Iktatószám: 1738/250/2022.

ZEÓ
ZUGLÓI EGYESÍTETT ÓVODA

Zuglói Egyesített Óvoda Adatvédelmi és Adatbiztonsági Szabályzata

I. Értelmező rendelkezések, fogalmak

Az Európai Parlament és Tanács a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016/679. rendelet (a továbbiakban: **GDPR)** 4. cikkének fogalom meghatározásai alapján:

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;

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;

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;

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

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

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

címzett**:** az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy 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;

harmadik fél: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak;

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

adatvédelmi incidens: a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 3. § 5. és 6. pontja sze*rint:*

közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;

kötelezően közzéteendő közérdekű adat: a Zuglói Egyesített Óvoda által kezelt és az lnfotv. 1. mellékletében, valamint egyéb jogszabályok alapján kötelezően nyilvánosságra hozandó információk körébe tartozó adat;

közzététel: az lnfotv.-ben meghatározott adatoknak internetes honlapon - www.zeo14.hu - digitális formában, bárki számára, személyazonosítás nélkül, korlátozástól mentesen, kinyomtatható és részleteiben is kimásolható módon, a betekintés, a letöltés, a nyomtatás, a kimásolás és a hálózati adatátvitel szempontjából is díjmentesen történő hozzáférhetővé tétele;

II. Általános rendelkezések

1.§ (1) Az Adatvédelmi és Adatbiztonsági Szabályzat (a továbbiakban: Szabályzat) célja, egyrészt, hogy meghatározza a Zuglói Egyesített Óvoda (a továbbiakban: ZEÓ) által gyűjtött személyes adatok kezelése során irányadó adatvédelmi és adatbiztonsági eljárásrendet, felelősségi rendet. Másrészt a GDPR és az Infotv. rendelkezései alapján biztosítani, hogy a természetes személyek magánszféráját az adatkezelő tiszteletben tartsa, a közérdekű és a közérdekből nyilvános adatokat pedig mindenki megismerhesse és terjeszthesse.

(2) A Szabályzat **személyi hatálya** kiterjed a ZEÓ közalkalmazottaira, munkavállalóira, közfoglalkoztatottaira, valamint a ZEÓ-val megbízási jogviszonyban álló személyekre (a továbbiakban: foglalkoztatottak).

(3) A Szabályzat **tárgyi hatálya** kiterjed a GDPR és az Infotv. által meghatározott, a ZEÓ által kezelt személyes adatokra, és adatkezelési tevékenységekre, azaz az utasítás rendelkezéseit kell alkalmazni bármely azonosított vagy azonosítható személyre vonatkozó információra. Annak

eldöntése során, hogy egy személy azonosítható-e vagy sem, figyelembe kell venni minden lehetséges eszközt, amely valószínűsíthetően felhasználható az adott személy azonosítására.

(4) Az utasítás előírásait alkalmazni kell a ZEÓ által vezetett nyilvántartások, adatbázisok és valamennyi egyedileg kezelt személyes adat, továbbá dokumentum esetében.

2. § A védelem szabályai **nem alkalmazhatóak** az olyan adatokra, amelyekkel – ún. anonimmá tételük következtében - az érintett többé nem azonosítható.

III. Az adatkezelés, az adatvédelem és adatbiztonság követelményrendszere

1. Felelősségi rend

3.§ Az Adatkezelőt fokozott felelősség terheli az adatok jogszabályszerű kezeléséért, védelméért és szolgáltatásáért.

4.§ A foglalkoztatottak által végzett adatkezelésnek az adatkezelés minden szakaszában meg kell felelnie a GDPR-ban és az Infotv.-ben foglalt személyes adatok kezelésére vonatkozó elveknek.

5.§ A ZEÓ szervezeti egységei, az egyes tagintézmények szakmai feladataik ellátása során kizárólag az adott feladat, a tevékenység megítélése érdekében, a vonatkozó jogszabályok rendelkezései alapján feltétlenül szükséges - és a személyes adatok körébe tartozó - adatok gyűjtését, tárolását, rendezését, felhasználását, nyilvánosságra hozatalát, archiválását láthatják el.

6.§ (1) Az alapelvek érvényesülését biztosító eljárásrendek kidolgozásáért és betartatásáért a ZEÓ vezetői (a továbbiakban együtt: vezetők) felelősek.

(2) Az adatkezelési eljárásrendeket a vezetők az adatvédelmi tisztviselő közreműködésével dolgozzák ki. Az eljárásrendeket, az adatvédelmi és az adminisztratív adatbiztonsági kockázatok feltérképezését és az adatkezelési elvek, szabályok alkalmazásának ellenőrzését a belső kontrollrendszer részeként kell kialakítani.

