meghatározott kivételi körbe tartozik, úgy ennek tényét az intézmény vezetője írásban rögzíti.

283. Amennyiben az intézmény vezetője az adatkezeléssel várhatóan érintett személyek jogaira és szabadságaira nézve magas kockázatot azonosít vagy jogszabályi rendelkezés alapján adatvédelmi hatásvizsgálattal kötelezően vizsgálandó adatkezelési tevékenységek esete áll fenn, adatvédelmi hatásvizsgálat lefolytatásáról dönt.

284. Az intézmény vezetője elrendeli az adatvédelmi hatásvizsgálat lefolytatását, vagy írásban rögzíti mellőzésének okait. Az adatvédelmi hatásvizsgálat lefolytatásáig vagy az annak elmaradásával kapcsolatos okok írásban történő rögzítéséig az adatkezelésről szóló döntés nem hozható meg.

285. Az adatvédelmi hatásvizsgálat lefolytatásában az intézmény vezető, az adatkezelés által érintett személy, közös adatkezelő, adatfeldolgozó, külsős beszállító, vagy szakember vesz részt. Az adatvédelmi hatásvizsgálatot az adatvédelmi tisztviselő segíti. Az adatvédelmi hatásvizsgálat iratai nem nyilvánosak.

286. Az intézmény vezető, az adatvédelmi tisztviselővel közösen az adatvédelmi hatásvizsgálatról összefoglaló értékelést készít a **2. függelékben** foglaltak alapján. Az összefoglaló értékelést az intézmény vezetője hagyja jóvá, melyet követően az adatkezelést el lehet kezdeni.

287. A hatásvizsgáltot a NAIH honlapján elérhető hatásvizsgálati szoftver (PIA szoftver) alkalmazásával kell teljesíteni.

288. Az adatvédelmi hatásvizsgálat megrendeléséért az intézmény vezetője a felelős. A hatásvizsgálatba az adatvédelmi tisztviselő tanácsát ki kell kérni.

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

290. Az adatvédelmi hatásvizsgálat és előzetes konzultáció részletes szabályaira a rendelet 35-36. cikkei és az Infotv. rendelkezései irányadók.

XII. RÉSZ

AZ ÉRINTETT JOGAI

46. Az érintetti jogok gyakorlásának garanciái

291. Az intézmény honlapján az érintettek jogairól tájékoztatót kell elhelyezni és azt folyamatosan karbantartani, amely tájékoztató jelen szabályzat **3. számú melléklet**e.

292. Az érintetti jogok gyakorlására vonatkozóan az intézmény külön szabályzatot alkalmaz.

293. Az adatkezeléshez kapcsolódó igényeket az intézmény vezetője részére be kell mutatni, aki gondoskodik azok határidőn belüli megválaszolásáról.

294. Minden esetben meg kell győződni arról, hogy a jogokat gyakorolni kívánó személy jogosult-e a jogok gyakorlására. Ebből a célból az érintettnek a jog gyakorlásához kapcsolódó személyes adatait előzetesen ellenőrizni kell. Az azonosítás során csak az azonosítás teljesítéséhez szükséges adat kezelhető.

295. A jogok gyakorlása során mások jogai, szabadságai nem sérülhetnek, ezért az intézmény a meg nem ismerhető adatok anonimizálásáról gondoskodik.

296. Az intézmény annak érdekében, hogy az érintett a jogait megfelelő módon és terjedelemben gyakorolhassa, az adatvédelmi tisztviselőt bevonja az érintettnek adandó választervezet előkészítésébe.

297. Az érintett jogait díjmentesen gyakorolhatja. A visszaélésszerű joggyakorlás esetén – így különösen ugyanarra az adatra vonatkozó ismételt kérelem esetén – önköltségi díj számítható fel.

298. Az érintett jogai:

a) átlátható tájékoztatás, kommunikáció és az érintett joggyakorlásának elősegítése;
b) előzetes tájékozódás – ha a személyes adatokat az érintettől gyűjtik;
c) az érintett tájékoztatása, ha a személyes adatait nem tőle szerezték meg;
d) hozzáférési jog;
e) helyesbítéshez való jog;
f) törléshez való jog (elfeledtetéshez való jog);
g) adatkezelés korlátozásához való jog;
h) a helyesbítéséhez, törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítés joga;
i) adathordozhatósághoz való jog;
j) tiltakozáshoz való jog;
k) automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást;
l) korlátozások;
m) tájékoztatás az adatvédelmi incidensről;
n) a felügyeleti hatóságnál panaszhoz való jog (hatósági jogorvoslathoz való jog);
o) a felügyeleti hatósággal szembeni bírósági jogorvoslat joga;
p) az adatkezelővel vagy az adatfeldolgozóval szembeni bírósági jogorvoslat joga;

47. Átlátható tájékoztatás, kommunikáció és az érintett joggyakorlásának támogatása

299. Az adatkezelő az érintett részére a személyes adatok kezelésére vonatkozó valamennyi információt és tájékoztatást díjmentesen, tömör, átlátható, érthető és könnyen hozzáférhető formában, világos és egyszerű nyelvezettel megfogalmazva kell nyújtania, különösen a gyermekeknek címzett bármely információ esetében. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – dokumentáltan kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

300. Az adatkezelő elősegíti az érintett jogainak a gyakorlását, ennek biztosítása érdekében konzultál az adatvédelmi tisztviselővel.

301. Az adatkezelő indokolatlan késedelem nélkül, de legfeljebb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a jogai gyakorlására irányuló kérelme nyomán hozott intézkedésekről. E határidő a GDPR-ban írt feltételekkel további két hónappal meghosszabbítható. A határidő meghosszabbításáról és annak okairól az érintettet egy hónapon belül tájékoztatni kell.

