A SZÉKESFEHÉRVÁRI NAPSUGÁR ÓVODA

Adatvédelmi és adatbiztonsági szabályzata

Hatályos: 2023.09.03.

Tartalom

Preambulum

A Székesfehérvári Napsugár Óvoda (továbbiakban: Óvoda) 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 Óvodaigazgató kiadja jelen adatvédelmi és adatbiztonsági szabályzatot (továbbiakban: szabályzat).

A szabályzat az elfogadást követő naptól hatályba lép, és az Óvoda alkalmazottaival, az óvodával szerződéses kapcsolatban állókkal az őket érintő terjedelemben meg kell ismertetni.

Az adatkezelő adatai

Székesfehérvári Napsugár Óvoda
székhely: 8000 Székesfehérvár, Salétrom utca 8.
tagóvoda: **Székesfehérvári Napsugár Óvoda Nefelejcs Tagóvodája**
cím: 8000 Székesfehérvár, Nefelejcs utca 54.
tagóvoda: **Székesfehérvári Napsugár Óvoda Szivárvány Tagóvodája**
cím: 8000 Székesfehérvár, Zombori út 19.
honlap címe: https://www.napsugar-nefelejcs-szivarvanyovoda.hu/
e-mail cím: napsugarovodaszfv@gmail.com
telefonszám: 22/312-305
adószám: 16700204-2-07
képviselő: Mályi Lilla telefon: 22/312-305

A szabályozás célja

Az Óvoda adatvédelmi, adatbiztonsági szabályzatának (a továbbiakban: Szabályzat) kibocsátásának célja, hogy 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.

A szabályzat célja azon belső szabályok megállapítása és intézkedések megalapozása, amelyek biztosítják, hogy az Óvoda adatkezelő és adatfeldolgozó tevékenysége megfeleljen GDPR és az Infotv. rendelkezéseinek.

A szabályzat hatálya

A Szabályzat hatálya természetes személyre vonatkozó személyes adatok Óvoda általi kezelésére terjed ki, az egyéni vállalkozót, egyéni céget, ügyfeleket, vevőket, szállítókat e szabályzat alkalmazásában természetes személynek kell tekinteni.

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

Az iratkezeléssel összefüggő szabályokat az Óvoda iratkezelési szabályzatával összhangban kell alkalmazni.

Az Óvoda elektronikus információs rendszereiben tárolt személyes adatok védelmére irányuló követelményeket az Informatikai Biztonsági Szabályzattal összhangban kell alkalmazni.

Jelen szabályzatban nem szereplő kérdésekben a GDPR szabályai szerint kell eljárni.

Az Óvoda adatvédelmi szervezetének felépítése

Az Óvoda felelősségi rendszere

Az Óvodaigazgató felel az intézményben az adatkezelés jogszerűségéért és a személyes adatok védelméért. Ennek értelmében:

a) az óvoda adatvédelmi és adatbiztonsági intézményrendszerének kiépítéséért és működtetéséért, ennek keretében az intézmény által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosítását célzó, hatáskörébe tartozó intézkedések megtételéért;
b) a közalkalmazottak adatvédelmi oktatásáért és továbbképzéséért;
c) az óvoda 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) az adatvédelmi követelmények érvényre juttatásért
f) a Szabályzatban foglaltak ellenőrzéséért, annak megsértése esetén a hiányosságok, szabálytalanságok felszámolásáért.

Az óvodában foglalkoztatottak felelőssége:

a) a szabályzatban leírtaknak megfelelően kezelik azon személyes adatokat, amelyek a feladataik ellátása során a tudomásukra jutott
b) betartják az intézmény által előírt adatvédelmi utasításokat, tudomásul bírnak arról, megszegésük esetén felelősségre vonhatóak

c) tudásukat naprakészen tartják, annak érdekében, hogy az adatvédelmi, adatbiztonsági előírásoknak eleget tegyenek, az adatvédelmi incidensek gyanúját felismerjék.