7.§ (1) A ZEÓ adatvédelemmel kapcsolatos feladatainak ellátásáért, a vonatkozó jogszabályok és utasítások betartásáért az intézményvezető a felelős. Az intézményvezető feladatkörében gondoskodik:

a) a személyes adatok kezelésére vonatkozó alapelvek érvényesüléséről,

b) az adatkezelési műveletekre vonatkozó utasítások jogszerűségéről,

c) az adatok biztonságáról, az ehhez szükséges szervezési és technikai intézkedések meghozataláról, eljárási szabályok kialakításáról,

d) az adatvédelemmel összefüggő tevékenységek és felelősségek körültekintő és egyértelmű elhatárolásáról.

(2) Az adatok biztonságát szolgáló intézkedéseket a technika mindenkori fejlettségére tekintettel kell meghozni, több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene.

2. Az adatvédelem tárgya

8.§ Az adatvédelem folyamatában a védelem tárgya:

a) a ZEÓ működése során keletkezett személyes adatok teljes köre, keletkezésüktől a megsemmisítésükig

b) az adathordozók, fizikai jellegüktől függetlenül, amelyek személyes adatokat tartalmaznak. Az adathordozók lehetnek papír alapú iratok, kimutatások, naplók, fotó-és videofelvételek, elektronikus, optikai és mágneses adathordozók, adattároló és adatkezelő informatikai rendszerek a vonatkozó informatikai szabályozás részletezése szerint, továbbá
c) az a fizikai környezet, ahol az adatállomány kezelése, tárolása történik.

3. A személyes adatok kezelésére vonatkozó elvek érvényesítése

9.§ (1) A GDPR 5. cikkével összhangban az adatkezelés során a ZEÓ az alábbi elvek érvényesülését tartja szem előtt:

- jogszerűség, tisztességes eljárás, átláthatóság
- célhoz kötöttség
- adattakarékosság
- pontosság
- korlátozott tárolhatóság
- integritás és bizalmas jelleg
- elszámoltathatóság

A célhoz kötöttség, adattakarékosság, pontosság, korlátozott tárolhatóság elvek érvényesülésének biztosítása

10.§ A ZEO vezetője, illetve az egyes tagintézmények vezetői kötelesek gondoskodni arról, hogy a jogszabályon alapuló adatkezelés célhoz kötötten, a szükségesség és arányosság elve alapján indokolható minimális körben, pontos, aktuális adattartalommal és a szükséges vagy jogszabály által meghatározott időtartamra történjen. A vezetők az adatvédelmi tisztviselővel együttműködve kötelesek ellenőrizni ennek betartását a kialakított munkafolyamatok esetében jogszabályváltozás esetén vagy szükség szerint, továbbá az új munkafolyamatok kialakítása során az új munkafolyamat bevezetése előtt minden esetben.

Integritás, bizalmas jelleg elv érvényesülésének biztosítása

11.§ (1) Az adatkezelés vagy adatbiztonság valamely elve sérülésének gyanúja esetén a foglalkoztatottak kötelesek értesíteni közvetlen vezetőjüket az incidens kivizsgálása és kezelése érdekében. A vezetők kötelesek értesíteni az intézményvezetőt és az adatvédelmi tisztviselőt minden olyan esetben, amikor incidens történt, különösen abban az esetben, ha az incidens nagy mennyiségű személyes adatot érint vagy különleges személyes adatot érint.
(2) Informatikai adatbiztonság sérülésének gyanúja esetén minden esetben értesíteni szükséges az incidensről az informatikai biztonságért felelős személyt is.
(3) Az adatvédelmi incidens feltárása és kezelése, jövőbeli megelőzése érdekében lefolytatásra kerülő eljárásban a foglalkoztatottak kötelesek közreműködni.

Elszámoltathatóság elve érvényesülésének biztosítása

12.§ (1) A megfelelő szintű adatkezelési tudatosság kialakítása és fenntartása érdekében oktatásokat kell tartani:
a) jogszabályváltozás esetén a jogalkalmazást megelőzően,
b) szervezeti egység vezetője hatáskörében kezelhető adatkezelési szabálytalanság esetén az esemény kezelését követően haladéktalanul vagy
c) adatkezelési szabálytalanság esetén a szabálytalanság kezelését követően haladéktalanul.
(2) A fent nevezetteken kívül a foglalkoztatottak részére évente legalább egyszer az adatvédelmi tisztviselő adatvédelemről és adatbiztonságról oktatást tart.
(3) Az oktatásokat és a belső kontrollrendszer részeként elvégzett adatvédelmi feladatokat dokumentálni szükséges.

