Adatvédelmi és Adatbiztonsági Szabályzat

2026.

Tartalom

Bevezetés

A Kozármislenyi Közös Önkormányzati Hivatal jegyzője, továbbá a szabályzat hatálya alá tartozó önkormányzatok polgármesterei és elnökei a vonatkozó Európai Uniós (így különösen a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló 2016/679. számú Európai Parlament és Tanács rendelete [továbbiakban: GDPR]), valamint hazai (így különösen az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [továbbiakban: Infotv.], kiemelten annak 25/A.§ (3) bekezdése alapján) jogszabályoknak való megfelelés érdekében a jelen szabályzat hatálya alá tartozó szervezetek adatkezeléseire vonatkozó szabályokat az alábbiak szerint állapítják meg.
Jelen Szabályzatban, egységes szerkezetbe foglalva az adatbiztonságra vonatkozó előírások is megtalálhatók.

I. Általános rendelkezések

A szabályzat hatálya

1.1. A szabályzat szervezeti hatálya kiterjed:

- Kozármislenyi Közös Önkormányzati Hivatalra,
- Kozármisleny Város Önkormányzatára,
- Egerág Község Önkormányzatára,
- Kisherend Község Önkormányzatára,
- Kozármislenyi Horvát Nemzetiségi Önkormányzatra,
- Kozármislenyi Német Nemzetiségi Önkormányzatra,
- Kozármislenyi Roma Nemzetiségi Önkormányzatra (továbbiakban együtt: adatkezelő szerv).

1.2. Jelen szabályzat személyi hatálya kiterjed az adatkezelő szervvel munka-, vagy egyéb foglalkoztatásra irányuló jogviszonyban álló személyekre (továbbiakban: foglalkoztatottak), valamint az adatkezelő szervvel egyéb szerződéses jogviszonyban álló személyekre, különösen azokra, akik a feladataik ellátása során személyes adatokkal dolgoznak.

1.3. A szabályzat tárgyi hatálya kiterjed az adatkezelő szerv kezelésében lévő minden olyan adatra, amely a GDPR és az Infotv. rendelkezései alapján a személyes adat kategóriájába esik, továbbá az adatkezelő szerv teljes feladatellátására és minden adatkezelési folyamatára.

A szabályzat célja

2.1. Figyelembe véve, hogy az adatkezelő szervnek a szokásos ügymenetében elengedhetetlenül szükséges személyes adatokat gyűjtenie és kezelnie, a adatkezelő szerv

számára a legfontosabb célkitűzések között szerepel az általa végzett adatkezelési, adatfeldolgozási folyamatok jogszerűségének, átláthatóságának, hitelességének, pontosságának és bizalmi jellegének erősítése, az adatok integritásának megőrzése, illetve az érintettek joggyakorlásának elősegítése tisztességes eljárási keretek kialakításával és fenntartásával.

2.2. Az adatkezelő szerv elkötelezte magát amellett, hogy szabályozási, szervezetalakítási és dokumentálási eszközei révén megteremti a zárt, teljes körű, folyamatos és a kockázatokkal arányos adatvédelem jogszerű mechanizmusait, melyek különösen a következők:
a) az adatkezelő szerven belüli biztonságtudatos viselkedés előmozdítása;
b) a jogszabályoknak megfelelő eljárásrendek létrehozása, továbbá az eljárásrendeknek megfelelő adatvédelmi gyakorlatok és operatív tevékenységek kialakítása;
c) az átláthatóságot és elszámoltathatóságot biztosító dokumentáció elkészítése;
d) az adatkezelő szervvel kapcsolatba kerülő személyek (így különösen az adatkezelő szervvel bármely jogviszonyban álló természetes személyek, ügyfelek) jogait és jogos érdekeit figyelembe vevő ügymenetek kialakítása;
e) a kezelt személyes adatok jogosulatlan felhasználásának megakadályozása;
f) az érintetti jogok biztosítása;
g) az adatvédelmi incidensek megelőzésére vonatkozó intézkedések meghozatala.

Értelmező rendelkezések

3. Jelen szabályzat alkalmazásában:
a) adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel;
b) 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;
c) adatkezelés korlátozása: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;
d) 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;
e) adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;
f) adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;
g) 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;
h) 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;
i) 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.);
j) 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;
k) 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;
l) nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;
m) nyilvántartási rendszer: a személyes adatok bármely módon – centralizált, decentralizált, funkcionális vagy földrajzi szempontok szerint – tagolt állománya, amely meghatározott ismérvek alapján hozzáférhető;
n) profilalkotás: személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használnak;
o) személyes adat: azonosított vagy azonosítható természetes személyre (a jelen Szabályzatban: „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;
p) személyes adatok különleges kategóriái: a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok.

Az érintettség vizsgálata

4.1. Az adatkezelő szerv belső vizsgálata során megállapította, hogy a GDPR hatálya alá tartozik, mivel személyes adatokat részben automatizált módon, illetve nem automatizált módon egy nyilvántartási rendszer részeként kezel, továbbá mint adatkezelő az Unión belül tevékenységi hellyel rendelkezik. Megállapításra került az is, hogy az adatkezelő szerv az Infotv. hatálya alatt áll, tekintve, hogy Magyarország területén automatizált eszközökkel és manuális módon folytat adatkezelést természetes személyek adataival kapcsolatban. Erre tekintettel a GDPR és az Infotv. előírásai a adatkezelő szerv valamennyi adatkezelési műveletére alkalmazandók, függetlenül azok formájától.

4.2. Az adatkezelő szerv kötelezettséget vállal arra, hogy minden egyéb magyarországi kötelező aktussal és jogszabállyal összhangban, azoknak megfelelve, az ágazati különös előírásokat is betartva folytatja az adatkezelési tevékenységét.

A szabályzat elsőbbsége

5. Az adatkezelő szerv minden belső szabályozó eszköz megalkotásakor figyelemmel van a jelen szabályzat rendelkezéseire. Az adatkezelő szerv egyéb belső szabályzóinak és jelen szabályzatnak az összeütközése esetén, azt a jelen szabályzat elsőbbségének kimondásával szükséges feloldani.

Az általános felülvizsgálat rendje

6.1. A Szabályzat általános felülvizsgálatára évente egy alkalommal kerül sor, továbbá minden olyan esetben, amikor a szabályozás időpontjában irányadó körülményekben jelentős változás történik. Jelentős változás különösen, ha a jogszabályi háttér, valamint az adatkezelési folyamatok vagy a kezelt adatok köre lényeges mértékben eltér a szabályozáskori állapotától. Szintén jelentős változásként értékelendő, ha az adatkezelési folyamat nem, de az alkalmazott informatikai rendszer vagy a tevékenységi hely fizikai környezete változik meg.

6.2. A fentiektől eltérő feltételek és határidők kerülhetnek megállapításra az egyes eljárásrendekkel és vizsgálatokkal kapcsolatban (különös felülvizsgálatok).

II. A szervezetrendszer

7.1. Az adatkezelő szerv a felelősségi körök egyértelmű kijelölésével és azok betartásával törekszik előmozdítani az adatvédelmi és adatbiztonsági szabályok betartását a szervezeten belül.