302. Ha az adatkezelő nem intézkedik 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.

48. Előzetes tájékozódáshoz való jog, ha a személyes adatokat az érintettől gyűjtik

303. Az érintett jogosult arra, hogy az adatkezeléssel összefüggő tényekről és információkról az adatkezelést megelőzően tájékoztatást kapjon az alábbiakról:

a) az adatkezelő és képviselője kilétéről és elérhetőségeiről,
b) az adatvédelmi tisztviselő elérhetőségeiről (ha van ilyen),
c) a személyes adatok tervezett kezelésének céljáról, az adatkezelés jogalapjáról,
d) jogos érdek érvényesítésén alapuló adatkezelés esetén, az adatkezelő vagy harmadik fél jogos érdekeiről,
e) a személyes adatok címzettjeiről – akikkel a személyes adatot közlik - illetve a címzettek kategóriáiról, ha van ilyen;
e) annak tényéről, ha az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat.

304. A tisztességes és átlátható adatkezelés biztosítsa érdekében az adatkezelőnek az érintettet a következő kiegészítő információkról kell tájékoztatnia:
a) a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól;
b) az érintett azon jogáról, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról;
c) az érintett hozzájárulásán alapuló adatkezelés esetén, a hozzájárulás visszavonásához való jogról, amely nem érinti a visszavonás előtt végrehajtott adatkezelés jogszerűségét;
d) a felügyeleti hatósághoz címzett panasz benyújtásának jogáról;
e) arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása;
f) az automatizált döntéshozatal tényéről, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikáról, és arra vonatkozóan érthető információkról, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

305. Ha az adatkezelő a személyes adatokon a gyűjtésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatnia kell az érintettet az eltérő célról és az előző pontban írt minden releváns kiegészítő információról.

49. Az érintett rendelkezésére bocsátandó információk, ha a személyes adatokat nem tőle szerezték meg

306. Ha az adatkezelő a személyes adatokat nem az érintettől szerezte meg, az érintettet az adatkezelőnek a személyes adatok megszerzésétől számított legkésőbb egy hónapon belül; ha a személyes adatokat az érintettel való kapcsolattartás céljára használják, legalább az érintettel való első kapcsolatfelvétel alkalmával; vagy ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor tájékoztatnia kell a megelőző cím első két pontjában írt tényekről és információkról, továbbá az érintett személyes adatok kategóriáiról, valamint a személyes adatok forrásáról és adott esetben arról, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e.

307. A további szabályokra a megelőző cím első két pontjában írtak irányadók.

50. Az érintett hozzáférési joga

308. Az érintett jogosult arra, hogy az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha igen, jogosult arra, hogy a személyes adatokhoz és az Előzetes tájékoztatáshoz való jog kezdetű című 357. pontjában írt információkhoz hozzáférést kapjon.

309. Ha személyes adatoknak harmadik országba vagy nemzetközi szervezet részére továbbítják, az érintett jogosult tájékoztatást kapni a GDPR 46. cikk szerinti továbbításra vonatkozó garanciákról.

51. A helyesbítéshez való jog

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

311. Az adatkezelés céljára figyelemmel, az érintett jogosult arra, hogy kérje a hiányos személyes adatok – egyebek mellett kiegészítő nyilatkozat útján történő – kiegészítését is.

312. A helyesbítés, kiegészítés gyakorlása esetén a megváltozott, illetve új adatok igazolását (bemutatását) kell kérni az érintettől.

52. A törléshez való jog („az elfeledtetéshez való jog”)

313. 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) a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;

b) az érintett visszavonja az adatkezelésre vonatkozó hozzájárulását, és az adatkezelésnek nincs más jogalapja;

c) az érintett tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre,

d) a személyes adatokat jogellenesen kezelték;

e) a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;

f) a személyes adatok gyűjtésére közvetlenül gyermeknek kínált, információs társadalommal összefüggő szolgáltatások kínálásával kapcsolatosan került sor.

314. A törléshez való jog nem gyakorolható, ha az adatkezelés szükséges

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

53. Az adatkezelés korlátozásához való jog

315. Az érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést, ha:
a) az érintett vitatja a személyes adatok pontosságát, ebben az esetben a korlátozás arra az időtartamra vonatkozik, amely alatt az adatkezelő ellenőrizheti a személyes adatok pontosságát;
b) az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és helyette 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 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.

316. Az adatkezelés korlátozása esetén a személyes adatokat a tárolás kivételével csak az érintett hozzájárulásával, vagy jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez, vagy személyek jogainak védelme érdekében, vagy fontos közérdekből lehet kezelni.

317. Az adatkezelés korlátozásának idejére intézkedni kell az adatokhoz való felhasználói hozzáférés megszüntetéséről, az érintett adat honlapról való eltávolításáról, illetve a papír alapú, illetve elektronikus tárolás megváltoztatásáról.

318. Az adatkezelés korlátozásának feloldásáról az érintettet előzetesen tájékoztatni kell.

54. A helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség

319. 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.

55. Az adathordozhatósághoz való jog

320. 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 hozzájáruláson, vagy szerződésen alapul; és

b) az adatkezelés automatizált módon történik.

321. Az érintett kérheti a személyes adatok adatkezelők közötti közvetlen továbbítását is.

322. Az adathordozhatósághoz való jog gyakorlása nem sértheti a törléshez való jogot. Az adtahordozhatósághoz való jog nem alkalmazandó abban az esetben, ha az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítványai gyakorlásának keretében végzett feladat végrehajtásához szükséges.

323. Az adathordozhatósághoz való jog gyakorlása nem érintheti hátrányosan mások jogait és szabadságait.

324. Az adathordozhatósághoz való jog az adatkezelő által feldolgozás eredményeként létrejövő adatok estén nem gyakorolható.

56. A tiltakozáshoz való jog

325. Az érintett amennyiben az adatkezelés közérdekű jogosítvány gyakorlásának keretében végzett feladat végrehajtásának szükséges, jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak jogos érdeken, alapuló kezelése ellen, ideértve a 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.