Az Óvoda szervezetén kívüli személyek részvétele az intézmény adatkezelésében

Az Óvoda adatvédelmi tisztviselője

Az Óvoda adatvédelmi tisztviselője, olyan Székesfehérvári Megyei Jogú Város Önkormányzata Humán Szolgáltató Intézet által kötött szerződéssel megbízott vállalkozó, aki szakmai szempontból rátermett, az adatvédelmi jogot és gyakorlatot szakértői szinten ismeri, a feladatok ellátására alkalmas.

Nem lehet adatvédelmi tisztviselő, aki az Óvodánál az adatkezeléssel kapcsolatos érdemi döntések meghozatalára jogosult, illetve annak a Ptk. 8:1 (1) bekezdés szerinti hozzátartozója.

Az adatvédelmi tisztviselő nevét, elérhetőségét a Nemzeti Adatvédelmi és Információszabadság Hatóság (továbbiakban: NAIH) részére be kell jelenteni, az Óvoda hivatalos hirdetési felületén közzé kell tenni, kijelöléséről az intézmény dolgozóit írásban tájékoztatni szükséges.

Az Óvodaigazgató az adatvédelmi tisztviselő számára, biztosítja a feladatainak ellátásához szükséges jogosultságokat, továbbá a hozzáférést az elektronikus rendszerekhez és iratokhoz.

Az adatvédelmi tisztviselő közvetlenül a Humán Szolgáltató Intézetnek tartozik felelősséggel, feladatai során nem utasítható.

Az Óvoda adatvédelmi tisztviselője feladatköre keretében:

a) ellátja az Óvoda adatvédelmi tevékenységének irányítását, tájékoztat, szakmai tanácsot, iránymutatást ad;
b) közreműködik, illetve 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 óvodaigazgatónál, 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 óvodát az adatkezelésekre vonatkozó jogszabályok és szabályzatok érvényre juttatásában, ennek során figyelemmel kíséri az

adatvédelemmel összefüggő jogszabályváltozásokat és jelzi az óvodaigazgatónak a munkáltatói szabályzatok módosításának szükségességét;

f) közreműködik az óvodával jogviszonyban állók oktatásában és igény szerinti vizsgáztatásában;
g) egyedi ügyekben kidolgozott állásfoglalásával segíti az egységes gyakorlat kialakítását;
h) adatkezelési tevékenységét érintő ügyekben kialakítja az Óvoda álláspontját, 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 Óvoda adatkezelési tájékoztatóinak naprakészen tartásáról;
k) peres ügyekben az Óvoda adatvédelemmel kapcsolatos álláspontját egyezteti a peres képviseletet ellátó személlyel. Az adatvédelemmel kapcsolatos perekben szakértőként vehet részt;
l) az Óvodaigazgató részére igény esetén éves összefoglalóban értékeli annak adatvédelmi tevékenységét;
m) adatvédelmi szempontból véleményezi a személyes adatokat tartalmazó informatikai nyilvántartásokra, szoftverekre vonatkozó fejlesztési javaslatokat;
n) feladat- és hatáskörében – a célhoz kötöttség elvére figyelemmel – jogosult az óvodánál folytatott adatkezelésekbe betekinteni, az adatkezelőtől felvilágosítást kérni;
o) ellenőrzi a GDPR-nak, valamint az egyéb uniós és tagállami adatvédelmi rendelkezéseknek, jelen belső szabályzatnak való megfelelést, képzést, auditokat;
p) közreműködik a betekintési és hozzáférési jogosultságok felügyeletében;
q) szakmai tanácsot ad a hatásvizsgálatra vonatkozóan, nyomon követi a hatásvizsgálat elvégzését.
r) ellenőrzi az adatfeldolgozók adatfeldolgozói szerződésben vállalt kötelezettségeinek betartását, amennyiben szerződésbe ütköző gyakorlatot tapasztal, ezt jelzi az Óvodaigazgató részére, javaslatot tesz a szerződéses kapcsolat megszüntetésére.