Az adatkezelő szerv vezetője

7.2. Az adatkezelő szerv vezetője felel az adatkezelő szerv vonatkozásában:
a) az adatkezelő szerv adatvédelmi és adatbiztonsági rendszerének kialakításáért és fenntartásáért;

b) a személyes adatok védelmére vonatkozó követelmények teljesüléséhez szükséges személyi, tárgyi és technikai feltételek megteremtéséért, amennyiben azok biztosítása az ő hatáskörébe tartozik;
c) az adattörlésre előírt határidők betartatásáért, valamint a határidők lejártát követően az adatok jogszerű törléséért;
d) az adatvédelmi tudatosságnövelés megszervezéséért;
e) azért, hogy az érintettek joggyakorlását és tájékoztatását biztosító körülmények megfelelő módon rendelkezésre álljanak;
f) az adatvédelmi hatásvizsgálatok lefolytatásáért, ezek rendszeres felülvizsgálatáért, valamint a szükséges feltételek és erőforrások biztosításáért;
g) az adatvédelmi incidensek nyilvántartásának vezetéséért, az előírt bejelentési kötelezettségek határidőben történő teljesítéséért a Nemzeti Adatvédelmi és Információszabadság Hatóság felé, valamint az incidenssel érintett személyek megfelelő tájékoztatásáért;
h) olyan adatvédelmi tisztviselő kijelöléséért, megbízásáért, aki a feladatai ellátására alkalmas, továbbá a neve és elérhetősége bejelentéséért a Nemzeti Adatvédelmi és Információszabadság Hatóságnak, valamint a tisztviselő megfelelő tájékoztatásáért;
i) annak biztosításáért, hogy az adatvédelmi tisztviselő hozzáférjen a személyes adatokhoz, az adatkezelési műveletekhez, valamint rendelkezésére álljanak a feladatainak ellátásához szükséges szakmai és tárgyi feltételek;
j) az adatvédelmi tevékenységgel összefüggő, jogszabályban előírt közzétételi kötelezettségek teljesítéséért;
k) annak garantálásáért, hogy az adatvédelmi tisztviselő összeférhetetlensége ne álljon fenn, illetve az esetlegesen felmerülő összeférhetetlenséget megfelelően kezeljék.

Az adatvédelmi tisztviselő

8.1. Az adatkezelő szerv jogszabályi kötelezettségeinek eleget téve vizsgálatot folytatott le annak érdekében, hogy megbizonyosodjon róla szükséges-e adatvédelmi tisztviselőt kijelölnie. Ennek alapján megállapítást nyert, hogy az adatkezelő szerv vonatkozásában a GDPR szabályainak megfelelően kötelező az adatvédelmi tisztviselő kijelölése. Az erről készült indokolás az 1. számú mellékletben olvasható.

8.2. Az adatvédelmi tisztviselőnek kizárólag olyan személy jelölhető ki, aki:
a) megfelelő szakmai rátermettséggel rendelkezik,
b) az adatvédelmi jog és gyakorlat területén szakértői ismeretekkel bír,
c) képes a GDPR 39. cikkében meghatározott feladatok ellátására.

8.3. Az adatkezelő szerv az adatvédelmi tisztviselő megbízását követően az adatvédelmi tisztviselő nevét és elérhetőségeit a Nemzeti Adatvédelmi és Információszabadság Hatóság felé haladéktalanul bejelenti, valamint saját honlapján közzéteszi.

8.4. Az adatvédelmi tisztviselő következő feladatokat látja el:
a) tájékoztat és szakmai tanácsot ad a GDPR, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban;

b) ellenőrzi a GDPR-nak, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezéseknek, továbbá az adatkezelő szerv, vagy az adatfeldolgozói személyes adatok védelmével kapcsolatos belső szabályainak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben részt vevő személyzet tudatosság-növelését;
c) kérelemre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat elvégzését;
d) együttműködik a Nemzeti Adatvédelmi és Információszabadság Hatósággal;
e) az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a Nemzeti Adatvédelmi és Információszabadság Hatóság felé.

8.5. Az adatvédelmi tisztviselő feladatait az adatkezelési műveletekhez fűződő kockázat megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményére és céljára is tekintettel végzi.

8.6. Az adatkezelő szerv az adatvédelmi tisztviselőt feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja. Az adatvédelmi tisztviselő közvetlenül a adatkezelő szerv vezetőjének tartozik felelősséggel.

A foglalkoztatottak

A szabályzat megismerése

9. A adatkezelő szerv vezetője kötelezettséget vállal arra, hogy minden tőle elvárható intézkedést megtesz annak érdekében, hogy a jelen szabályzatot, illetve annak tartalmát a foglalkoztatottak megismerjék és megértsék az abban foglalt kötelezettségeiket.

Általános felelősségi szabályok

10.1. Valamennyi foglalkoztatott, aki a feladata ellátása során a személyes adatokon műveleteket végez, vagy az adatkezelő szerv birtokában lévő személyes adatokhoz hozzáféréssel rendelkezik, köteles azokat kizárólag a feladatellátása/munkavégzése körében és céljából kezelni, illetve feldolgozni, mely kötelezettség keretében:
a) a feladatellátás/munkavégzés során megszerzett személyes adatok vezetői írásos engedély nélkül nem oszthatók meg harmadik személyekkel, illetve nem hozhatók nyilvánosságra;
b) mások személyes adatai nem kezelhetőek önkényesen;
c) az adatok kezelésekor az adatbiztonsági elvárásoknak megfelelő körültekintéssel és elővigyázatossággal kell eljárni. Személyes adatokon csak a vezetői utasításnak megfelelő adatkezelési tevékenységek végezhetők.

10.2. A személyes adatok megosztására az adatkezelő szerven belüli jogosultsággal nem rendelkező személyekkel sincs lehetőség.

10.3. Minden foglalkoztatottnak kötelessége rendszeresen felülvizsgálni az általa kezelt adatokat, a szükségtelen és jogellenes adatkezelési műveletek megakadályozása érdekében, így különösen

a) a feladatkörükbe tartozó személyes adatok közül a jogalap, illetve cél nélkül kezelt adatokat törölni kötelesek. Ha az adatok törölhetőségével kapcsolatban kétség merül fel, feltétlenül az adatkezelő szerv vezetőjéhez kell fordulni;
b) amennyiben felmerül egy adattal kapcsolatban a pontosítás szükségessége – mert az hibás, hiányos vagy aktualitását vesztette – akkor azt haladéktalanul helyesbíteni, vagy ha ez nem lehetséges törölni kell.

10.4. A személyes adatokat a lehető legkevesebb adattároló helyen szükséges tárolni.

10.5. A foglalkoztatottak vezetői engedély nélkül nem készíthetnek személyes adatokat tartalmazó nyilvántartást vagy egyéb forrást.

10.6. Abban az esetben, ha az adatkezelő szerv valamely foglalkoztatottja adatvédelmi incidens bekövetkezésének lehetőségét észleli, vagy az adatfeldolgozótól adatvédelmi incidensre vonatkozó értesítést kap késedelem nélkül, de legkésőbb a tudomásszerzést követő 12 órán belül köteles azt jelezni az adatkezelő szerv vezetője felé.

10.7. Az adatkezelő szerv minden foglalkoztatottja fegyelmi, kártérítési, szabálysértési és büntetőjogi felelősséggel tartozik a munkavégzése során tudomására jutott személyes adatok jogszerű kezeléséért.

III. Érintetti jogok

Előzetes tájékoztatás

11. Az adatkezelő szerv kötelezettséget vállal az érintetti jogok tiszteletben tartására és a gyakorlásuk elősegítésére, így az adatkezelő szerv tájékoztatja az érintettet a jelen szabályzat 21.2. pontjában rögzített információkról.

A hozzáféréshez való jog

12.1. Az adatkezelő szerv az érintett számára visszajelzést biztosít arra vonatkozóan, hogy az érintett személyes adatainak kezelése folyamatban van-e. Amennyiben folyamatban van a személyes adatok kezelése, akkor személyes adataihoz, valamint a következő információkhoz férhet hozzá:
a) adatkezelés céljai,
b) személyes adatok kategóriái,
c) címzettek, címzettek kategóriái,
d) adattárolás tervezett időtartama vagy annak meghatározásának szempontjai;
e) érintett jogai,
f) automatizált döntéshozatal, illetve profilalkotás ténye, módszere és következményei.

12.2. Az adatkezelő szerv az adatkezeléssel érintett személyes adatok másolatát ingyenesen az érintett rendelkezésére bocsátja, feltéve, hogy az nem érinti hátrányosan mások jogait és szabadságait.

12.3. Az érintett által ismételten benyújtott, továbbá a nyilvánvalóan megalapozatlan vagy túlzó kérelmekért adminisztratív költségeken alapuló, ésszerű mértékű díj számítható fel.

A helyesbítéshez való jog

13.1. Kérésre az adatkezelő szerv indokolatlan késedelem nélkül helyesbíti az érintettre vonatkozó pontatlan személyes adatokat.

13.2. Figyelembe véve az adatkezelés célját, az érintett jogosult arra, hogy kérje a hiányos személyes adatok kiegészítését.