326. Az előző két pontban rögzített jogra legkésőbb az érintettel való első kapcsolatfelvétel során kifejezetten fel kell hívni a figyelmét, és az erre vonatkozó tájékoztatást egyértelműen és minden más információtól elkülönítve kell megjeleníteni.

327. Az információs társadalommal összefüggő szolgáltatásokhoz kapcsolódóan az érintett a tiltakozáshoz való jogot műszaki előírásokon alapuló automatizált eszközökkel is gyakorolhatja, amelyre legkésőbb az első kapcsolatfelvétel során fel kell hívni az érintett figyelmét.

328. Ha a személyes adatok kezelésére 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.

57. Automatizált döntéshozatal, profilalkotás

329. Az érintett jogosult arra, hogy ne terjedjen ki rá a kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.

330. 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.

331. Az iménti bekezdés a) és c) pontjában említett esetekben az adatkezelő köteles megfelelő intézkedéseket tenni az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében, ideértve az érintettnek azt a jogát, hogy az adatkezelő részéről emberi beavatkozást kérjen, magyarázatot kapjon, álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be. Automatizált adatkezelés gyermekre, különleges adatokra, bűnügyi adatokra nem vonatkozhat.

58. Korlátozások

332. Az adatkezelőre vagy adatfeldolgozóra alkalmazandó uniós vagy tagállami jog jogalkotási intézkedésekkel a GDPR 23. cikkben meghatározott esetekben korlátozhatja jogok és kötelezettségek (Rendelet 12-22. cikk, 34. cikk, 5. cikk) terjedelmét, hatályát, ha a korlátozás tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát.

59. Tájékoztatás az adatvédelmi incidensről

333. 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.

334. Az adatvédelmi incidensről szóló tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább:

a) az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

c) az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

d) az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

335. Az érintettet nem kell az tájékoztatni, ha:

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, magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;

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.

60. A felügyeleti hatóságnál (NAIH) történő panasztétel joga

336. Az érintett jogosult panaszt tenni a felügyeleti hatóságnál (Nemzeti Adatvédelmi és Információszabadság Hatóság), ha megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti a GDPR-t. Az a felügyeleti hatóság, amelyhez a panaszt benyújtották, köteles tájékoztatni az ügyfelet a panasszal kapcsolatos eljárási fejleményekről és annak eredményéről, ideértve azt is, hogy az ügyfél jogosult bírósági jogorvoslattal élni.

61. A felügyeleti hatósággal szembeni bírói jogorvoslat joga

337. Az egyéb jogorvoslatok sérelme nélkül, minden természetes és jogi személy jogosult a hatékony bírósági jogorvoslatra a felügyeleti hatóság rá vonatkozó, jogilag kötelező erejű döntésével szemben.

338. Az érintett jogosult a bírósági jogorvoslatra, ha a felügyeleti hatóság nem foglalkozik a panasszal, vagy három hónapon belül nem tájékoztatja az érintettet a benyújtott panasszal kapcsolatos eljárási fejleményekről vagy annak eredményéről.

339. A felügyeleti hatósággal szembeni eljárást a felügyeleti hatóság székhelye szerinti tagállam bírósága előtt kell megindítani.

340. Ha a felügyeleti hatóság olyan döntése ellen indítanak eljárást, amellyel kapcsolatban az egységességi mechanizmus keretében az Európai Adatvédelmi Testület előzőleg véleményt bocsátott ki vagy döntést hozott, a felügyeleti hatóság köteles ezt a véleményt vagy döntést a bíróságnak megküldeni.

62. Az adatkezelővel vagy az adatfeldolgozóval szembeni bírósági jogorvoslat joga

341. A rendelkezésre álló 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 a GDPR-nak nem megfelelő kezelése következtében megsértették a jogait.

342. 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.

XIII. RÉSZ

ZÁRÓ RENDELKEZÉSEK

63. A Szabályzat megállapítása, módosítása és beépítése

343. A Szabályzat megállapítására és módosítására az intézmény vezetője jogosult.

344. Jelen szabályzatot az intézménynél helyben szokásos helyen és módon ismertetni kell az alkalmazottakkal, a szülők, szerződéses partnerek részére igény esetén meg kell küldeni, át kell adni.

345. Jelen szabályzat az intézménynél helyben szokásos helyen és módon történt kihirdetést követő napon hatályba lép.

346. A szabályzatot a jogszabályi környezet, a NAIH joggyakorlatának jelentős változása, az intézmény tevékenységében, adatkezeléseiben bekövetkező jelentős változás esetén soron kívül, egyéb esetben 3 évente felül kell vizsgálni.

347. Az intézmény vezetője gondoskodik arról, hogy az adatvédelmi szabályzatban meghatározott előírások az intézmény folyamataiban és mindennapjaiban érvényre jussanak.

348. Jelen szabályzatban foglaltak betartása és érvényesítése az intézmény valamennyi alkalmazottjának kötelessége.

349. A Szabályzat rendelkezéseit meg kell ismertetni az intézmény valamennyi alkalmazottjával (foglalkoztatottjával), és a munkavégzésre irányuló szerződésekben elő kell írni, hogy betartása és érvényesítése minden alkalmazott (foglalkoztatott) lényeges munkaköri kötelezettsége. A közalkalmazotti kinevezés kiegészítés mintáját jelen szabályzat **12. számú melléklete** tartalmazza.

350. Az intézmény jelen szabályzat alapján az alkalmazottak kinevezését kiegészíti, amennyiben törvényben meghatározott titoktartási kötelezettség nem áll fenn a személyes adatok kezelése kapcsán, jele szabályzat szerint titoktartási kötelezettséget ír elő.

351. A kinevezés módosításban a szabályzatban foglaltak be nem tartása esetére egy havi alapbéréig terjedő szankció állapítható meg, amennyiben az alkalmazott által okozott adatvédelmi incidenst legalább az adatvédelmi felügyeleti hatóság (NAIH) részére be kell jelenteni.