4. A személyes adatok kezelésére vonatkozó elvek érvényesítése

13.§ (1) A fenti pontban nevezett alapelvek érvényesülése és érvényesítése érdekében a köznevelési feladatok közmegelégedésre számot tartó ellátása során az adott feladat szerinti ügymenet részeként biztosítani kell az adatkezelés szabályainak maradéktalan betartását, a természetes személyek adatainak a védelmét a jogellenes felhasználástól.
(2) Az adatkezelés során biztosítani kell:
a) az adott egyén szempontjából fontos adatok helyes, pontos kezelését. A hibás adat előfordulása esetén annak észlelésekor hivatalból, valamint az érintett kezdeményezésekor a pontosítást haladéktalanul teljesíteni kell;
b) hogy az adott személy adatai kizárólag a jogszabály rendelkezéseivel összhangban kerüljenek feldolgozásra, rögzítésre, felhasználásra, valamint ne kerüljenek illetéktelenek birtokába;
e) hogy a személyes adatoknak a közérdekű adatokkal való együttes alkalmazásuk esetén ne akadályozzák a közérdekű adatok nyilvánosságát, szolgáltatását, de a személyes adat védelme biztosított legyen;
d) a különböző célú adatok, adatállományok és adatbázisok folyamatos vezetését, aktualizálását és az adathordozó fajtájától független folyamatos rendelkezésre állását és elérhetőségét az arra jogosultak számára. A személyes adatok tekintetében minden esetben biztosítani kell a zárt kezelést és a jogszabályok szerinti előírásoknak megfelelő hozzáférést;
e) a különböző adatok, adatállományok és adatbázisok valódiságát, pontosságát, részletességét, hitelességét;
f) hogy a hiányos, a pontatlan, a régi adatok pontosításra, aktualizálásra, és az idejét múlt adatok törlésre kerüljenek;
g) az adatok, adatállományok és adatbázisok (akár számítógépes, akár manuális) fizikai biztonságát.

IV. Az adatkezelés jogalapja

14.§ A személyes adatok kezelése kizárólag akkor és annyiban jogszerű, amennyiben legalább az alábbiak egyike teljesül:
a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek

védelme miatt szükséges;
e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.
Az első albekezdés f) pontja nem alkalmazható a közhatalmi szervek által feladataik ellátása során végzett adatkezelésre.

15.§ (1) Egy közhatalmi tevékenységet vagy egyéb közfeladatot ellátó szerv – mint költségvetési szerv – minden közjogi és magánjogi jogviszonyának, és az ahhoz járulékosan kapcsolódó adatkezelési jogviszonyainak kizárólag közfeladatai ellátásával összefüggésben lehet alanya, ettől eltérő minősége fogalmilag kizárt. Ebből fakadóan e jogalap, mintegy magába olvasztja, elnyeli a további adatkezelési jogalapokat.
(2) A ZEO adatkezelésének a jogalapja a GDPR 6. cikk (1) bekezdés e) pontja, azaz **az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges.**
(3) A 14. §-ban meghatározott jogalapok közül más jogalapot csak abban az esetben lehet az adatkezelés jogalapjául választani, ha kivételesen a GDPR 6. cikk (1) bekezdés e) pontja nem alkalmazható.

16.§ Az egyes adatkezelésekhez kapcsolódó adatkezelési tájékoztatók készítése során a GDPR 39. cikk (1) bekezdés a) pontja szerint minden esetben ki kell kérni a Hivatal adatvédelmi tisztviselőjének szakmai állásfoglalását, tanácsát.

V. Adatvédelem és adatbiztonság a munkahelyi feladatellátás során

1. Adminisztratív és informatikai adatbiztonság

17.§ Az adatkezelő köteles gondoskodni az általa kezelt adatok adminisztratív és informatikai biztonságáról. Az adatokat védeni kell a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés vagy sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

18.§ A foglalkoztatottak kötelesek a megőrzésre nem kerülő és feleslegessé vált iratok és egyéb nyomtatványok, feljegyzések megsemmisítésére, melyet - ahol rendelkezésre áll - irodai megsemmisítővel kell végrehajtani. A papírvagdalék a kommunális szemétbe üríthető.

19.§ (1) Nagy mennyiségű felesleges papírt vagy, ahol nem áll rendelkezésre irodai megsemmisítő át kell adni Budapest Főváros XIV. Kerület Zuglói Polgármesteri Hivatal Gondnoksági Osztály részére megsemmisítésre.
(2) A kommunális szemétbe (papírkosárba) ép vagy rekonstruálható formában nem kerülhet személyes, vagy egyéb okból nem nyilvános adatot hordozó papír.

20.§ (1) Személyes, vagy egyéb okból nem nyilvános adatot hordozó papír nem maradhat folyosón vagy egyéb, kulccsal nem zárható helyen őrizetlenül. Az óvodai csoportszobákat e

szempontból zárhatónak kell tekinteni.
(2) A személyes adatot tartalmazó iratok, így különösen a felvételi és mulasztási napló, az óvodai csoportnapló, a gyermek fejlődését nyomon követő dokumentáció munkaidőben sem hagyhatók asztalon vagy nyílt tárolásban az utcai vagy udvari ablakok közelében, ha arra közelről rálátás lehetséges.

21.§ (1) Az óvodai csoportszobákat munkaidőn kívül, illetve munkaidőben, a munkatársak távollétében kulcsra zárva kell tartani.
(2) A vas iratszekrényeket, lemezszekrényeket az iroda elhagyása esetén munkaidőben is zárni kell.