A törléshez való jog

14.1. Az érintett jogosult arra, hogy kérésére az adatkezelő szerv által kezelt személyes adatait töröljék.

14.2. A törlést a következő körülmények fennállása esetén kötelező végrehajtani:
a) nincs szükség a cél eléréséhez a személyes adatok kezelésére vagy a cél megvalósult;
b) az érintett visszavonja a hozzájárulását az adatkezeléshez és nincs más jogalap;
c) az érintett tiltakozik az adatkezelés ellen és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;
d) az adatok kezelése jogellenesen történik.

Az elfeledtetéshez való jog

15. Az elfeledtetéshez való jog értelmében, ha az adatkezelő szerv nyilvánosságra hozta az adatot, és azt törölni köteles, akkor ésszerűen elvárható lépéseket tesz annak érdekében, hogy tájékoztasson más adatkezelőket a szóban forgó adatok törléséről.

Az adatkezelés korlátozásához való jog

16. Az adatkezelő szerv az érintett kérésére korlátozza az adatkezelést, ha az alábbiak valamelyike teljesül:
a) ha az érintett vitatja a kezelt személyes adatok pontosságát, az adatkezelés korlátozható arra az időtartamra, amíg az adatok pontosságának ellenőrzése be nem fejeződik;
b) ha az adatkezelés jogellenesnek bizonyul, de az érintett ellenzi a kezelt személyes adatainak törlését;
c) ha az adatkezelés eredeti céljának eléréséhez már nincs szükség az adatokra, de az érintett igényli azokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez;
d) ha az érintett tiltakozott az adatkezelés ellen és ennek kivizsgálása még folyamatban van a folyamat időtartamára korlátozható az adatkezelés.

Adathordozhatósághoz való jog

17. Amennyiben az adatkezelés jogalapja a GDPR 6. cikk a) vagy b) pontján (hozzájáruláson vagy szerződés teljesítésén) alapul és automatizált módon történik, az érintett jogosult arra, hogy az adatkezelő szerv által gyűjtött adatait tagolt, széles körben használt formátumban megkapja. A kapott adatokat az érintett jogosult más adatkezelőhöz továbbítani vagy az adatkezelő szerv által továbbíttatni.

Tiltakozáshoz való jog

18.1. Az érintett jogosult arra, hogy saját helyzetével kapcsolatos okokból bármikor tiltakozzon az olyan adatkezeléssel szemben, amely a GDPR 6. cikk (1) bekezdés e) pontján alapul, azaz a közérdekű feladat ellátásához szükséges. A megalapozott és megfelelő tiltakozás esetén az adatkezelő szerv megszünteti az adatkezelést, kivéve, ha arra olyan kényszerítő erejű jogos indokok vagy jogi igények érvényesítése, védelme miatt továbbra is szükség van, amelyek az érintett jogaival szemben elsőbbséget élveznek.

18.2. A tiltakozáshoz való jogról a fenti esetekben külön tájékoztatni kell az érintettet a kapcsolatfelvételkor.

Az adatkezelő szerv értesítési kötelezettsége

19. A adatkezelő szerv minden címzettet tájékoztat valamennyi helyesbítésről, törlésről vagy korlátozásról, amellyel az érintett személyes adatait közölték, kivéve, ha az lehetetlennek bizonyul vagy aránytalan nehézséggel jár.

IV. Tájékoztatási eljárásrend

Előzetes tájékoztatás

20.1. Alapvető elvárás az adatkezelő szerv összes adatkezelésével kapcsolatban, hogy az érintettek felé kommunikált tájékoztatásnak tömörnek, átláthatónak és érthetőnek kell lennie, mindezt könnyen hozzáférhető, világos és közérthető formában kell megtenni. Különös figyelmet kell fordítani a szabályzat betartására kiskorúaknak címzett bármely információ esetén.

20.2. A tájékoztatás történhet írásban – ideértve az elektronikus utat is – és szóban is, feltéve, hogy az érintett személyazonossága megfelelő módon igazolásra került.

21.1. Amennyiben a személyes adatok közvetlenül az érintettől származnak, a megszerzés időpontjában kell a tájékoztatási kötelezettség teljesítéséhez szükséges információkat az érintett rendelkezésére bocsátani.

21.2. Az érintettől gyűjtött személyes adatokra vonatkozó tájékoztatásnak tartalmaznia kell a következő információkat:
a) az adatkezelő megnevezése és elérhetősége;
b) az adatkezelés célja és jogalapja;
c) a személyes adatok címzettje, illetve címzettek kategóriái, ha van ilyen;
d) adattovábbítás ténye, feltételei és részletei;
e) a személyes adatok tárolásának időtartama vagy annak meghatározásának szempontja;
f) az érintetti jogok felsorolása és magyarázata;
g) a hatósághoz fordulás jogának kiemelése;
h) a személyes adat átadás elmaradásának következményei;
i) az adatkezelési tevékenység során esetlegesen alkalmazott automatizált döntéshozatal, illetve profilalkotás ténye, továbbá az alkalmazott módszer és az érintettre vonatkoztatva, a módszerből adódó következmények leírása;
j) ha az eredeti céltól eltérő célú további adatkezelés van kilátásban,
k) adatvédelmi tisztviselő elérhetősége.

21.3. Abban az esetben, ha a személyes adatok nem az érintettől származnak:
a) a megszerzéstől számított ésszerű határidőben, de legkésőbb egy hónapon belül;
b) ha a személyes adatok az érintettel való kapcsolattartás céljából kerülnek felhasználásra, legalább a kapcsolatfelvételkor;
c) ha várhatóan más címzettel is közlik az adatokat, legkésőbb a személyes adatok első alkalommal való közlésekor az érintettet tájékoztatni kell.

21.4. Az érintettől különböző személytől gyűjtött személyes adatokra vonatkozó tájékoztatás többletkövetelményei:
a) a kezelt személyes adatok körének meghatározása;
b) a személyes adatok forrásának meghatározása, és adott esetben arra vonatkozó információ, hogy nyilvánosan hozzáférhető forrásból származnak-e.

V. Adatkezelési kérés- és panaszkezelési eljárásrend

22.1. Az előzetes tájékoztatást követően gondoskodni kell arról, hogy az érintett adatalanyok az elvárt hatékonysággal kapjanak információt és segítséget.

22.2. Az adatkezelő szerv tudatosságnöveléssel és a munkaköri leírások megfelelő meghatározásával kiemelt figyelmet fordít arra, hogy az érintettek az előzetes tájékoztatás eljárásánál ismertetett módon és formában, az ott felsorolt információkat a kérelmeiknek megfelelően megkapják.

22.3. Az adatkezelő szerv az érintettek esetleges panaszait a tájékoztatási eljárásrendnek megfelelően kezeli, illetve szükség szerint meghozza és végrehajtja az érintetti panasznak megfelelő intézkedéseket. Abban az esetben, ha nem kerül sor intézkedések megtételére, az adatkezelő szerv késedelem nélkül, de legkésőbb 25 napon belül tájékoztatja erről az érintettet, az elmaradás okainak és a jogorvoslati lehetőségek megjelölésével együtt.

22.4. Az érintetti kérelmekre irányadó válaszadási határidőt, a jogszabályi elvárásoknak megfelelően, az adatkezelő szerv 25 napban maximálja. Szükség esetén, ha a kérelmek száma és összetettsége azt indokolja, az említett határidő két hónappal meghosszabbítható.

22.5. Az adatkezelő szerv az érintettek kéréseit a formájuktól és a választott kommunikációs csatornától függetlenül befogadja. Így azok érkezhetnek telefonon, elektronikus vagy hagyományos levélben, illetve akár személyesen szóban is. Ha elektronikus úton történt a kérelem benyújtása, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri.

22.6. Az adatkezelő szerv az érintetti kérésekről és panaszokról naprakész nyilvántartást vezet.

VI. Az adatkezelési és adatfeldolgozási eljárásrend

Az adatkezelő szerv által kezelt adatok

23.1. Az adatkezelő szerv által feladatellátása során kezelt, illetve feldolgozott adatok vonatkozhatnak a foglalkoztatottjaira, az ügyfeleire, a velük jogviszonyban álló egyéb személyekre, azok törvényes képviselőire, meghatalmazottjaira, továbbá bármely olyan személyre, akivel az adatkezelő szerv feladatellátása során vagy azzal összefüggésben kapcsolatba kerül.