Az Óvoda hatálya alá tartozó adatkezelés érintettje a személyes adatai kezeléséhez és jogai gyakorlásához kapcsolódó kérdésben közvetlenül fordulhat az adatvédelmi tisztviselő felé. A panaszt az adatvédelmi tisztviselő 15 napon belül köteles elbírálni, amennyiben valamennyi szükséges információ rendelkezésére áll.

Az érintett jogosult arra, hogy kérje az adatvédelmi tisztviselőtől, hogy személyét nem fedjék fel az Óvodaigazgató, vagy bármely más alkalmazott előtt. Az adatvédelmi tisztviselő ennek a kérésnek köteles eleget tenni. Az érintettet azonban köteles arról is tájékoztatni, hogy ennek hiányában az adott adatvédelmi probléma adott esetben nem orvosolható.

Az adatfeldolgozókra, közös adatkezelőkre, az intézménnyel szerződéses jogviszonyba kerülő önálló adatkezelőkkel kapcsolatos követelmények

Amennyiben az Óvoda közfeladatának ellátásához adatfeldolgozó igénybevétele szükséges, az adatfeldolgozó felelősségét a GDPR 28. cikke szerinti tartalommal írásban, önálló szerződésben vagy a szolgáltatási szerződés részeként rögzíteni kell.

Ezen kötelezettség alól az adatkezelő akkor mentesül, ha az adatfeldolgozó igénybevételének kereteit és garanciális feltételeit jogszabály határozza meg.

Közös adatkezelői jogviszony létesítésénél az írásbeli megállapodásnak az általános adatvédelmi rendelet 26. cikke szerinti tartalmi elemeit magában kell foglalnia.

Önálló adatkezelővel kötött szerződés esetén, mindenképpen szükséges kitérni a személyes adatok védelme és biztonsága érdekében alkalmazandó intézkedésekről.

A fenti szerződések megkötése előtt az adatvédelmi tisztviselő véleményét szükséges kikérni.

Az Óvodánál folytatott adatkezelések jogalapjára vonatkozó szabályok

Az Óvoda közfeladatot ellátó szerv, az adatkezelési tevékenységeit főszabályként a GDPR 6. cikk (1) bekezdés e) pontja szerint végzi. Ettől eltérő GDPR 6. cikkében foglalt jogalapot, az Óvoda akkor alkalmazhat, ha az adott adatkezelési tevékenység az intézmény közfeladatának ellátásához nem szükséges.

Az Óvoda adatkezelési tájékoztatóira vonatkozó előírások

Az Óvoda adatkezelési tájékoztatói adatkezelési célonként készülnek, annak érdekében, hogy az érintettek számára átlátható legyen.

A közalkalmazotti jogviszonyt létesítő személyek számára a belépéshez szükséges dokumentációval együtt, továbbá elektronikus úton kell megküldeni az őket érintő adatkezelési tájékoztatókat.

A személyesen megjelenő érintetteket, a rájuk vonatkozó adatkezelésekről az ügyintézés helyén papír alapon, illetve figyelemfelhívó jelzés útján kell tájékoztatni.

Az Óvoda az adatkezelési tájékoztatókat, amennyiben az a szülőket, egyéb külső partnereket is érinti, papír alapon a vezetői irodában, és az intézmény honlapján az „Adatkezelési tájékoztatók” cím alatt teszi közzé.

Az Óvoda adatkezelési tevékenységének nyilvántartása

Az Óvoda adatvédelmi tisztviselője elektronikusan végzi, az intézmény adatkezelési tevékenységének nyilvántartását.

A nyilvántartás a GDPR 30. cikk által meghatározott tartalommal kerül összeállításra. A nyilvántartásban szereplő adatkezelési tevékenységeknek összhangban kell lennie a kapcsolódó adatkezelési tájékoztatóban foglaltakkal.