22.§ Személyes adatok továbbítása során az adatkezeléssel megbízott foglalkoztatott és az iratkezelésért, postázásért felelős személy együttesen felelősek azért, hogy az adatok felfedés nélkül (ép, lezárt borítékban/csomagban, a küldemény érdemi szövege ne legyen kívülről olvasható) továbbításra kerüljenek a címzett részére.

E felelősség a küldeménynek a posta részére történő átadásig tart.

23.§ Az egyes óvodák épületének területén őrizetlenül hagyott, illetve elveszett, majd megtalált iratokat, okmányokat a ZEO a székhelyén őrzi a személyazonosságát igazoló érintett (képviselője, gondnoka, megbízottja) részére történő átadásig. Az érintettet az irat, okmány előkerüléséről az intézményvezetőt értesíti.

24. § A ZEÓ az adatnyilvántartások rendszerének felépítése, a jogosultságok meghatározása, és egyéb szervezeti intézkedések útján gondoskodik arról, hogy a személyes adatokat tartalmazó iratokat csak azok a foglalkoztatottak ismerhessék meg, akiknek erre munkakörük, feladatuk ellátása érdekében szükségük van.

25.§ Személyes adatot tartalmazó Excel táblázatot elektronikus levélben küldeni egyéb címzett részére kizárólag oly módon lehet, ha az Excel táblázatot jelszó védelemmel látjuk el. A címzett részére a küldött Excel táblázat megtekintéséhez szükséges jelszót külön emailben vagy telefonon keresztül adjuk meg.

26.§ (1) Az óvodák épületéből személyes adatot tartalmazó dokumentumot, naplót kivinni nem lehet.
(2) A foglalkoztatott által az otthoni munkavégzéshez esetlegesen szükséges személyes adatot tartalmazó iratot adathordózóra csak abban az esetben lehet kimenteni, ha az adathordozót jelszóval védjük.

2. Adatvédelem a szülőkkel/ a szülői felügyeleti jogot gyakorló személlyel történő kapcsolattartás során

27.§ A személyes adatok kezelésével kapcsolatos ügyekben csak a feladatkör szerint illetékes személy járhat el, működhet közre (ZEÓ vezetője, tagintézmény vezető)

28.§ 37.§ A gyermek szülője/szülői felügyeleti jogot gyakorló személy és a kíséretében levő személyek csak az ZEÓ közalkalmazottai jelenlétében tartózkodhatnak az irodában, várakozásra a várót, folyosót - vehetik igénybe.

29.§ Telefonon történő hivatalos beszélgetést zárt (csukott) ajtók mögött lehet folytatni. A gyermek szülője/szülői felügyeleti jogot gyakorló személy jelenlétében csak saját gyermeke ügyében folytatható telefonbeszélgetés, ezen kívül általános jellegű információk továbbíthatók harmadik személy részére.

30.§ Fogadóóra tartása esetén egyidejűleg egy gyermek szülője/szülői felügyeleti jogot gyakorló személy lehet egy helyiségben.

31.§ Nem azonosított személy, telefonáló, elektronikus levelet küldő nem kaphat a gyermekről érdemi információkat, sem személyes adatok nem adhatók ki nem azonosított személy részére. Azonosítatlan személy csak általános tájékoztatásban részesülhet, illetve számára közérdekű adatok adhatók ki.

32.§ Személyes adatot tartalmazó érdemi döntés és egyéb személyes adatot tartalmazó irat kizárólag ügyfélkapun keresztül vagy postai úton küldhető, ezen iratokat elektronikus levélben küldeni nem lehet.

33.§ Adatszolgáltatás személyes adatokat tartalmazó adatbázisból az alábbi módon történhet, ha jogszabály eltérően nem rendelkezik:

a) az érintett a ZEÓ által kezelt saját személyes adataiba betekinthet, arról tájékoztatást kérhet úgy, hogy ezalatt más természetes személy személyes adatait nem ismerheti meg,

b) az érintett megkeresésére válaszolva, személyes adatokat szolgáltató okiratot személyenként kell elkészíteni és iktatni, amennyiben ez nem lehetséges, az iratot anonimizálni szükséges.

3. Szerződések adatvédelmi rendelkezései, adatfeldolgozói szerződések

34.§ Személyes adatok kezelését eredményező szerződések adatvédelmi rendelkezései szövegezéséhez a szerződés előkészítése során az adatvédelmi tisztviselő tanácsát ki kell kérni.

4. Számítástechnikai és egyéb adatkezelésre alkalmas eszközök munkahelyi használata

35.§ (1) A foglalkoztatottak a rendelkezésükre bocsátott munkaeszközöket kizárólag munkavégzés céljából használhatják, a számítástechnikai eszközök magánhasználata nem megengedett.

(2) Ha a foglalkoztatott a számítástechnikai eszközön a 44. § (1) bekezdésében meghatározottakkal ellentétben munkaviszonnyal össze nem függő személyes adatot tárol, a munkáltató a magánszférát tiszteletben tartva köteles eljárni, így nem kezelheti az ily módon tárolt személyes adatot, továbbá lehetőséget kell biztosítania a foglalkoztatott számára a magánadatokkal való rendelkezésre.