23.2. Az adatkezelő szerv adatkezelései ügyviteli, nyilvántartási, ellenőrzési, valamint egyéb céllal történnek,
a) az ügyviteli típusú adatkezelés egy jogviszony (szerződés, megállapodás, jogszabályi kötelezettség) létrejöttéhez, feldolgozásához és lezárásához kapcsolódik, így a meghatározott feladatok ellátásához, a résztvevők azonosításához és az elszámoláshoz szükséges adatokra kell, hogy korlátozódjon. Ennek megfelelően az ilyen adatkezelések esetén személyes adatok, csak a jogviszonyhoz kapcsolódó iratokban, kommunikációban, illetve segédletekben szerepelhetnek,
b) nyilvántartási célú adatkezelés során az egyes adatfajtákból létrejövő adatállományok teszik lehetővé az adatok visszakereshetőségét és azonosíthatóságát. Az ilyen jellegű nyilvántartásoknak mindig az ügyviteli típusú adatkezelésekhez kell igazodniuk,
c) az ellenőrzések lebonyolításához szükséges egy védendő és jogszerű érdek fennállása. Ellenőrzések irányulhatnak közvetlenül az adatalany tevékenységére, de elképzelhető, hogy az ellenőrzés tárgya eltérő, az adatalany annak csak véletlen/járulékos résztvevője,
d) az adatkezelő szerv egyéb adatkezelési célokkal is végezhet adatkezelési tevékenységet, ha annak jogszabályi feltételei egyébként fennállnak.

Az adatkezelés alapelvei

Jogszerűség, tisztességes eljárás és átláthatóság elve

24.1. A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni. Ezen alapelv szerint az adatkezelés csak abban az esetben tekinthető jogszerűnek, ha az nemcsak az adatvédelmi tárgyú jogszabályoknak, hanem bármely egyéb személyes adatokat érintő normának is megfelel.

24.2. A jogszerű adatkezelés eléréséhez a következőkre kell különösen tekintettel lenni:
a) a személyes adatok védelméhez való jog a természetes személyek alapvető joga, amely biztosítja az érintettek információs önrendelkezési jogát;
b) az információs önrendelkezési jog tiszteletben tartása érdekében az adatkezelő szerv személyes adatot csak az alábbi jogalapok megléte esetén kezel:
ba) az érintett előzetes, önkéntes és kifejezett hozzájárulása;
bb) a szerződés teljesítése, a teljesítéshez szükséges mértékben;
bc) amennyiben az adatkezelés az adatkezelő szerv által ellátott közfeladat ellátásához szükséges;
bd) az adatkezelő szerv vagy harmadik fél jogi kötelezettségének teljesítése;
be) az érintett vagy más természetes személy létfontosságú érdeke.

24.3. Tisztességes az eljárás, ha az az érintetti jogok érvényesülését és az érintettek jogérvényesítését aktívan (kérések és panaszok kezelése) és passzívan (előzetes tájékoztatás) is elősegíti.

24.4. Átláthatóság alatt mindenekelőtt az érintettek számára egyértelműen meghatározható adatkezelési folyamatok kialakítása értendő, de e mellett az adatkezelő szervnél alkalmazott gyakorlatok áttekinthetőségét, elhatárolhatóságát és nyomonkövethetőségét is jelenti.

Célhoz kötöttség elve

25.1. Személyes adatokat csak meghatározott, egyértelmű és jogszerű célból lehet kezelni vagy feldolgozni. Az adatokat az eredeti céllal össze nem egyeztethető módon tilos kezelni.

25.2. Az alapelv megköveteli, hogy személyes adatokat csak az előre meghatározott cél megvalósulásához szükséges mértékben és ideig lehet kezelni. Az adatkezelő szerv adatkezeléseinél fontos azt is figyelembe venni, hogy csak olyan adatok kezelhetők, amelyek az adatkezelés megvalósításához elengedhetetlenül szükségesek és a cél elérésére alkalmasak.

Adattakarékosság elve

26.1. Az adatkezelésnek mindig az említett céloknak megfelelőnek és relevánsnak kell lennie, továbbá szükséges mértékre kell, hogy korlátozódjon.

26.2. Az alapelvnek megfelelően kerülni kell a felesleges, értelmezhetetlen vagy előre meg nem határozott, jövőbeni célhoz kapcsolódó adatok kezelését.

Pontosság elve

27.1. Az adatokat a kezelésük során pontos és naprakész állapotban kell tartani, minden szükséges intézkedést meg kell tenni annak érdekében, hogy a pontatlan adatokat töröljék vagy helyesbítsék.

27.2. Az alapelv értelmében, ha a kezelt személyes adatok körében pontatlan (hiányos, hibás, sérült) adatok merülnek fel, azokat haladéktalanul pontosítani szükséges. Az érintett kérésének hiányában is az adatkezelő szerv a pontatlan adatokat pontosítani törekszik. A pontosítás meghiúsulása esetén, a pontatlan adatokat valamennyi informatikai rendszerből, adattárolóról és irattárból törölni kell.

27.3. Az adatkezelő szerv teljes szervezete, így valamennyi foglalkoztatottja köteles mindent megtenni annak érdekében, hogy a személyes adatok naprakészek legyenek.

Korlátozott tárolhatóság elve

28.1.A személyes adatok tárolása csak a cél megvalósításához szükséges ideig megengedett.

28.2. Az alapelvnek megfelelően a személyes adatok kezelésének időben mindig meghatározottnak kell lennie. Semmilyen személyes adat sem kezelhető előre meghatározott időkorlát nélkül, továbbá tilos a készletező adatkezelés. Így minden adatkezelési folyamattal érintett személyes adat tekintetében, meg kell állapítani az előirányzott törlési időt.

Integritás és bizalmas jelleg elve

29.1. Az adatkezelést oly módon kell végezni, hogy a megfelelő technikai és szervezési intézkedések alkalmazásával az adatok biztonsága adott legyen.

29.2. Az alapelv által megkövetelt adatbiztonságnak ki kell terjednie mind az elektronikus és a papír alapú adatkezelésekre is, továbbá ezeket fizikai, logikai és adminisztratív intézkedésekkel kell védeni.

Elszámoltathatóság elve

30.1. Az elveknek való megfelelést minden adatkezelési és feldolgozási folyamat tekintetében garantálni kell, továbbá az ennek igazolásához szükséges intézkedéseket is meg kell tenni.

30.2. Az adatkezelő szerv az elszámoltathatóság érdekében világosan meghatározza az adatkezelési irányelveit, átlátható tájékoztatási rendszert hoz létre, nyilvántartást vezet az adatkezelésekről és az esetleges érintetti kérésekről, illetve panaszokról, továbbá az adatvédelmi incidensekről.

Hozzájárulás szabályai

31.1. Az adatkezelő szerv hozzájáruláson alapuló adatkezelései csak akkor lehetnek jogszerűek, ha az érintett egyértelmű megerősítő cselekedettel, például írásbeli – ideértve az elektronikus úton tett – vagy szóbeli nyilatkozattal önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulását adja saját személyes adatai kezeléséhez.

31.2. Hozzájárulással csak az előzetes tájékoztatási kötelezettség teljesítése és az érintett önkéntességének igazolása után kezdhető meg adatkezelés.

31.3. Az önkéntesség nem igazolható, ha az adatkezelés kizárólag az adatkezelő szerv érdekeit szolgálja és a hozzájárulást alá-fölérendeltségi viszonyban adták meg az érintettek. Hozzájárulás önkéntességének bizonyítása az adatkezelő szerv kötelezettsége, így azok megadásáról az adatkezelő szerv nyilvántartást vezet.

31.4. Hozzájárulás bármely olyan formában megadható, amely alapján az érintett azonosítása lehetséges és a hozzájárulás megtörténte rögzíthető.

Adatfeldolgozók igénybevétele

32.1. Az adatkezelő szerv bizonyos adatkezelési tevékenységek vonatkozásában adatfeldolgozót vehet igénybe. Az adatfeldolgozó az adatkezelő szerv megbízásából, annak utasításai szerint az adatkezelő szerv számára adatfeldolgozást végez.