Az adatvédelmi tisztviselő a nyilvántartást folyamatosan aktualizálja, frissíti, az intézmény tájékoztatása alapján.

Az adatbiztonságra vonatkozó követelmények

Az Óvoda az általa kezelt személyes adatok bizalmassága sértetlensége és rendelkezésre állása érdekében szervezési és technikai védelmi intézkedéseket alkalmaz. Ezek az intézkedések az érintettekre nézve megjelenő kockázatokkal arányosak, a technológiai fejlődés szempontjából naprakészek, zártak, teljes körűek.

Az óvoda a személyes adatok kezelésének helyszínéül szolgáló épület megfelelő fizikai, és tűzvédelméről gondoskodik. A személyes adatok kezelése zárható helyiségébe csak az arra jogosultak léphetnek be.

Az Óvoda azon alkalmazottai, akik személyes adat meghatározott csoportját nem kezelik (pl. alkalmazotti adatok, alkalmazottak pénzügyi adatai, ügyféladatok) azokhoz nem férhetnek hozzá, a személyes adatokat tartalmazó dokumentumokat zárható szekrényben kell őrizni. A monitorok rálátásvédelméről, az óvodaigazgatónak, az informatikai eszköz őrizetlenül hagyása esetén a kijelző zárolásáról és jelszavas védelméről az alkalmazottaknak gondoskodni kell.

Az Óvoda feladatellátásával összefüggő személyes adatot tartalmazó iratot, illetve adathordozót az Óvoda épületéből kivinni tilos, arra kizárólag az Óvodaigazgató előzetes írásbeli engedélyével kerülhet sor. Nem vonatkozik ez a kitétel arra az alkalmazottra, aki mindezt a munkaköri feladatának ellátásával összefüggésben teszi. A dolgozó ebben az esetben is köteles gondoskodnia megfelelő adatbiztonsági követelmények betartásáról.

Az Óvoda felhőszolgáltatás igénybevétele esetén olyan szolgáltatót választ, amelynek tárhelye az Európai Unió valamely országában található.

Az Óvoda alkalmazottai kötelesek az általuk használt laptopot jelszóvédelemmel ellátni, azt elzárva, vagy személyes őrizetben tartani.

Az Óvoda eszközein a felhasználónevek, jelszavak megjegyzése nem állítható be. Jelszó papír alapon nem tárolható.

Az Óvoda személyes adatot tartalmazó dokumentumot, személyesen zárt borítékban, vagy postai úton, amennyiben elengedhetetlenül szükséges, elektronikus úton jelszóval védve küldi az intézményen belülre és kívülre is.

Telefonon személyes adatot az Óvoda, a hívó fél minden kétséget kizáró azonosítása nélkül nem adhat ki.

A beépített és alapértelmezett adatvédelem elvének érvényesülése az óvodánál

A dolgozók mobiltelefonján alkalmazott mobileszköz- kezelési (MDM) megoldások

A csoportba feltöltött képfelvételek készítésére az óvodapedagógus a saját mobil eszközét használja, ezért az intézmény mobileszköz- kezelési (MDM) megoldásokat alkalmaz.

A dolgozók az eszközeiket jelszóvédelemmel látták el, továbbá vállalják, hogy gyermekekről készült képeket a zárt internetes csoportba történő feltöltéskor, de legkésőbb 5 munkanapon belül visszaállíthatatlanul törlik.

A dolgozók tudomásul bírnak arról, hogy a gyermekről csak a hozzájáruló nyilatkozatban megadott adatkezelési célokkal összefüggésben készíthetnek felvételt a gyermekről, amennyiben ahhoz a törvényes képviselő hozzájárult. Tudomásul bírnak arról, hogy a gyermekről, tilos olyan felvételt készíteni, amely sérti a gyermek emberi méltóságát.