352. Az intézmény az adatvédelmi szabályok megszegése esetén az érintettel szemben fegyelmi eljárást kezdeményezhet, illetve büntető feljelentést tesz, amennyiben annak elmulasztásával bűncselekményt valósít meg.

353. Az intézmény állományába újonnan került olyan személyeket, akik munkakörüknél fogva személyes adatokat kezelnek, az adatvédelmi tisztviselő köteles az állományba vételt követő három munkanapon belül adatvédelmi oktatásban részesíteni és részére a szükséges jogszabályokat, belső normákat és egyéb segédanyagokat rendelkezésre bocsátani, majd az oktatást követő egy héten belül vizsgáztatásukat elvégezni.

354. Az intézmény személyes adatok kezelő állománya évente adatvédelmi oktatáson vesz részt, amelyet adatvédelmi tisztviselő tart. Az éves oktatás során incidenskezelési gyakorlat megtartására is sor kerülhet (nem valós adatokkal).

355. Az intézményvezető, a rá vonatkozó adatvédelmi szabályok betartásáról és a hozzá tartozó állomány kapcsán a szabályok érvényesüléséről gondoskodik. Az érintett vezető a 1. sz. melléklet rá vonatkozó részét figyelemmel kíséri, a változást jelzi az intézmény vezetője részére.

356. Az adatkezelő szerv adatvédelmi tevékenységének célellenőrzését az adatkezelő szerv vezetője rendelheti el. Az informatikai biztonsági feltételek teljesülését az intézmény vezetőjének döntése alapján ellenőrizni kell, eredményéről összefoglalót kell készíteni a vezető részére.

357. Jelen szabályzatot valamennyi alkalmazott számára elérhetővé kell tenni, mind elektronikusan, mind papír alapon.

358. Jelen szabályzat és annak mellékletei dr. Kozma Gergely e.v. szellemi terméke, aki fenntart minden jogot ide értve a fordítást, többszörözést, értékesítést is.

*1. függelék k*érdőív az előzetes kockázatelemzéshez

Első rész: Szükséges-e a hatásvizsgálat lefolytatása? Előzetes adatvédelmi kockázatelemzés

1. Használ vagy fejleszt-e olyan informatikai rendszert, amely személyes adatokat kezel?

Igen Nem ☐

2. Szükséges-e személyes adatokat gyűjteni a szolgáltatás működtetéséhez?

Igen Nem ☐

3. Megvalósul-e a korábbiaktól eltérő célú adatkezelés már meglévő személyes adatokkal kapcsolatban?

Igen Nem ☐

a) Alkalmaz új adatköröket gyűjtő technológiát, amely jelentő mértékben megváltoztatja az adatkezelést?

Igen Nem

b) Ha releváns szervezeti változás következik be:

– az egyesülés, beolvadás vagy egyéb szervezeti átalakulás hatással van-e az adatbázisokra?

Igen Nem

– ez a változás eredményezi új adatok kezelését vagy új nyilvánosságra hozatali eljárásokat?

Igen ☐ Nem

c) Ha ez az információ már korábban be lett gyűjtve:

– érint-e új vagy nagy létszámú érintett csoportot?

Igen Nem

– rögzít-e ezen felül további személyes adatot?

Igen ☐ Nem

4. A szolgáltatás korlátozza-e az érintettek személyes adataikhoz való hozzáféréséhez fűződő jogait?

Igen ☐ Nem

5. Tervezi-e egymást követő 12 hónapból álló időszak során nagyszámú érintettekre vonatkozó személyes adatainak kezelését?

Igen ☐ Nem ☐

6. Megvalósul-e különleges adatok, tartózkodási helyre utaló adatok, illetve gyermekekre vagy alkalmazottakra vonatkozó, széles körűnyilvántartási rendszerekben tárolt adatok kezelése?

Igen ☐ Nem

7. Megvalósul-e profilalkotás, amelyre az érintett személy tekintetében joghatással bíró vagy az egyént hasonlóan jelentő mértékben érintőintézkedések épülnek?

Igen ☐ Nem

8. Megvalósul-e egészségügyi ellátás nyújtására, járványügyi kutatásokra, mentális vagy fertőző betegségekre irányuló felmérésekre vonatkozó személyes adatok kezelése, amennyiben az adatok feldolgozására meghatározott egyénekre széles körben vonatkozó intézkedések vagy döntések meghozatala érdekében kerül sor?

Igen ☐ Nem

9. Megvalósul-e nyilvánosság számára hozzáférhetőterületek (közterületek) nagyarányú, automatizált nyomon követése?

Igen ☐ Nem ☐

10. Megvalósul-e olyan adatkezelés, amely során a személyes adatok megsértése várhatóan hátrányosan érintené az érintett személyes adatainak, magánéletének, jogainak vagy jogos érdekeinek védelmét?

Igen ☐ Nem

11. Az adatkezelő vagy adatfeldolgozó főtevékenységei olyan eljárásokat foglalnak-e magukban, amelyek jellegüknél, alkalmazási területüknél, illetve céljaiknál fogva az érintettek rendszeres és rendszerszerűmegfigyelését igénylik?

Igen ☐ Nem ☐

12. A személyes adatokat olyan jelentő számú személy számára teszi-e hozzáférhetőé, amely észszerűn elvárható módon nem korlátozható?

Igen ☐ Nem

13. Létrejön-e új azonosító vagy hozzáférési jogosultságot ellenőzőrendszer, például biometrikus azonosítás?

Igen ☐ Nem

14. Megfigyelés alatt állnak-e az érintettek helyváltoztatás, másokkal való kommunikáció vagy egyéb magatartás tanúsítása közben?

Igen Nem

15. Megvalósul-e automatizált adatfeldolgozás?

Igen ☐ Nem

16. Személyes adatok védelmének növelése érdekében elő́r-e (ha volt ilyen) a korábbinál magasabb szintűadatbiztonsági követelményeket?