32.2. Adatfeldolgozás történhet megállapodás, vagy jogszabályi előírás alapján. A megállapodás alapján történő adatfeldolgozást írásba kell foglalni. A jogszabályi előírás alapján történő adatfeldolgozást nem szükséges írásba foglalni, amennyiben az adatfeldolgozói jogviszonyt jogszabály teljeskörűen szabályozza.

32.3. Adatfeldolgozói megállapodás minimális tartalmi követelményei az alábbiak:
a) az adatkezelő szerv és az adatfeldolgozó megjelölése;
b) az adatfeldolgozó feladatai;
c) a feldolgozásra átadott személyes adatok típusa, az adatok, valamint az érintettek köre;
d) a szerződés teljesítésére és megszűnésére vonatkozó rendelkezések;
e) a felelősségi kérdések, illetve helytállási kötelezettségek harmadik személy irányába;
f) az adatkezelő utasítási jogköre;
g) az adatfeldolgozó joga további adatfeldolgozók igénybevételére;
h) az adatvédelmi incidensekkel kapcsolatos tájékoztatási kötelezettség;
i) az adatfeldolgozó titoktartási kötelezettsége;
j) az érintetti jogok biztosítására vonatkozó előírások;
k) az adatfeldolgozó adatbiztonsági megfelelőségére vonatkozó nyilatkozata.

Adatkezelési nyilvántartás

33.1. Az adatkezelő szerv az adatkezelési folyamatokról nyilvántartás vezet, melyben a következő információk kerülnek feltüntetésre:
a) az adatkezelő neve és elérhetősége;
b) az adatkezelés célja;
c) az érintetti kategóriák;
d) a személyes adatok fajtái;

e) a címzettek kategóriái;
f) adattovábbítás harmadik országba vagy nemzetközi szervezethez;
g) az egyes adatkategóriákra előírt törlési határidő;
h) technikai és szervezési intézkedések összegzése.

33.2. A nyilvántartást naprakész állapotban kell tartani.

VII. Az adatközlési eljárásrend

34.1. Adatközlések lehetnek adattovábbítások és adatküldések. Adattovábbítás megvalósulhat harmadik személyhez történő adatközléssel, külföldre történő adatközléssel, harmadik országba történő adatközléssel, vagy nyilvánosságra hozatallal.

34.2. Az Európai Gazdasági Térségen belüli adattovábbítás csak a szabályzat által meghatározott valamely jogalap fennállása esetén lehetséges. Harmadik országba vagy nemzetközi szervezet részére továbbított adatokra minden esetben a GDPR V. fejezetében található rendelkezéseket kell megfelelően alkalmazni.

34.3. Hozzájáruláson alapuló adatkezelések tekintetében történő adattovábbításra a hozzájárulásnak kifejezetten ki kell terjednie.

34.5. Az adattovábbítás körülményeit a következő pontok szerint kell dokumentálni:
a) az adattovábbítás címzettje;
b) adattovábbítás célja, időpontja, jogalapja;
c) érintett személyek és adatok köre;
d) az adattovábbítás módszere.

34.5. A jogszabály által kifejezetten nevesített, adattovábbítási felhatalmazásokkal érintett eseteken kívüli egyéb adattovábbítások vonatkozásában, az adattovábbítást megelőzően ki kell kérni az adatvédelmi tisztviselő véleményét. Az adatok továbbítására kizárólag érdemi vizsgálatot követően, akkor van lehetőség, ha a vizsgálat eredményeként annak megállapítására kerül sor, hogy az adattovábbítás az adatvédelmi szabályok betartásával, az érintetti jogok tiszteletben tartása mellett megvalósítható.

34.5. Adatküldésnek minősül az adatkezelő szerv saját szervezet rendszerén belüli adatközlés, az adatok adatfeldolgozó részére történ átadása, valamint az érintett saját személyes adataihoz történő hozzáférése.

VIII. Az adatvédelmi hatásvizsgálat eljárásrendje

35.1. Ha az adatkezelés valamely – 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 szerv 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.

35.2. Az adatvédelmi hatásvizsgálat célja az adatkezelés jellegének feltárása, szükségességének és arányosságának vizsgálata, valamint a személyes adatok kezeléséből eredően a természetes személyek jogait és szabadságait érintő kockázatok kezelésének elősegítése, e kockázatok értékelésével és a kezelésükre szolgáló intézkedések meghatározásával.

35.3. Az adatvédelmi hatásvizsgálatot különösen az alábbi esetekben kell elvégezni:
a) természetes személyekre vonatkozó egyes személyes jellemzők olyan módszeres és kiterjedt értékelése, amely automatizált adatkezelésen – ideértve a profilalkotást is – alapul, és amelyre a természetes személy tekintetében joghatással bíró vagy a természetes személyt hasonlóképpen, jelentős mértékben érintő döntések épülnek;
b) a személyes adatok különleges kategóriáira vonatkozó személyes adatok nagy számban történő kezelése; vagy
c) nyilvános helyek nagymértékű, módszeres megfigyelése.

35.4. A hatásvizsgálat kiterjed legalább:
a) a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő szerv közfeladata ellátásához fűződő érdekeket;
b) az adatkezelés céljaira figyelemmel, az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
c) az érintett jogait és szabadságait érintő kockázatok vizsgálatára; és
d) a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

35.5. Az adatkezelő szerv 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.

35.6. Ha az adatvédelmi hatásvizsgálat azt jelzi, hogy a kockázat mérséklését célzó garanciák, biztonsági intézkedések és mechanizmusok hiányában, az adatkezelés magas kockázattal járna a természetes személyek jogaira és szabadságaira nézve, és a adatkezelő szerv vezetőjének véleménye alapján a kockázat nem mérsékelhető a rendelkezésre álló technológiák és a végrehajtási költségek szempontjából észszerű módon, akkor az adatkezelési tevékenység megkezdése előtt a felügyeleti hatósággal konzultálni kell.

IX. Incidenskezelési eljárásrend

36.1. Az adatkezelő szerv a természetes személyek jogaira és szabadságaira nézve kockázattal járó adatvédelmi incidenst indokolatlan késedelem nélkül, de lehetőség szerint a

tudomásszerzéstől számított hetvenkét órán belül bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak. Abban az esetben, ha a bejelentés akadályba ütközik, akkor a késedelem okát és minden egyéb fontos információt is meg kell küldeni a hatóságnak.

36.2. Ha bizonyítható, hogy az incidens nem jár kockázattal a természetes személyek jogaira és szabadságaira, akkor el lehet tekinteni a bejelentéstől.

36.3. A bejelentésért az adatkezelő szerv vezetője a felelős.

36.4. Az incidensről szóló bejelentésben legalább a következőket meg kell jelölni:
a) az incidens jellegét, az érintettek becsült számát és kategóriáit;
b) az érintett adatok becsült számát és kategóriáit;
c) az incidensből eredő valószínűsíthető következményeket;
d) a hátrányos következmények enyhítését célzó már megtett vagy tervezett intézkedéseket;
e) a kapcsolattartó nevét és elérhetőségeit.

36.5. Az adatkezelő szerv az adatvédelmi incidensekről nyilvántartást vezet, amiben felsorolja a kapcsolódó tényeket és körülményeket, a következményeket és hatásokat, illetve a megtett intézkedéseket.

36.6. Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár, az adatkezelő szerv a hatóság mellett, indokolatlan késedelem nélkül értesíti az érintettet is. Az érintett számára a tájékoztatást világosan és közérthetően kell megadni, kitérve legalább az incidens jellegére, a következményekre és a megtett vagy tervezett intézkedésekre, illetve a kapcsolattartó megnevezésére. Ha a tájékoztatás megtétele aránytalan erőfeszítéssel járna, az érintettek nyilvánosan közzétett információkkal vagy hasonlóan hatékony intézkedéssel is tájékoztathatók.

X. Az adatbiztonságra vonatkozó alapvető rendelkezések

Az adatbiztonság alapkövetelményei

37.1. Az egyes adatbiztonsági intézkedéseket az adatkezelő szerv a kockázatokkal arányos módon, a tudomány és a technológia állásának és a megvalósítás költségeinek figyelembevételével, valamint az adatkezelési és feldolgozási folyamatok jellegére, hatókörére és céljaira, továbbá a természetes személyek jogaira és szabadságaira tekintettel határozza meg.