A dolgozó telefonján egyéb gyermekkel összefüggő személyes adat kezelése tilos.

A dolgozó tudomásul bír arról, hogy a munkáltató az Mt. 11/A .§-a alapján a dolgozó telefonját jelenlétében ellenőrizheti. Az ellenőrzés kiterjed az adatkezelés jogalapjának, céljának ellenőrzésére, illetve, hogy az adattörlés megvalósult-e az előírt határidőben. Az ellenőrzés a szükségesség arányosság elvének figyelembevételével egy dolgozó által tett nyilatkozat formájában valósul meg, amelyben arról nyilatkozik, hogy a szabályzatban foglalt kötelezettségének eleget tesz.

Az Óvoda internetes zárt csoportjaira vonatkozó előírások

Az oldalon/ csoportban kizárólag olyan tartalmak oszthatók meg, amelyek nem sértik mások jogait, a közösségi oldal alapelveit, illetve az internet általános használatával összefüggő más szabályokat és feltételeket. Ezek közül is a legfontosabb: személyes adatok kezeléséhez megfelelő jogalap szükséges (általában az érintett hozzájárulása).

Tilos mást kellemetlen, kínos helyzetben bemutató fénykép önkényes posztolása, becsületsértő kommentelés, tiltott tartalmak megosztása, egyéb informatikai rendszert érintő visszaélés.

A különleges adatok megosztása a zárt csoportban szigorúan tilos. Ilyennek minősül például a gyermek betegsége, dolgozó betegsége (egészségügyi adata), az érintettek vallási hovatartozása, világnézeti meggyőződése, nemzetisége, faji, etnikai származása, politikai véleménye, genetikai és biometrikus adata, szexuális élete, illetve szexuális irányultsága.

A zárt csoportban közzétett fotók nyilvánosságra hozatala (pl. facebookon más csoportban, hírfolyamban való megosztás), amelyen **több gyermek** is szerepel, tilos.

A fentiek megvalósulása esetén a magánszemély adatkezelő is felelősségre vonható (NAIH eljárás, másik szülő által indítható személyiség jogi per), illetve a csoportból is kizárásra kerül.

Az adminisztrátor az adott oldalon zajló mindennemű adatkezelési tevékenységéért felelős. Módja van személyeket eltávolítani és kitiltani az oldalról/ csoportból, valamint a csoport nevében bejegyzést közzétevő személy kilétét megtekinteni.

A zárt csoport adminisztrátora óvodapedagógus lehet.

A zárt csoportban maximum gyermekeként két fő, a gyermek törvényes képviselői vehetnek részt, olyan profillal, amely alapján beazonosíthatóak az adminisztrátor számára. Ettől a szabálytól eltérni kizárólag előzetes írásbeli kérelem alapján lehet.

Az óvodában minden óvodai csoport külön virtuális közösséget hoz létre.

Az internetes zárt csoporthoz való csatlakozás önkéntes, a hozzájárulás megadása, azzal valósul meg, hogy arra jogosultként kéri a felvételét.

Az óvodában a gyermekekről készült fénykép/videofelvételek készítéséhez, illetve a virtuális csoportban való megosztásához a törvényes képviselők külön nyilatkozatban tett írásbeli hozzájárulása szükséges, amit az Óvoda a beiratkozáskor írásban, külön formanyomtatványon nyilatkoztatja a törvényes képviselőket.

Az óvodai jogviszony végén a szülők a csoportból kiléptetésre kerülnek, ezt követően az adminisztrátor is elhagyja a csoportot, így a csoport megszűnik. Amennyiben a csoportban lévő gyermekek törvényes képviselői a csoportot nem szeretnék megszüntetni, azt szülői közösségként működtetik tovább, amelyre vonatkozóan az Intézmény nem tartozik felelősséggel. Az óvoda alkalmazottja köteles kilépni a csoportból.