Igen ☐ Nem

17. Személyes adatokkal való visszaélés megelőzése érdekében bevezetésre kerülnek-e új vagy módosított előírások?

Igen ☐ Nem ☐

18. Személyes adatok tárolásával kapcsolatban bevezetésre kerülnek-e új vagy módosított előírások?

Igen ☐ Nem

19. Megvalósul-e tudományos kutatási vagy statisztikai célból történőadatkezelés?

Igen ☐ Nem

20. Az adatkezelés kiterjed-e különleges adatokra?

Igen ☐ Nem

21. Megvalósul-e bármilyen más, magánszférát érintő magatartás?

Igen ☐ Nem

22. Végeztek-e már korábban hatásvizsgálatot? Ha a válasz igen, csatolja a dokumentumot!

Igen ☐ Nem

Második rész: Előzetes hatásvizsgálat

1. Ki a tájékoztatásra kötelezett személy (név, telefonszám, e-mail-cím)? (Ha van adatvédelmi tisztviselő, akkor az ő adatai.)

2. Mutassa be a szolgáltatás működését, felépítését!

3. Ki az adatkezelő (név, telefonszám, e-mail-cím, postai cím)?

4. Mi az adatkezelés pontos címe/helye/webhelye? (Csak akkor töltse ki, ha az eltér az adatkezelő címétől!)

5. Mi az adatkezelés célja, módja és jogalapja?

6. Mi az adatkezelés időtartama?

7. Kíván-e adatfeldolgozót igénybe venni? Ha igen, mutassa be részletesen az adatfeldolgozó személyét (kapcsolattartó, adatkezeléssel összefüggő tevékenység, adatfeldolgozó címe, adatfeldolgozás helye, technológiája stb.)!

8. Melyek a kezelni kívánt adatkörök?

9. Határozza meg a gyűjteni kívánt adatok mennyiségét, illetve az érintett személyek számát (hozzávetőlegesen)!

10. Melyek az adatfelvétel formái? Megvalósulhat az adatgyűjtés személy azonosítására alkalmas igazolvány segítségével is? Ha igen, fejtse ki!

11. Az adatszolgáltatás önkéntes? Ha igen, az érintettek megfelelő mértékben tájékoztatva vannak-e a kezelt adatok köréről, illetve jogaikról?

12. Az érintetteknek van-e lehetőségük arra, hogy adataik kizárólag meghatározott célokra történő felhasználásához nyújtsanak hozzájárulást? Ha igen, hogyan?

13. Megvalósul-e harmadik országba irányuló adattovábbítás? Ha igen, írja le a továbbítandó adatok fajtáit, a továbbítás címzettjének adatait, valamint az adattovábbítás jogalapját!

14. Fejtse ki, milyen lépéseket tesz az adatok biztonságának megőrzése érdekében!

15. Ha megfelelő szintűnek vélt az adatok biztonsága, milyen eszközök óvják az azonosítatlan hozzáféréstől?

16. A megfelelő védelmi eszközöket használja azonosítatlan hozzáférés megakadályozása érdekében? Fejtse ki álláspontját!

17. Van egyéb közlendő információja?

Harmadik rész: További analízis

1. Hogyan biztosítja az érintettek jogainak érvényesítését?

2. Fejtse ki azokat az Ön által is ismert, alternatív megoldásokat, amelyek az eredeti eljáráshoz képest a cél elérése mellett kisebb mértékben érintenék a magánszférát!

3. Milyen módszerekkel kívánja csökkenteni az azonosított kockázati tényezőket?

4. Hogyan ellenőrzi az adatok teljességét?

5. Megfelelően naprakészek-e a gyűjtött adatok? Ha igen, támassza alá válaszát!

6. Kifejtett és részletezett az adatok természete?

7. Kinek van hozzáférési joga (lehetősége) a személyes adatokhoz?

8. Mi alapján kerülnek kiválasztásra azok a személyek, akik rendelkeznek ezzel a joggal?

9. A személyes adatokhoz való hozzáférés feltételei, módja, korlátai rögzítve vannak?

10. Milyen eszközök biztosítják az adatkezelés céljától eltérő felhasználás megakadályozását?

11. Hozzáférhet-e más rendszer a saját rendszerben kezelt adatokhoz? Ha igen, fejtse ki!

12. Az adatkezelés idejének lejárta után milyen módon kerülnek törlésre az adatok? Hogyan lesz dokumentálva az adattörlés?

2. függelék az adatvédelmi hatásvizsgálatról szóló összefoglaló értékelés tartalmi elemei

1. A tervezett vagy megváltozott adatkezelés leírása:

A tervezett/megváltozott adatkezelés folyamatának leírása, melyben bemutatásra kerülnek az alábbiak:

a) adatkezelés jellege, hatóköre, körülményei;

b) a személyes adatok, a címzettek, valamint a személyes adatok tárolási időtartamának meghatározása;

c) funkcionális leírás az adatkezelési műveletről;

d) módszeres leírás az adatfeldolgozásról, az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;

e) jogalap meghatározása;

f) a személyes adatokhoz használt eszközök (hardverek, szoftverek, hálózatok, személyek, papírok vagy papíralapú továbbítási csatornák) megnevezése;

g) a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az e rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat;

h) az adatkezelésre vonatkozó, rendelkezésre álló igazgatási rendszerterv vagy folyamatleírás bemutatása;

i) hatásvizsgálatra vonatkozó szerep- és felelősségi körök meghatározása.

2. Az adatkezelési műveletek szükségességi és arányossági vizsgálata:

a) meghatározottak, kifejezettek és jogosak-e a cél(ok) [célhoz kötöttség elve – GDPR rendelet 5. cikk (1) bekezdés b) pontja];

b) az adatkezelés jogszerűsége (GDPR rendelet 6. cikk);

c) a kezelni kívánt adatok megfelelőek, relevánsak, és csak a szükséges adatokra korlátozódnak [adattakarékosság elve – GDPR rendelet 5. cikk (1) bekezdés c) pontja];

d) korlátozott tárolási időtartam [korlátozott tárolhatóság elve – GDPR rendelet 5. cikk (1) bekezdés e) pontja].