37.2. Az elektronikus információs rendszerekben tárolt és feldolgozott adatok sértetlenségének megőrzése érdekében gondoskodni kell az ügyviteli és üzemeltetési folyamatok és szabályok megfelelő kialakításáról, így különösen:
a) az adatosztályozás során legalább a magas vagy kritikus biztonsági osztályba sorolt adatokat titkosítottan kell tárolni, kezelni és továbbítani;
b) a munkaállomás és a felhasználó folyamatos és egyértelmű azonosítását biztosítani kell;

c) az adatkezelési műveletekre használt informatikai rendszerelemeknek a biztonság elvárt fokának megfelelő módon bizalmasnak és sértetlennek kell lenniük, továbbá a szükséges mértékben rendelkezésre kell állniuk.

37.3. Adattovábbítás esetén, annak biztonságáról az adatkezelő szerv és a címzett szervezet között olyan megállapodást kell kötni, amely mindkét fél által támasztott követelményeknek megfelel.

37.4. Biztosítani kell az elektronikus üzenetekben továbbított információk biztonságát és rendelkezésre állását. Ehhez meg kell határozni azokat az eljárásokat, amelyeket az elektronikus üzenetek továbbítása során alkalmaznak.

37.5. A hardver eszközök selejtezése, megsemmisítése, vagy továbbértékesítése előtt a hardver eszköz adathordozóját visszaállíthatatlanul törölni kell.

Jogosultságkezelési eljárásrend

38.1. Az adatkezelő szerv kiemelten fontosnak tartja, hogy minden felhasználó csak azokhoz az erőforrásokhoz, információkhoz és adatokhoz férjen hozzá, amelyek a munkavégzéshez, feladatellátáshoz feltétlenül szükségesek.

38.2. A használatban lévő valamennyi informatikai rendszerben tárolt adathoz hozzáférni csak a személyazonosság és a jogosultság ellenőrzésével lehetséges, ezáltal elháríthatók a rendszerekhez való jogosulatlan hozzáférések.

38.3. Hitelesítés és azonosítás nélkül csak az adatkezelő szerv honlapjának publikus oldalai használhatók, egyéb felhasználói tevékenység nem végezhető.

38.4. Az egyes alkalmazásokban funkciónkként, illetve egyes adatkörökre vonatkozóan szükséges a hozzáférés korlátozása, illetve a jogosultsággal nem rendelkezők kizárása.

38.5. Az adatkezelő szerv egyes felhasználóinak hozzáférési szintje a belépéskor kerül meghatározásra és szükség szerint kell felülvizsgálni. Az adatkezelő szerv minden felhasználója csak a munkaköréhez feltétlenül szükséges adatokhoz férhet hozzá.

Jelszókezelés

39.1. Az adatkezelő szerv informatikai rendszereihez való hozzáféréshez fizikai hitelesítési eszközöket vagy felhasználói név és jelszó párost használ.

39.2. Az adatkezelő szerv a megfelelő jelszó használat érdekében, minden foglalkoztatottjától elvárja, hogy a jelszavaik a következő követelményeknek megfeleljenek:
a) a jelszavak bizalmasságát és titkosságát megőrizzék, azokat mindenki számára hozzáférhetetlen helyen tárolják;

b) tilos a jelszavakat szervezeten belül és azon kívül is megosztani;
c) a jelszavaknak legalább 8 karakterből kell állniuk, illetve vegyesen kis és nagybetűket, számokat, írásjeleket és lehetőség szerint ékezetes betűket is tartalmazniuk kell;
d) a felhasználói jelszavakat javasolt 6 havonta, de legalább évente meg kell változtatni;
e) tilos a munkahelyi/munkavégzési céllal használt jelszavakat, magáncélú bejelentkezési felületeken is használni;
f) tilos olyan módon meghatározni, hogy az, az adott felhasználóra jellemző legyen.

39.3. A jelszavak kezelésekor a titkosságot a felhasználónak meg kell őriznie, hogy az más tudomására ne juthasson, ennek megfelelően az elektronikus rendszerekbe való belépéskor, illetve a jelszó megváltoztatásakor a jelszavak azonosíthatatlanul kell, hogy megjelenjenek a képernyőn.

39.4. A jelszavakat tartalmazó fájlokat (illetve ezeknek a jelszavakat tartalmazó részét) visszafejthetetlen (egyirányú) kódolással kell tárolni, ezekhez az állományokhoz hozzáférési jogosultságot az adatkezelő szerv vezetője vagy az általa kijelölt személy kaphat.

39.5. A felhasználók hozzáférési jogait rendszeresen át kell tekinteni, hogy minden felhasználó csakis azokhoz az információkhoz férhessen hozzá, amelyek munkájához aktuálisan szükségesek.

40.1. A fizikai hitelesítésre szolgáló eszköz – így különösen token, chipkártya, vagy más, fizikailag birtokolt hitelesítő eszköz – kizárólag annak a személynek a használatára jogosít, akinek a nevére azt kiállították. Az ilyen eszköz más személy részére nem ruházható át, nem kölcsönözhető, és ideiglenes jelleggel sem adható át.

40.2. A fizikai hitelesítő eszközt a jogosult felhasználó köteles rendeltetésszerűen használni, megóvni az elvesztéstől, sérüléstől és jogosulatlan hozzáféréstől. Tilos a fizikai hitelesítő eszközt őrizetlenül hagyni vagy olyan módon tárolni, hogy ahhoz illetéktelen személy hozzáférhessen. Munkaidőn kívül az eszközt biztonságos helyen kell elhelyezni.

40.3. Amennyiben a fizikai hitelesítő eszköz használatához kiegészítő azonosító – különösen PIN-kód – tartozik, azt a felhasználó köteles bizalmasan kezelni. A kiegészítő azonosító nem tárolható együtt a fizikai hitelesítő eszközzel, nem rögzíthető az eszközön, és nem lehet azonos más, hivatali vagy magáncélú azonosítóval.

40.4. A fizikai hitelesítő eszköz kizárólag hivatali célokra használható. Tilos annak magáncélú informatikai rendszerekhez, nem engedélyezett alkalmazásokhoz vagy nem hivatali szolgáltatásokhoz történő felhasználása.

40.5. A fizikai hitelesítő eszköz elvesztését, eltulajdonítását, sérülését, illetve bármilyen, a jogosulatlan használat gyanúját felvető körülményt a felhasználó köteles haladéktalanul jelezni az adatkezelő szerv vezetője részére. A bejelentést követően a szükséges technikai és szervezési intézkedéseket haladéktalanul meg kell tenni.

40.6. A fizikai hitelesítő eszköz használatával végrehajtott műveletek a jogosult felhasználó felelősségi körébe tartoznak. A jogosultság megszűnésével – így különösen a jogviszony megszűnése vagy a munkakör megváltozása esetén – a fizikai hitelesítő eszközt haladéktalanul vissza kell szolgáltatni, és/vagy a hozzá kapcsolódó jogosultságokat meg kell szüntetni.

41. A adatkezelő szerv legalább évente egyszer felülvizsgálja a felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, a felelősségüket, továbbá ellenőrzi a Szabályzat vonatkozó rendelkezéseinek a megvalósulását, illetve betartását.

Szervezeti tudatosságnövelés

42.1. Az adatkezelő szerv valamennyi felhasználójának a munkakörének és a biztonsági szintnek megfelelő tudással kell rendelkeznie a szervezet biztonsági szabályairól és eljárásrendjeiről.

42.2. Az ismeretek rendszeres frissítéséről és bővítéséről gondoskodni kell a szervezettől elvárható mértékben.

42.3. Az adatvédelmi tudatosságnak legalább a következőkre kell kiterjednie:
a) az adatbiztonság megfelelő szintjének eléréséhez szükséges technikai és szervezési intézkedések ismeretére;
b) a szervezetet és a felhasználókat terhelő jogi felelősségre;
c) az adatbiztonsági incidensek megelőzésére, valamint az elhárító és kárenyhítő intézkedésekre;
d) az információs rendszerek rendeltetésszerű és biztonságos használatára;
e) az adatkezeléssel összefüggő belső szabályzatok és eljárások ismeretére;
f) az adatkezelő szervet terhelő egyéb jogszabályi kötelezettségekre, különös tekintettel az adatkezelési rendelkezésekre és az etikai szabályokra.