Az informatikai eszközök ellenőrzésével kapcsolatos adatkezelés

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

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

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

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

A jogviszony megszűnését megelőzően az alkalmazott gondoskodik arról, hogy az esetlegesen informatikai eszközön lévő, magáncélú adatait törölje. A jogviszony addig nem szüntethető meg, amíg az alkalmazott hozzáférését az intézmény által biztosított informatikai rendszerhez, vagy eszközhöz nem vonták vissza. A jogviszony megszűnését követő 30 nap elteltével az Óvoda az informatikai eszközön tárolt személyes adatokat megsemmisíti.

A munkáltató az informatikai eszközökön tárolt adatokat ellenőrizheti az Mt. 11/A .§-a alapján.

Az alkalmazott köteles haladéktalanul, de legkésőbb a tudomásszerzést követő 8 órán belül bejelenteni az óvodaigazgató részére, ha informatikai eszközét elvesztette és közölni, hogy az eszközön megközelítőleg hány, és milyen jellegű személyes adat volt.

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

Az Óvoda eszközein a felhasználónevek, jelszavak megjegyzése nem állítható be. Jelszó papír alapon nem tárolható.

A munkahelyi internethasználatra és elektronikus levelezésre vonatkozó adatkezelés

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

Az Óvoda informatikai eszközeire interneten elérhető szoftver csak óvodaigazgatói engedéllyel telepíthető, amit rendszergazda teljesít. A szoftver telepítését személyesen, vagy rendszergazdai felhasználónév és jelszó megadása alapján engedélyezett. A külső forrásból kapott vagy letöltött, nem engedélyezett programok használata tiltott!

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

A munkahelyi mobiltelefon használatával kapcsolatos adatkezelés

A munkahelyi mobiltelefon használata a dolgozók részre a szülőkkel való gyermeket érintő kapcsolattartás céljából megengedett.

Telefonon személyes adatot az Óvoda, a hívó fél minden kétséget kizáró azonosítása nélkül nem adhat ki.

Adatvédelmi incidensek kezelése, orvoslása

Az adatvédelmi incidensek megelőzése, kezelése, a vonatkozó jogi előírások betartása, ellenőrzése az óvodaigazgató feladata.

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

Amennyiben az Óvoda ellenőrzésre jogosult alkalmazottai adatvédelmi incidenst észlelnek, haladéktalanul személyesen, vagy telefonon és e-mail-ben értesíteniük kell az óvodaigazgatót, az óvodaigazgató helyettest és az adatvédelmi tisztviselőt.

Az Óvoda alkalmazottai kötelesek szóban és írásban is jelezni a vezetőnek, vagy a munkáltatói jogok gyakorlójának, ha adatvédelmi incidenst, vagy arra utaló eseményt észlelnek.

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

Adatvédelmi incidens bejelentése esetén az óvodaigazgató az adatvédelmi tisztviselő bevonásával – haladéktalanul megvizsgálja a bejelentést.

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

A kivizsgálás eredménye alapján hibák, hiányosságok orvoslására haladéktalanul intézkedni kell.

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.

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

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.

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

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

Adatvédelmi incidensek nyilvántartása

Az adatvédelmi incidensekről 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.

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

Adatvédelmi incidens bejelentése a NAIH részére, illetve az érintettek tájékoztatása

Az adatvédelmi incidenseket nyilván kell tartani és amennyiben kockázatot jelentenek az érintettekre vonatkozóan, úgy a NAIH részére is be kell jelenteni.

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.

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

Nem kell azonban az érintetteket tájékoztatni, ha

a) az óvoda megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták;
b) az óvoda 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)

Nem belső adatvédelmi incidens

Amennyiben az Óvoda 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
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.

Az adatvédelmi incidensek eljárásrendje

Az adatvédelmi incidensek hatékony kezelése érdekében az Óvoda külön eljárásrendet dolgozott ki, amely részletesen szabályozza, az adatvédelmi incidens esetében megtenni szükséges lépéseket, az eljárásrend mellékletét képezi, az adatvédelmi incidens nyilvántartás is.