3. Meglévő vagy tervezett intézkedések: az adatkezeléssel összefüggő, a hatásvizsgálat elvégzésekor meglévő intézkedések felsorolása pl. jogosultságkezelés.

4. A jogokat és szabadságokat érintő kockázatok vizsgálata:

A kérdőívek kitöltése, valamint az érintettekkel történő esetleges konzultáció után a hatásvizsgálatot lefolytató szerv az adatkezelés minden releváns részelemének ismeretében elvégzi a kockázatkezelést, amelynek elemei az alábbiak:

a) a lehetséges kockázati tényezők azonosítása,

b) a kockázati tényezők értékelése,

c) a kockázati tényezők csökkentésére, megszüntetésére irányuló javaslatok megfogalmazása.

A kockázati tényezők azonosításában nagy szerepe van továbbá az érintettekkel való konzultációnak. A GDPR rendelet az érintettekkel való konzultációt nem szükségszerűen írja elő. Az adatkezelő „adott esetben" kéri ki az érintettek, illetve képviselőik véleményét. Ha az adatkezelő végleges döntése eltér az érintettek véleményétől, akkor dokumentumokkal alá kell támasztania annak végrehajtásának vagy elvetésének okait. Az adatkezelőnek dokumentumokkal kell indokolnia azt is, hogy miért nem kéri ki az érintettek véleményét, amennyiben úgy dönt, hogy erre nincs szükség.

4.1. Konzultáció az érintett szereplőkkel

Azonosítani kell az érintett szereplők lehetséges körét, majd megfelelő mértékben tájékoztatni kell őket az eljárásról. A tájékoztatás célja – a visszajelzések útján – a negatív hatások csökkentése, illetve a figyelem felhívása a jogorvoslati lehetőségre. A tájékoztatás során ki kell térni az eljárás menetére, idejére, várt eredményére. Az esetleges konzultációt már a tervezési/fejlesztési szakaszban célszerű elvégezni, hogy az érintettek észrevételeit, ajánlásait esetlegesen implementálni lehessen, jelentős többletköltség nélkül. Az érintetti kör nincs korlátozva, a projekt tárgyát tekintve érintett lehet állami és civil szervezet, támogató, szolgáltató, fejlesztő és az adatkezelés adatalanyai egyaránt.

Az érintettek hatásvizsgálatba való bevonásának lehetőségei:

– az egyes érintett kategóriák meghatározása és párbeszéd folytatása az egyes kategóriák képviselőivel;

– konzultációs eljárások biztosítása, hogy az érintetteknek lehetőségük legyen álláspontjaik kifejtésére;

– a tervezet érintettek számára történő hozzáférhetővé tétele.

A konzultáció formája többféle lehet: interjú, közvélemény-kutatás, meghallgatás, workshop, online konzultáció.

A tervezett adatkezelés negatív hatásainak csökkentése vagy kiküszöbölése érdekében célszerű a visszajelzéseket dokumentálni, és az adatkezelés megvalósítása során figyelembe venni.

4.2. A lehetséges kockázatok csoportjai

Személyeket érintő kockázatok:

– az adatok nem megfelelő nyilvánosságra hozatala növeli annak esélyét, hogy olyan adatokat is megosztanak, amelyeket jogszerűen nem lehetne;

– az adatkezelés célja megváltozhat, így az idő múlásával a tárolt adatokat másra használják fel az érintett tudta nélkül;

– adatbázisok összefésülése, amelynek köszönhetően olyan felhasználói profilok hozhatók létre, amelyekből új információk nyerhetők ki;

– azonosítók összekapcsolása, amely meggátolja az anonim felhasználást.

Szervezetet érintő kockázatok:

– adatvédelmi hatóság álláspontjába vagy olyan jogszabályi előírásba való ütközés, amelynek következményeként bírság vagy más szankciók is kiszabhatók;

– olyan problémák felmerülése, amelyekre csupán a projekt elindítását követően derül fény, és a kijavításuk rendkívül költségigényes;

– az adatminimalizálás elvébe ütköző felesleges, készletező, esetleg többszöri adatgyűjtés, amely így csökkentheti a projekt hatékonyságát;

– a bizonytalan és nem megfelelő adatkezelés a társadalomban bizalomvesztést eredményezhet, amely bevételcsökkenés formájában jelenhet meg;

– adatvesztés, amely az érintettek számára kárt okoz, valamint az érintettek részéről kártérítési igényt generál.

Jogi szabályozásnak való megfelelés vizsgálata:

– az adatkezelés nem felel meg a tagállami hatóság állásfoglalásaiban foglaltaknak, az ágazatspecifikus előírásoknak vagy az alkotmányjogi előírásoknak.

4.3. Az adatvédelmi kockázatok rangsorolása

Az elemzés az 1. függelékben szereplő kérdéssor alapján azonosított kockázatok és az érintett konzultáció értékelésével folytatódik. A magánszférára gyakorolt hatásuk mértéke alapján megkülönböztethető:

– alacsony (esély van a kockázat megjelenésére, de vannak enyhítő körülmények);

– közepes (valószínű, hogy megjelenik a kockázat, ha nem történik korrekció);

– magas (megjelenik a kockázat, ha nem történik korrekció) szintű kockázat.

Egy kockázat mértékét négy tényező befolyásolja:

A személyes adatkezelés alapját képező elektronikus információs rendszer kritikussága: nem kritikus = 1 kritikus = 2.

Az adatkezelés hatóköréhez tartozó adatokhoz képest (pl. az adott népesség aránya) az adatkezelés

1. kis számú = 1,

2. közepes = 2,

3. nagy számú = 3

érintett adatkezelését valósítja meg.

A kockázat elhárításának ügyviteli sürgőssége: a bejelentő nem ítéli sürgősnek = 1, a bejelentő sürgősnek ítéli = 2.

Az adatkezelés fontossága (súlya) a szervezet szempontjából: kritikus = 3, nem kritikus = 1.