42.4. A tudatosságnövelés módszertanának meghatározása, ütemezése és tárgyának megválasztása az adatkezelő szerv vezetőjének hatáskörébe tartozik. Az adatkezelő szerv vezetője e körben az adatvédelmi tisztviselő bevonását kezdeményezi.

Ellenőrzési eljárásrend

43.1. A Szabályzatban meghatározott eljárásrendek és előírások betartása nélkül a Szabályzat célja nem biztosítható. Ennek érdekében az adatkezelő szerv vezetői eseti vagy rendszeres ellenőrzéseket tarthatnak. Az ellenőrzések során feltárt szabálysértések a vonatkozó jogszabályok és belső szabályzatok szerint felelősségre vonást vonhatnak maguk után.

43.2. Az ellenőrzés lefolytatásához meg kell határozni az érintett területeket, és az ezekhez tartozó célkitűzéseket. A célkitűzéseknek megfelelően kell kijelölni az ellenőrzés eszközeit és

tartalmi követelményeit. Az ellenőrzés eredményének értékelésével levonhatók a megfelelő következtetések az adatbiztonságra vonatkozóan.

43.3. Az adatkezelő szerv nem vesz igénybe a felhasználók megfigyelésére és ellenőrzésére, külön erre a célra fejlesztett célszoftvereket.

43.4. Az ellenőrzés során feltárt mulasztásos vagy tevőleges szabálysértések esetén fegyelmi eljárást jelen Szabályzat Adatvédelmi fegyelmi eljárásra vonatkozó rendelkezései szerint kell indítani.

43.5. Az adatkezelő szerv ellenőrzései során a következő területekre fektet nagy hangsúlyt:
a) a szervezet megfelel-e a jogszabályok által megkövetelt személyi, tárgyi és eljárási feltételeknek;
b) az informatikai biztonsági szint megfelel-e a kezelt személyes adatok által megkívánt adatbiztonsági elvárásoknak;
c) a Szabályzat rendelkezéseit az érintett foglalkoztatottak megfelelően ismerik és betartják-e azokat.

Az asztali munkaállomások, mobil eszközök ellenőrzése

44. Az adatkezelő szerv által a foglalkoztatottjai részére munkavégzés céljából rendelkezésre bocsátott számítógépet, laptopot a foglalkoztatottjai kizárólag munkaköri feladata ellátására használhatja. A magáncélú használatot az adatkezelő szerv megtiltja, ezen eszközökön a foglalkoztatott semmilyen személyes adatot, magáncélú levelezést nem kezelhet és nem tárolhat. A munkáltató ezen eszközökön tárolt adatokat ellenőrizheti. A tényleges magánhasználat ellenőrzése céljából adatgyűjtésre kizárólag a foglalkoztatott jelenlétében, illetve tájékoztatása mellett – személyiségi jogaira és az adatvédelemi előírásokra tekintettel – a nyilvánvalóan visszaélésszerű magánhasználat esetén van csak lehetőség.

Adatvédelmi fegyelmi eljárás

45.1. A Szabályzat előírásainak súlyos megsértésének minősül, és fegyelmi eljárás megindítását alapozhatja meg különösen az alábbi esetek valamelyike:
a) valamely informatikai rendszerhez tartozó hozzáférési adatok illetéktelen személy részére történő átadása vagy tudomására hozatala;
b) szabálysértés következtében személyes adatok illetéktelen személy birtokába kerülése;
c) szabálysértés következtében személyes adatok elvesztése, megsemmisülése, illetve olyan sérülése, amelynek következtében a személyes adatok rendelkezésre állása nem biztosítható;
d) személyes adatok szándékos meghamisítása;
e) szabálysértés következtében az adatkezelő szerv adatbiztonsági intézkedései, védelmi megoldásai vagy a biztonsági rendszer működése illetéktelen személyek számára megismerhetővé válik;
f) a Szabályzat rendelkezéseinek ismételt szándékos vagy többszöri gondatlan megsértése.

45.2. A fegyelmi eljárás megindításáért az adatkezelő szerv vezetője a felelős, lefolytatására a hatályban levő egyéb fegyelmi ügyekre vonatkozó szabályokat kell alkalmazni.

XI. Biztonsági intézkedések katalógusa

46. Az adatkezelő szerv összhangban a Szabályzat alapelveivel és szellemiségével törekszik a normatív szabályozáson túl a gyakorlatban megvalósítani az adatbiztonsági előírásokat. Ennek érdekében érthető és jól körülhatárolt munkahelyi magatartási szabályokat alkot, továbbá egyéb kötelező biztonsági intézkedésekről gondoskodik, amelyek a Szabályzat általános elvárásait ültetik át az adatkezelő szerv ügymenetébe. Az adatkezelő szerv folyamatosan gondoskodik a felhasználói tudatosságának növeléséről, abból a célból, hogy tudatában legyenek a biztonsági fenyegetéseknek és elkötelezettek legyenek a Szabályzat előírásainak betartására.

Papír alapú adatkezelésekre vonatkozó szabályok

47.1. A papír alapon tárolt adatokat biztonságos, illetve jogosulatlanok számára hozzáférhetetlen helyen kell tárolni. A használatban lévő iratokhoz csak az arra jogosult foglalkoztatottak férhetnek hozzá.

47.2. Ha az elektronikus úton felvett adatokat a belső szabályok és gyakorlatok szerint nyomtatni szükséges, azokat legalább elkülönített és lehetőleg elzárt irattárolóban kell tárolni. Az adatkezelő szerv foglalkoztatottjai kötelesek arról gondoskodni, hogy az ilyen iratokhoz illetéktelenek ne férhessenek hozzá. A kinyomtatás okának megszűntével a papír alapú iratokat haladéktalanul meg kell semmisíteni.

47.3. Az irattárba való iratokat zárható száraz, az állaguk megóvására alkalmas helyiségben kell tárolni, a tűz és vagyonvédelem biztosítása érdekében.

Elektronikus adatkezelésre vonatkozó szabályok

48.1. Az információs rendszerekben úgy kell tárolni az adatokat, hogy megfelelő védelmet tudjon biztosítani a jogosulatlan hozzáféréstől, szándékos és véletlen törléstől, illetve külső támadásokkal szemben. Külső támadások vonatkozásában különösen védelmet kell nyújtani a kémprogramokkal, vírusokkal és rendszerfeltörésekkel szemben.

48.2. A hozzáférés és hitelesítés érdekében a munkaállomásokat jelszavas beléptetéssel kell ellátni, továbbá a védendő adatokat erős jelszavakkal kell védeni.

48.3, A foglalkoztatottak a munkaállomás ideiglenes elhagyása esetén kötelesek a munkaállomást képernyőzárral védeni, amelyet úgy kell beállítani, hogy a munkamenet folytatásakor ismételten hitelesítse a foglalkoztatottat.

49. Amennyiben személyes adatok tárolására mobil eszközök kerülnek felhasználásra, azokat biztonságos helyen, illetéktelen személyektől elzártan kell tárolni. A személyes adatokat tároló mobil eszközöket, csak az adatkezelő szerv vezetőjének engedélyével és utasításainak megfelelően lehet az adatkezelő szerv területéről kivinni.

50. Az adatokat csak az adatkezelő szerv vezetője által meghatározott hardver egységeken lehet tárolni.

51. Felhő alapú tárolás esetén előzetesen meg kell győződni arról, hogy a külső tárhelyszolgáltató megfelel-e, az adatkezelő szerv által megkövetelt adatvédelmi jogi és technikai követelményeknek.

52. Az adattárolásra szolgáló munkaállomásokat folyamatosan vírusirtó szoftverrel és tűzfallal kell védeni.

53. Az adatkezelő szerv belső hálózatára kapcsolt információs rendszerekre tilos ellenőrizetlen szoftvereket letölteni és telepíteni.

54. Személyes adatokat csak olyan levelezőrendszer használatával szabad küldeni, amelynek biztonsága és zártsága igazolt a szolgáltató által.