Az adatvédelmi incidens nyilvántartást az adatvédelmi tisztviselő vezeti, incidens esetén a NAIH részére megküldi.

Az érintetti joggyakorlásra vonatkozó szabályok

Az óvoda az érintettek joggyakorlásával kapcsolatosan külön eljárásrendet alakított ki. Érintetti joggyakorlással kapcsolatos kérelmek mind elektronikus úton az Óvoda központi e-mail címén, mind papír alapon – személyesen, vagy postai úton az intézmény székhelyére címezve – előterjeszthetők, amelyre az adatkezelési tájékoztatókban utalni szükséges.

Az adatkezeléshez kapcsolódó igényeket az óvodaigazgató részére be kell mutatni, aki gondoskodik annak határidőn belüli megválaszolásáról.

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.

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

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

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

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 helyesbítéshez, 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;

Az óvoda az érintetti joggyakorlás elősegítéséhez formanyomtatványokat készített, ezeket, az érintetti joggyakorlást elősegítő eljárásrend tartalmazza.

Adatvédelmi hatásvizsgálat és előzetes konzultáció

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.

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

Az adatvédelmi hatásvizsgálat szükségességének megállapításához az 1. függelékben foglalt kérdéseket szükséges megválaszolni.

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 Óvodaigazgató írásban rögzíti.

Amennyiben az óvodaigazgató 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.

Az adatvédelmi hatásvizsgálat lefolytatásáig vagy az annak elmaradásával kapcsolatos okok írásban történő rögzítéséig az adatkezelésről szóló döntés nem hozható meg.

Az adatvédelmi hatásvizsgálat lefolytatásában az óvodaigazgató és szükség esetén az általa kijelölt személy vesz részt. Az adatvédelmi hatásvizsgálatot az adatvédelmi tisztviselő segíti. Az adatvédelmi hatásvizsgálat iratai nem nyilvánosak.

Az adatkezelési hatásvizsgálatot végző az adatvédelmi hatásvizsgálatról összefoglaló értékelést készít a 2. függelékben foglaltak figyelembevételével. Az összefoglaló értékelést, amennyiben nem az Óvodaigazgató készítette, az óvodaigazgató hagyja jóvá, melyet követően az adatkezelést el lehet kezdeni.

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

Ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az Óvoda által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az adatkezelő konzultál a NAIH-al.

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

Hatósági megkeresések

Személyes adatot érintő adatszolgáltatást kizárólag az Óvodaigazgató beleegyezésével lehet teljesíteni. Személyes adatot hatósági, bírósági **megkeresés alapján** az Óvodaigazgató, míg a NAIH megkeresése alapján az Óvodaigazgató, vagy felkérése esetén az adatvédelmi tisztviselő jogosult kizárólag írásban és csak akkor **kiadni**, ha

a) a megkeresés papír alapon kiadmányozott, hivatalos postai küldeményként feladott, vagy elektronikusan kiadmányozott hivatali kapura érkezett, és

b) a megkereső szerv a megkeresésben megjelölte azt a személyt, akiről a fentiekben meghatározott szerv, vagy hatóság a személyes adat kiadását kéri, valamint a kért adatok fajtáját, az adatkérés célját és a teljesítés határidejét.

Amennyiben a megkeresés az előző pontban írtaknak nem felel meg (pl. telefonon, e-mailben érkezik) fel kell hívni a megkeresés szabályszerű előterjesztésére. Amennyiben a megkereső kiléte kétséges, a megkeresés jogszerűségéről szükséges meggyőződni (pl. a megkereső szerv ügyintézőjének telefonos megkeresése útján).