A kockázati szint számértékét a tényezők összege adja.

Ha az adott eseménynél egy tényező nem értékelhető, akkor a legkisebb számértéket kell használni.

A tényezők alapján három kockázati szint használható:

Magas = 8 vagy több

Közepes = 5–7

Alacsony = 4

4.4. A „valószínűsíthetően magas kockázattal járó” adatkezelési műveletek megállapítása

Értékelési szempontok:

– Értékelés vagy pontozás: ideértve a profilalkotást és az előrejelzést is, különösen „az érintett munkahelyi teljesítményére, gazdasági helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körökre, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy mozgására vonatkozó jellemzők” alapján [GDPR rendelet (71) és (91) preambulum bekezdés]. Erre példaként említhető a pénzügyi vállalkozás, amely hitelreferencia-, pénzmosás és a terrorizmus finanszírozása elleni vagy csalásellenes adatbázist használ ügyfelei szűrésére, vagy a biotechnológiai vállalat, amely közvetlenül a fogyasztóknak kínál genetikai vizsgálatokat, hogy értékelje és előre jelezze a betegségek kockázatát és az egészségügyi kockázatokat, vagy a vállalkozás, amely viselkedési vagy üzletszerzési profilokat készít a honlapjának használata vagy böngészése alapján.

– Joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal: adatkezelés, amelynek célja a „természetes személy tekintetében joghatással bíró” vagy „a természetes személyt hasonlóképpen jelentős mértékben érintő” döntések meghozatala [GDPR rendelet 35. cikk (3) bekezdés a) pontja]. Az adatkezelés adott esetben például egyének kirekesztését vagy hátrányos megkülönböztetését eredményezheti. Az egyénekre nézve csekély vagy semmilyen hatással nem járó adatkezelés nem felel meg ennek a konkrét szempontnak. Az itt

említett fogalmakról további felvilágosítást nyújt majd a 29. cikk szerinti adatvédelmi munkacsoport soron következő, profilalkotásról szóló iránymutatása.

– Módszeres megfigyelés: érintettek megfigyelése, nyomon követése vagy ellenőrzése céljából végzett adatkezelés, többek között a hálózatokon keresztüli adatgyűjtés vagy a „nyilvános helyek nagymértékű, módszeres megfigyelése” [GDPR rendelet 35. cikk (3) bekezdés c) pontja]. Az ilyen jellegű megfigyelés azért tartozik a figyelembe veendő szempontok közé, mivel a személyes adatok gyűjtése olyan körülmények között folyhat, ahol előfordulhat, hogy az érintettek nem tudják, ki gyűjti és hogyan használja fel adataikat. Ezen kívül az egyéneknek talán nincs lehetőségük elkerülni, hogy közterületeken (vagy nyilvános helyeken) érintetté váljanak ilyen adatkezelésben.

– Különleges adatok vagy fokozottan személyes jellegű adatok: ide tartoznak a személyes adatok a GDPR rendelet 9. cikkében meghatározott különleges kategóriái (például az egyének politikai véleményére vonatkozó adatok), valamint a GDPR rendelet 10. cikkében meghatározott, büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre vonatkozó személyes adatok. Példaként említhető az általános kórház, amely nyilvántartást vezet a betegek kórtörténetéről, vagy a magánnyomozó, aki megőrzi az elkövetők adatait. A GDPR rendelet e rendelkezésein túlmenően bizonyos adatkategóriák tekinthetők úgy, hogy fokozzák az egyének jogait és szabadságait érintő lehetséges kockázatokat. Ezek a személyes adatok (a fogalom általánosan ismert jelentését tekintve) különlegesnek minősülhetnek, mivel otthoni vagy magánjellegű tevékenységekhez kapcsolódnak (például elektronikus hírközlési tevékenységekhez, amelyek bizalmassága védendő), kihatnak valamely alapvető jog gyakorlására (például helymeghatározó adatok, amelyek gyűjtése megkérdőjelezi a mozgás szabadságát), vagy az őket érintő jogsértések egyértelműen súlyos hatást gyakorolnak az érintett mindennapi életére (például pénzügyi adatok, amelyek csalásra használhatók). E tekintetben lényeges lehet, hogy az érintett vagy valamely harmadik személy már nyilvánosan hozzáférhetővé tette-e az adatokat. A személyes adatok nyilvános hozzáférhetősége az értékelés során egyik tényezőként figyelembe vehető, ha az adatok bizonyos célú további felhasználására lehet számítani. Ez a szempont olyan adatokra is vonatkozhat, mint például a személyes iratok, e-mailek, naplók, jegyzetelési funkcióval rendelkező e-olvasókból származó jegyzetek, valamint az életnaplózó alkalmazásokban tárolt, rendkívül személyes jellegű adatok.

– Nagy számban kezelt adatok: a GDPR rendelet nem határozza meg, mi értendő nagy szám alatt, jóllehet a GDPR rendelet (91) preambulum bekezdés nyújt némi iránymutatást. Mindenesetre a GDPR rendelet 29. cikke szerinti adatvédelmi munkacsoport ajánlása szerint különösen az alábbi tényezőket kell figyelembe venni annak megállapításakor, hogy az adatkezelés nagy számban történik-e:

a) az érintettek száma konkrét számadatként vagy a lakosság arányában;

b) a kezelt adatok mennyisége vagy adatfajták köre;

c) az adatkezelési tevékenység időtartama vagy állandó jellege;

d) az adatkezelési tevékenység földrajzi kiterjedése.

Adatkészletek egymással való megfeleltetése vagy összevonása például két vagy több, különböző célokból, illetve eltérő adatkezelők által végzett adatkezelési műveletből származó adatokkal, az érintett észszerű elvárásait meghaladó módon.