(3) A munkáltató a foglalkoztatottaknak a munkavégzés céljából rendelkezésre bocsátott munkaeszközök (számítógép, laptop, nyomtató) használatát jogosult ellenőrizni. Az ellenőrzés a munkavégzéssel összefüggő indokolt cél lehet.

(4) Az ellenőrzésnek az elérni kívánt céllal arányosnak kell lennie, nem sértheti a foglalkoztatott alapvető jogait.

(5) A foglalkoztatottak által használt munkaeszközök munkáltató általi ellenőrzése akkor jogszerű, ha az ellenőrzés pontos részleteiről, az ellenőrzést megelőzően a GDPR előírása szerinti formában és módon tájékoztatják a foglalkoztatottat. Az ellenőrzésről jegyzőkönyvet kell felvenni.

36.§ Az adatbiztonság vagy az informatikai rendszer védelme okán az informatikai hálózatot üzemeltető, fenntartó rendszergazda vagy informatikus az informatikai vagy egyéb eszköz tartalmába jogosult betekinteni. Az így megismert adatokat harmadik személy számára – így a munkáltató részére – nem jogosult továbbítani.

VI. Érintetti jogok érvényesülése

37. § A GDPR 6. cikk (1) bekezdés e) pontja szerinti jogalap esetén az érintettet a GDPR 13. és 14. cikke szerint a következő jogok illetik meg.

1. *A hozzáféréshez való jog*

Az érintett jogosult arra, hogy a ZEÓ-tól tájékoztatást kérjen arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy megismerje azt, hogy a ZEÓ
- mely személyes adatait;
- milyen jogalapon;
- milyen adatkezelési cél miatt;
- mennyi ideig kezeli;
- a ZEÓ kinek, mikor, milyen jogszabály alapján, mely személyes adataihoz biztosított hozzáférést vagy kinek továbbította a személyes adatait;
- milyen forrásból származnak a személyes adatai;
- történik-e automatizált döntéshozatal.

A ZEÓ az adatkezelés tárgyát képező személyes adatok másolatát az érintett erre irányuló kérésére első alkalommal díjmentesen bocsátja a rendelkezésére, ezt követően adminisztratív költségeken alapuló, ésszerű mértékű díjat számíthat fel. Az adatbiztonsági követelmények teljesülése és az érintett jogainak védelme érdekében a ZEÓ köteles meggyőződni az érintett és a hozzáférési jogával élni kívánó személy személyazonosságának egyezéséről, ennek érdekében a tájékoztatás, az adatokba történő betekintés, illetve azokról másolat kiadása is az érintett személyének azonosításához kötött.

2. *A helyesbítéshez való jog*

Az érintett személy kérheti, hogy a ZEÓ módosítsa valamely személyes adatát. Amennyiben az érintett hitelt érdemlően igazolni tudja a helyesbített adat pontosságát, a ZEÓ a kérést legfeljebb egy hónapon belül teljesíti, és erről az általa megadott elérhetőségen értesíti az érintett személyt.

3. *A zároláshoz (adatkezelés korlátozásához) való jog*

Az érintett személy kérheti, hogy a személyes adatai kezelését a ZEÓ korlátozza (az adatkezelés korlátozott jellegének egyértelmű jelölésével és az egyéb adatoktól elkülönített kezelés biztosításával) amennyiben:
- vitatja a személyes adatai pontosságát (ebben az esetben a ZEÓ arra az időtartamra korlátozza az adatkezelést, amíg ellenőrzi a személyes adatok pontosságát);
- az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását;
- az adatkezelőnek már nincs szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;
- az érintett 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).

4. *A tiltakozáshoz való jog*

Az érintett személy bármikor tiltakozhat az adatkezelés ellen, ha álláspontja szerint a ZEÓ a

személyes adatát nem az adatkezelési tájékoztatóban megjelölt céllal összefüggésben kezelné. Ebben az esetben a ZEÓ-nak kell igazolnia, hogy a személyes adat kezelését 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.

5. *A törléshez való jog*

Az érintett csak akkor élhet a törléshez való jogával, ha a ZEÓ-ra ruházott közhatalmi jogosítványok gyakorlása keretében végzett, vagy a Hatóság közérdekű feladatainak végrehajtásához az adat nem szükséges.

6. *Jogorvoslathoz való jog*

Ha az érintett úgy ítéli meg, hogy a ZEÓ a személyes adatainak kezelése során megsértette a hatályos adatvédelmi követelményeket, akkor

a) panaszt nyújthat be a Nemzeti Adatvédelmi és Információszabadság Hatósághoz, cím: 1055 Budapest, Falk Miksa utca 9-11., postacím: 1374 Budapest, Pf. 603., E-mail: ugyfelszolgalat@naih.hu, honlap: www.naih.hu)

b) lehetősége van adatainak védelme érdekében bírósághoz fordulni, amely az ügyben soron kívül jár el. Ebben az esetben szabadon eldöntheti, hogy a lakóhelye (állandó lakcím) vagy a tartózkodási helye (ideiglenes lakcím), illetve a Hatóság székhelye szerint illetékes törvényszéknél nyújtja-e be keresetét. A lakóhelye vagy tartózkodási helye szerinti törvényszéket megkeresheti a http://birosag.hu/ugyfelkapcsolatiportal/birosag-kereso oldalon. A ZEO székhelye szerint a perre a Fővárosi Törvényszék rendelkezik illetékességgel.