Az adatot ki kell adni, amennyiben a feladatkörében eljáró hatóság szabályszerű helyszíni ellenőrzést folytat és a dokumentum az ellenőrzés lefolytatásához szükséges. Szabályszerű a **helyszíni ellenőrzés**, ha

a) az ellenőrök az ellenőrzést megelőzően átadják megbízólevelüket, amely tartalmazza a megbízó nevét, az ellenőrzés tárgyát, időszakát, és a megbízott ellenőr azonosító adatait, és
b) az ellenőrök igazolják a megbízó levél alapján személyazonosságukat.

Kivételesen (különösen indokolt esetben) akkor is teljesíthető a hatósági, bírósági megkeresés, ha papír alapon nem áll rendelkezésre a megkeresés eredeti példánya (például mert a megkeresés a nyomozati cselekmények sürgőssége miatt telefaxon érkezett).

A megkeresés akkor teljesíthető, ha

a) a kért adatokat az Óvoda jogszerűen kezeli,
b) a kért adatok kezelésére a megkereső fél is jogosult
c) az adatok rendelkezésre állnak (amennyiben nem közhiteles nyilvántartásból történik az adatszolgáltatás, ennek tényére a válaszban szükséges utalni)
d) a megkeresés biztonságosan teljesíthető (pl. titkosított e-mail keresztül.

ZÁRÓ RENDELKEZÉSEK

A Szabályzat megállapítása, módosítása és beépítése

A Szabályzat megállapítására és módosítására az óvodaigazgató jogosult.

Jelen szabályzatot az óvodában helyben szokásos helyen és módon ismertetni kell az alkalmazottakkal, illetve az Info.tv. előírásainak megfelelően a közadatárban is közzé kell tenni.

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

A szabályzatot a jogszabályi környezet, a NAIH joggyakorlatának jelentős változása, az óvoda tevékenységében, adatkezeléseiben bekövetkező jelentős változás esetén soron kívül, egyéb esetben 3 évente felül kell vizsgálni. A következő felülvizsgálat ideje:2025.

Az Óvodaigazgató gondoskodik arról, hogy az adatvédelmi szabályzatban meghatározott előírások az Óvoda folyamataiban és mindennapjaiban érvényre jussanak.

Jelen szabályzatban foglaltak betartása és érvényesítése az Óvoda valamennyi alkalmazottjának kötelessége.

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

A Szabályzat rendelkezéseit meg kell ismertetni az Óvoda valamennyi alkalmazottjával, amelynek érvényesítése minden alkalmazott lényeges munkaköri kötelezettsége.

Az óvoda jelen szabályzat alapján a munkavégzéssel együtt nem járó személyes adatok átadása esetére titoktartási kötelezettséget ír elő.

Az óvoda az adatvédelmi szabályok megszegése esetén az azt okozó személlyel szemben fegyelmi eljárást kezdeményez, indokolt esetben büntető feljelentést tesz.

Az óvoda állományába újonnan került olyan személyeket, akik munkakörüknél fogva személyes adatokat kezelnek, az adatvédelmi tisztviselő, vagy más erre megbízott személy köteles az állományba a felvételt követő hónapban adatvédelmi oktatásban részesíteni és részére a szükséges jogszabályokat, belső normákat és egyéb segédanyagokat rendelkezésre bocsátani.

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

Az adatkezelő szerv adatvédelmi tevékenységének célellenőrzését az óvodaigazgató rendelheti el. Az informatikai biztonsági feltételek teljesülését félévente ellenőrizni kell, eredményéről tájékoztatni kell az Óvodaigazgatót.

A szerzői jogról szóló 1999. évi LXXVI. törvény (továbbiakban: Szjt.) 1. § (1) bekezdése értelmében jelen szabályzat szerzői műnek minősül, így annak minden része szerzői jogi védelem alatt áll.

Székesfehérvár, 2023.09.01.

…….

Mályi Lilla óvodaigazgató

*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 meglévőszemélyes 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 munkavállalókra 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 érintőmagatartás?

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.

Szervezeteket 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 hatásköréhez 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), a munkavállalók, 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.