– Adatkészletek egymással való megfeleltetése vagy összevonása

– Kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok (GDPR rendelet 75. preambulum bekezdés): az ilyen jellegű adatok kezelése azért tartozik a figyelembe veendő szempontok közé, mivel nincs hatalmi egyensúly az érintettek és az adatkezelő között, ami azt jelenti, hogy az egyének adott esetben nem tudják adataik kezelését könnyen engedélyezni vagy ellenezni, illetve nem tudják a jogaikat gyakorolni. A kiszolgáltatott helyzetben lévő érintettek közé sorolhatók a gyermekek (ők úgy tekintendők, mint akik nem tudják tudatosan és átgondoltan ellenezni vagy engedélyezni adataik kezelését), az alkalmazottk, a lakosság különleges védelmet igénylő, kiszolgáltatottabb helyzetben lévő rétegei (mentális betegségben szenvedők, menedékkérők vagy az idősek, betegek stb.), valamint az egyének minden olyan esetben, amikor az érintett és az adatkezelő közötti kapcsolatban egyenlőtlen helyzet alakul ki.

– Új technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása: például az ujjlenyomat- és az arcfelismerés együttes használata a hatékonyabb beléptetés érdekében stb. A GDPR rendelet egyértelműen megfogalmazza [hogy „a technológia elismert állásának megfelelő” módon meghatározott új technológia használata szükségessé teheti az adatvédelmi hatásvizsgálat elvégzését [GDPR rendelet 35. cikk (1) bekezdés, (89) és (91) preambulum bekezdés]. Ennek oka, hogy az ilyen technológiák használatához újfajta adatgyűjtési és -felhasználási formák kapcsolódhatnak, ami magas kockázattal járhat az egyének jogaira és szabadságaira nézve. Az új technológiák bevezetésének személyes és társadalmi következményei tehát beláthatatlanok lehetnek. Az adatvédelmi hatásvizsgálat révén az adatkezelő megismerheti és orvosolhatja az ilyen jellegű kockázatokat. Például bizonyos, a „dolgok internetét” használó alkalmazások jelentős hatást gyakorolhatnak az egyének mindennapi életére és magánéletére, ezért szükségessé teszik az adatvédelmi hatásvizsgálat elvégzését.

– Azok az esetek, amikor az adatkezelés önmagában véve „megakadályozza, hogy az érintettek a jogaikat gyakorolják vagy szolgáltatásokat vegyenek igénybe vagy szerződést érvényesítsenek” [GDPR rendelet 22. cikk és (91) preambulum bekezdés]. Ide tartoznak az érintettek számára szolgáltatás igénybevételének vagy szerződéskötésnek a lehetővé tételére, módosítására vagy elutasítására irányuló adatkezelési műveletek. Erre példa, ha egy bank hitelreferencia-adatbázis alapján szűri ügyfeleit, hogy eldöntse, kínál-e nekik hitelt.

Az esetek többségében az adatkezelő tekintheti úgy, hogy két szempontnak megfelelő adatkezelés esetében szükség van adatvédelmi hatásvizsgálatra.

4.5. A hatásvizsgálat mellőzésének esetei:

– ha az adatkezelés valószínűsíthetően nem jár „magas kockázattal […] a természetes személyek jogaira és szabadságaira nézve” [GDPR rendelet 35. cikk (1) bekezdés];

– ha az adatkezelés a jellegét, hatókörét, körülményét és céljait tekintve nagyon hasonlít olyan adatkezelésre, amelyről már készült adatvédelmi hatásvizsgálat. Ilyen esetekben

felhasználhatók a hasonló adatkezelés adatvédelmi hatásvizsgálatának eredményei [GDPR rendelet 35. cikk (1) bekezdés];

– ha az adatkezelési műveleteket felügyeleti hatóság meghatározott, azóta változatlan feltételek mellett 2018. május előtt ellenőrizte (lásd a GDPR rendelet III. fejezet C. szakaszát);

– ha a GDPR rendelet 6. cikk (1) bekezdés c) vagy e) pontja szerinti adatkezelési művelet jogalappal rendelkezik az uniós vagy tagállami jogban, a jog szabályozza az adott adatkezelési műveletet, és az említett jogalap megállapítása során már készült adatvédelmi hatásvizsgálat [GDPR rendelet 35. cikk (10) preambulum bekezdés], kivéve, ha a tagállam kimondta, hogy az adatkezelési műveletet megelőzően hatásvizsgálatot szükséges végezni;

– ha az adatkezelés szerepel azoknak az adatkezelési műveleteknek a (felügyeleti hatóság által összeállított) nem kötelező jegyzékében, amelyekre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni.

5. A kockázatok kezelésére irányuló intézkedések:

Az azonosított kockázati tényezők kategorizálása után a következő lépés a kockázatokat csökkentő eljárások megfogalmazása, amelyek csökkentik vagy megszüntetik az adott kockázati tényezőt.

A kockázat kezelésére irányuló intézkedések bemutatása, ideértve a személyes adatok védelmét és a rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

– Az adatbiztonság informatikai szempontú meghatározása.

6. Dokumentáció, azaz a kockázatelemzés összegzése, eredményének megállapítása:

Beszámoló elkészítése, a folyamat, a fennmaradó kockázatok leírása, gazdasági szempontú értékelése. Annak indoklással alátámasztott megállapítása, hogy szükséges-e az előzetes konzultáció.

7. Nyomon követés és felülvizsgálat:

Az adatkezelő szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

A kockázatok kezelésére hozott döntések rendszeres felülvizsgálatának a vezetési folyamat részévé kell válnia. Ezen túlmenően, az azonosítás–elemzés–értékelés–kezelésfolyamat (a kockázatok karaktereitől függő gyakoriságú) rendszeres ismétlése kritikus fontosságú az időbeli reagálás biztosítása miatt. A kockázatkezelési folyamatot magát, illetve eredményét (elemzés, döntéshozatal, ellenőrzés, kiegészítve a kontroll folyamatokkal) folyamatosan dokumentálni kell, és gondoskodni kell a külső-belső érintettek megfelelő, rendszeres tájékoztatásáról is.