VII. Térfigyelő kamerák alkalmazása

38. § A ZEÓ egyes tagintézményei épületeikben, azok zárt udvarán zártláncú térfigyelő kamerarendszert üzemeltet. A kamerákkal kapcsolatos adatkezelésre külön adatkezelési tájékoztató vonatkozik, amely elérhető az egyes tagintézményekben.

VIII. Adatkezelési tevékenységek nyilvántartása

39. § Az adatvédelmi tisztviselő legalább 3 évente, de jogszabályváltozást követően haladéktalanul felülvizsgálja, aktualizálja az adatleltárt.

40. § A ZEÓ vezetője és az egyes tagintézmények vezetői kötelesek együttműködni az adatvédelmi tisztviselővel az adatkezelési tevékenységek nyilvántartásának felvételében és felülvizsgálatában, kötelesek határidőben pontos adatokat átadni az adatvédelmi tisztviselő részére.

41. § (1) A ZEÓ vezetője az új adatkezelési tevékenységet, annak megkezdését megelőzően, vagy a már folyamatban lévő adatkezelés körülményeiben bekövetkező változást a nyilvántartás szerinti adatkörök vonatkozásában, haladéktalanul köteles bejelenteni az adatvédelmi tisztviselőnek az adatvedelem@zuglo.hu címen

(2) A bejelentés alapján az adatvédelmi tisztviselő az új adatkezelési tevékenységet rögzíti, vagy módosítja a nyilvántartásban szereplő adatokat. Szükség esetén az illetékes szervezeti egységgel vagy egységekkel is konzultál.

(3) Az adatkezelési tájékoztatót és jelen szabályzatot a ZEÓ honlapjára fel kell tölteni.

IX. Adatvédelmi hatásvizsgálat

42.§ (1) Az adatvédelmi hatásvizsgálatot a GDPR 35. és 36. cikke alapján az adatvédelmi tisztviselő irányításával egy munkacsoport végzi, melynek tagjai az adatvédelmi tisztviselő, az informatikai munkatárs, a ZEÓ vezetője vagy a vezető által kijelölt munkatárs.

(2) Adatvédelmi hatásvizsgálat elvégzésére van szükség, ha olyan új technológia, program, rendszer, alkalmazás vagy olyan új eszköz használata kerül bevezetésre, amely személyes adatokat kezel vagy alkalmas ezek kezelésére.

43.§ (1) Az adatvédelmi hatásvizsgálatnak tartalmaznia kell:

a) az adatkezelés bemutatását, ennek körében különösen a kezelt személyes adatok körét, a személyes adatok kezelésének célját, jogalapját, a tárolás időtartamát, a címzetteket és azokat a személyeket, akik az adatokhoz hozzáférhetnek

b) az adatkezelés folyamatát az adatgyűjtéstől az adatok megsemmisítéséig

c) az adatkezeléshez kapcsolódó felelősségi viszonyokat

d) a személyes adatok kezelésére szolgáló eszközöket (operációs rendszerek, alkalmazások, adatbázis-kezelő rendszerek, helyiségek, egyéb eszközök)

e) annak bemutatását, hogy a gyűjtött adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak, a szükségesre korlátozódnak (adattakarékosság)

f) adatminőséget biztosító intézkedéseket (pontosság)

g) azt, hogy az érintetteket milyen módon tájékoztatják az adatkezelésről

h) a hozzájáruláson alapuló adatkezelés esetében a hozzájárulást az érintettől milyen módon szerzik be, a hozzájárulások nyilvántartása milyen módon történik, azok visszakereshetőségének biztosítását

i) hogyan biztosítják az érintetti jogokat (hozzáférés, adathordozhatóság, helyesbítés, törlés, korlátozás, tiltakozás)

j) adatfeldolgozó részére milyen körben, milyen módon, célból, jogalappal történik a személyes adatok továbbítása, adatfeldolgozói kötelezettségeket, adatkezelő ellenőrzési kötelezettségét, jogosultságát

k) az Európai Unión kívülre történő adattovábbítás esetén az érintett országok megnevezését, továbbá, hogy az adatkezelés és - tárolás megfelelő védelmi szintje biztosított-e

l) Európai Unión belüli adattovábbítás leírását az adatkezelésre vonatkozó szabályok szerint

m) adatvédelmi incidens elkerülése, illetve annak megvalósulása esetén annak kezelése érdekében tervezett intézkedéseket, amelyek hozzájárulnak az adatbiztonság megteremtéséhez

n) adatkezelési kockázatok – adatokhoz való jogosulatlan hozzáférés, adatok véletlen vagy jogellenes megváltoztatása, adatvesztés - feltérképezését a kockázat súlyossága és a bekövetkezésének valószínűsége alapján

o) az adatvédelmi tisztviselő véleményét

p) Az adatvédelmi hatásvizsgálat 1 példányát a ZEÓ székhelyén, 1 példányt az adatvédelmi tisztviselőnél kell az iratkezelés szabályai szerint őrizni.

(2) A vizsgálat jelentéssel zárul, amely nem nyilvános.

X. Adatvédelmi incidens kezelése

44.§ (1) *Adatvédelmi incidens* a GDPR 4. cikk 12. pontja szerint fogalom meghatározása szerint 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.

(2) Adatvédelmi incidens észlelése esetén a foglalkoztatott kötelessége a tagintézmény vezetőjét haladéktalanul, de legkésőbb 1 munkaórán belül tájékoztatni az incidensről.

(3) A ZEÓ vezetője tájékoztatja az *adatvédelmi tisztviselőt* és informatikai adatbiztonság vélhető sérülése esetén az *informatikus szakembert,* függetlenül attól, hogy az adatvédelmi incidens 3. személy által történt bejelentés-, adatfeldolgozói tevékenységgel összefüggő feladat ellátás során vagy saját munkakörben történt észlelés során jutott a belső szervezeti egység tudomására.

(4) Az adatvédelmi incidensről szóló tájékoztatást az adatvedelem@zuglo.hu email címre kell megküldeni.

45.§ (1) A tájékoztatással egy időben az incidens elhárítása érdekében szükséges és megfelelő intézkedéseket is meg kell tenni.

(2) A tájékoztatásnak tartalmaznia kell:

a) az incidens (észlelt esemény) leírását
b) az incidens észlelésének időpontját
c) az érintettek körét és
d) amennyiben megbecsülhető, az érintettek hozzávetőleges számát.

46.§ Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az 55. cikk alapján illetékes felügyeleti hatóság (Nemzeti Adatvédelmi és Információszabadság Hatóság) által e célra biztosított elektronikus felületen, - kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

47.§ Tudomásszerzésnek az az időpont tekinthető, amikor az adatkezelő ésszerű mértékű bizonyossággal rendelkezik arról, hogy olyan biztonsági esemény történt, amely személyes adatokkal kapcsolatos jogellenes műveletekhez vezethet.

48.§ Annak eldöntése, hogy az adatvédelmi incidens kockázati szintje, az eset összes körülményeit

és az alkalmazott adatbiztonsági intézkedéseket figyelembe véve miként minősül, az adatvédelmi tisztviselőből, az informatikai szakemberből, valamint a ZEÓ vezetője és/vagy az általa kijelölt munkatársából álló munkacsoport feladata. A munkacsoport összehívását az adatvédelmi tisztviselő kezdeményezi. Sürgős esetben elektronikus úton történő kommunikáció is megengedett.

49.§ Az adatvédelmi tisztviselő, az informatikai szakember, A ZEÓ vezetője és/ vagy az általa kijelölt munkatárs feltárja az adatvédelmi incidens okait, az incidens bekövetkezésének időpontját, az incidenssel érintett személyes adatok körét, az érintettek körét és számát. Amennyiben az érintettek száma nem határozható meg pontosan, akkor a hozzávetőleges számát.

50. § Az adatvédelmi tisztviselő a vizsgálatot folyamatosan dokumentálja.

51.§ Az adatvédelmi incidensről - a GDPR-ban előírt esetben - a ZEÓ vezetője tájékoztatja az érintettet. A tájékoztatási kötelezettség jelzése és a tájékoztatás elkészítése az adatvédelmi tisztviselő és az informatikai vezető vagy munkatárs feladata.

52.§ (1) Az adatvédelmi incidens kivizsgálásának eredménye alapján az adatvédelmi tisztviselő, az érintett szervezeti egység vezetője és az informatikai adatbiztonság sérülése esetén az informatikai szakember intézkedési terv javaslatot készít.

(2) Az intézkedési tervben a ZEÓ vezetője meghatározza:

a) az adatvédelmi incidens orvoslására teendő intézkedéseket, beleértve az incidensből eredő hátrányos következmények enyhítését

b) a jövőbeni incidensek elkerülése érdekében teendő intézkedéseket és

c) a feladatok végrehajtásának határidejét, felelősé(ei)t.

53.§ Az adatvédelmi incidenseket, az incidens feltárását rögzítő dokumentumokat, az intézkedési tervet, annak végrehajtásáról szóló beszámolót az adatvédelmi tisztviselő nyilvántartja. A dokumentálásban az incidens kezelésének felelősei kötelesek együttműködni.

XI. Az adatvédelem szervezete

1. Az adatvédelmi tisztviselő feladatai

54. § A GDPR 37. cikk (1) bekezdés a) pontja szerint az adatkezelő és az adatfeldolgozó adatvédelmi tisztviselőt jelöl ki minden olyan esetben, amikor az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat.

55.§ Az adatvédelmi tisztviselő beosztásában közvetlenül a jegyző alá tartozik, a szervezeti egységet tekintve pedig az Igazgatási és Hatósági Főosztályhoz tagozódik be.

56.§ Az adatvédelmi tisztviselő:

a) figyelemmel kíséri és értelmezi az információs önrendelkezést, a személyes adatokat, a közérdekű és közérdekből nyilvános adatokat érintő jogszabályokat és állásfoglalásokat, azokat a ZEÓ tevékenységének folyamataira alkalmazza

b) javaslatot tesz az adatvédelemmel összefüggő belső szabályozórendszerre, megírja, és

folyamatos aktualizálja az adatvédelmi és adatbiztonsági szabályzatot, azt a kapcsolódó dokumentumokkal összehangolja

c) közreműködik, illetőleg segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában

d) ellenőrzi az adatkezelésre vonatkozó jogszabályok és szabályzatok rendelkezéseinek betartását, az adatbiztonsági követelmények érvényesülését mind a papír alapú, mind az elektronikus eljárások során

e) ellenőrzi a kötelezően közzéteendő közérdekű adatok publikálásának teljesítését, szükség szerint intézkedést kezdeményez

f) kivizsgálja a tárgyban hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy adatfeldolgozót

g) panasz esetén, illetve hivatalból vizsgálatot kezdeményez az adatkezelésre, az érintettek jogai érvényesülésére, valamint a közérdekű adatok közzétételére vonatkozó rendelkezések betartása érdekében

h) tájékoztatást nyújt az adatvédelmi ismeretekről

i) részt vesz a belső kontrollrendszer folyamatok kialakításában, módosításában az adatvédelem célkitűzéseinek megvalósítása érdekében

j) részt vesz a követelmények meghatározásában az informatikai rendszerek kialakítására és üzemeltetésére, az informatikai biztonság megfelelő szintjének elérése és fenntartása érdekében, a rendszerek életciklusának folyamatában

k) állásfoglalásával, javaslatával közreműködik a közérdekű adatigénylések megválaszolásában

l) közreműködik az adatvédelmi hatásvizsgálat elvégzésében;

m) az adatvédelmi incidens eseményét, a körülmények feltárását, a megtett intézkedéseket dokumentálja, jogszabályban előírt esetben a NAIH részére szolgáló tájékoztatót elkészíti;

n) évente általános adatvédelmi oktatást, szükség esetén eseti oktatást tart a foglalkoztatottak részére. Az oktatásokat dokumentálja

o) vezeti az adatvédelmi incidensekkel kapcsolatban megtett intézkedésekről szóló nyilvántartást, a személyes adatok védelmével kapcsolatosan hozzá érkezett panaszokról, bejelentésekről szóló nyilvántartást, a közérdekű adatok nyilvánosságával kapcsolatosan hozzá érkezett panaszokról, bejelentésekről szóló nyilvántartást

2. A foglalkoztatottak kötelezettségei

57. § A ZEÓ valamennyi foglalkoztatottja köteles:

a) az adatvédelmi előírásokat megismerni, és maradéktalanul betartani;

b) előzetesen egyeztetni az adatvédelmi tisztviselővel a személyes adatok kezelését vagy a közérdekű adatok nyilvánosságát érintő ügyekben, továbbá a Nemzeti Adatvédelmi és Információszabadság Hatóság közreműködését igénylő kérdésekben;

c) a hozzá érkező adatigénylési kérelmekről, bejelentésekről tájékoztatni az adatvédelmi tisztviselőt az adatvedelem@zuglo.hu címen

d) tájékoztatni az adatvédelmi tisztviselőt a felmerült adatvédelmi visszásságról;

e) az adatvédelmi tisztviselő észrevétele esetén az adatkezeléssel kapcsolatosan feltárt visszásságot haladéktalanul megszüntetni;

f) adatokat, iratokat az adatvédelmi tisztviselő kérésére adatvédelmi vizsgálathoz, hatásvizsgálathoz, incidenskezeléshez átadni. E feladat ellátása során valamennyi foglalkoztatott felelősséggel tartozik a személyes adatokat tartalmazó dokumentumok teljes körűségéért.

XII. Záró rendelkezések

58.§ A személyes adatok kezelésével kapcsolatos, a jelen utasításban nem szabályozott kérdések tekintetében a GDPR, az Infotv., valamint az ágazati jogszabályok rendelkezései az irányadók.

59.§ Ez a Szabályzat 2022. szeptember 1-jén lép hatályba.

60.§ A foglalkoztatottak jogviszony létesítésekor kötelesek a Szabályzatot megismerni, és ezt a megismerési záradék aláírásával igazolni (1. számú melléklet).

Budapest, 2022. szeptember 1.

Farkas Tibor Jánosné
intézményvezető

Zuglói Egyesített Óvoda 1144 Budapest, Füredi park 6-8.