Számítógép használati elvek

55.1. A felhasználók kötelesek arra, hogy csak az általuk, adott pillanatban ténylegesen használt papír alapú dokumentumokat és adatokat tartsák az asztalon, illetve jelenítsék meg a képernyőn. Kötelesek továbbá arra is, hogy a munkavégzés felfüggesztésekor vagy annak befejeztével a dokumentumokat és adatokat ne hagyják hozzáférhető helyen (clean desk policy).

55.2. A felhasználók kötelesek meggyőződni arról, hogy a munkavégzésük alatt jogosulatlanok nem nyernek betekintést a kezelt személyes adatokba vagy egyéb szenzitív információkba.

55.3. Külső támadások esetén különösen védelmet kell nyújtani a kémprogramokkal, vírusokkal és rendszerfeltörésekkel szemben.

55.4. Amennyiben személyes adatok tárolására mobil eszközök kerülnek felhasználásra, azokat biztonságos helyen, illetéktelen személyektől elzártan kell tárolni.

Fizikai védelem

56.1. A felhasználóknak tilos a munkaállomás hardver konfigurációját megváltoztatni, a hardver eszköz belsejébe bármilyen okból belenyúlni, burkolatukat megbontani, továbbá a külső perifériák csatlakozását megszüntetni.

56.2. Az adatkezelő szerv nyomtatóit úgy kell elhelyezni, hogy a kinyomtatott anyagok illetéktelen kezekbe ne kerülhessenek.

Szoftveres védelem

57.1. A felhasználóknak tilos bármilyen szoftvert előzetes jóváhagyás nélkül telepíteni a munkaállomásokra. A szoftver igényeket az adatkezelő szerv vezetője felé kell jelezni.

57.2. A munkaállomások operációs rendszereit úgy kell beállítani, hogy ha öt percen túl a rendszer használaton kívül van, az automatikusan lezárja a munkaállomást. Így a munka újbóli megkezdésekor a felhasználó a felhasználónév és jelszó páros megadásával ismét azonosíthatja magát.

57.3. A foglalkoztatottak továbbá kötelesek arra, hogy az általuk őrizetlenül hagyott berendezéseket, mobil eszközöket és alkalmazásokat saját maguk zárják le.

Távoli elérés

58.1. Távoli hozzáférés és munkavégzés csak indokolt esetben engedélyezhető, továbbá kizárólag akkor, ha a munkavégzés biztonsága legalább az adatkezelő szerv által elvárt szintet képes elérni.
58.2. A mobil eszközök használatakor ellenőrizni kell az eszközökhöz való hozzáférést, azok logikai és fizikai védelmét, az adatmentések megvalósulását és a biztonságos környezeten kívüli munkavégzés körülményeit.

58.3. A külső összeköttetések munkaidőn kívül feltétlenül szükségesen elérni kívánt rendszerekhez engedélyezettek.

58.4. A mobil eszközök szállítása során biztosítani kell, hogy az eszköz ne legyen kitéve erős rázásnak vagy ütésnek. A mobil eszközt tilos felügyelet nélkül hagyni.

58.5. A hordozható eszközökön külön engedéllyel tárolt személyes adatok és szenzitív információk védelmére hardveres és/vagy szoftveres titkosító eszközök használata szükséges. Ilyen esetben a titkosító kulcsokat külön eszközön kell tárolni.

Internethasználat

59.1. Tekintve, hogy az adatkezelő szerv ügymenete, feladatellátása szempontjából elengedhetetlen az internetkapcsolat a felhasználóknak a következő előírásokat kell követniük a munkájuk során:
a) tilos az internetet jogellenes célokra használni, illetve mások személyiségi jogait megsérteni;
b) tilos mások szerzői jogait megsérteni vagy tiltott haszonszerzésre irányuló tevékenységet folytatni;
c) tilos szoftvereket szándékosan jogellenes módon terjeszteni;

d) tilos másokat sértő módon használni az internetet;
e) tilos mások vallási, etnikai, politikai vagy egyéb érzékenységét sérteni;
f) tilos másokat zaklató tevékenységet folytatni;
g) tilos az adatkezelő szerv tevékenységi körén kívül eső haszonszerzésre irányuló direkt üzleti tevékenység és reklámok terjesztése;
h) tilos a hálózatot nagymértékben és indokolatlanul megzavaró vagy veszélyeztető tevékenység;
i) tilos a hálózatot és erőforrásait szándékosan túlzott mértékben igénybe venni;
j) tilos az interneten a beszállítókat és szolgáltatókat, illetve azok termékeit vagy szolgáltatásait minősíteni;
k) tilos az adatkezelő szerv által képviselt értékek szerint méltatlan oldalak keresése vagy látogatása;
l) tilos olyan adatot, információt vagy szoftvert le vagy feltölteni, amely összeférhetetlen a Szabályzat előírásaival;
m) tilos az internetről ingyenesen letölthető szoftverek munkaállomásokra történő letöltése és telepítése;
n) internetezés közben el kell utasítani azokat a felbukkanó párbeszéd ablakokat, amelyek segédprogramok telepítésére, vagy egyes funkciók kikapcsolására ösztönöznek.
59.2. Az adatkezelő szerv fenntartja a jogot arra, hogy a felhasználók számára bármely weboldal látogatását a jövőben megtiltsa, vagy a böngészési tevékenységet olyan módon korlátozza, hogy taxatívan felsorolja, melyek azok az oldalak, amelyek látogathatók.

Elektronikus levelezés

60.1. A munkahelyi levelezés során kezelt minden postafiókkal kapcsolatban be kell tartani a Szabályzatot és a jogszabályok vonatkozó rendelkezéseit. Ennek elmaradása esetén szankció alkalmazandó.

60.2. Az adatkezelő szerv hálózatán történő elektronikus levelezésre a felhasználók csak saját elektronikus levelezési címüket használhatják. A felhasználók postafiókjaikat minden körülmények között csak munkavégzésre használhatják.

60.3. Az adatkezelő szerv levelezőrendszerének megosztott postafiókjához a hozzáférés előre meghatározott jogosultság alapján történik.

60.4. Levelezéssel kapcsolatos különös tiltások:
a) tilos a közízlést, az adatkezelő szerv jó hírnevét veszélyeztető, erkölcstelen tartalmú e-mail küldése;
b) tilos a levelezőrendszert személyes adatok, egyéb szenzitív információk vagy dokumentumok kijuttatására használni;
c) tilos az adatkezelő szerv hivatalos ügyeit a nem munkavégzésre rendelt levélcímen intézni;
d) tilos feliratkozni nem szakmai jellegű hírlevél szolgáltatásra;
e) tilos olyan üzenetekre válaszolni, amely az adatkezelő szerv rendszeréről, a felhasználó hozzáférési adatairól vagy más védettnek minősített információról kér tájékoztatást;

f) tilos személyes adatokat tartalmazó dokumentumokat vagy adatbázisokat titkosítás nélkül továbbítani.

XII. Záró rendelkezések

61. Jelen szabályzat 2026. február 16. napján lép hatályba.

62. Jelen szabályzat hatályba lépésével a 2005. december 1. napjától hatályos „Adatvédelmi és Adatbiztonsági Szabályzat" hatályát veszti.

Kozármisleny, 2026. február 16.

A Kozármislenyi Közös Hivatal részéről:

.....

Dr. Göndöcz András, jegyző
Kozármislenyi Közös Önkormányzati Hivatal

A szabályzat hatálya alá tartozó Önkormányzatok részéről:

.....

Dr. Pohl Marietta, polgármester
Kozármisleny Város Önkormányzata

.....

Rácz János, polgármester

Egerág Község Önkormányzata

.....

Varga Zsolt, polgármester

Kisherend Község Önkormányzata

.....

Barics Arnold, elnök

Kozármislenyi Horvát Nemzetiségi Önkormányzat

.....

Horváthné Hauschl Edit Anna, elnök

Kozármislenyi Német Nemzetiségi Önkormányzat

.....

Orsós Mária, elnök

Kozármislenyi Roma Nemzetiségi Önkormányzat

1. számú melléklet: Adatvédelmi Tisztviselő kijelölésének indokolása

A GDPR 37. cikk (1) bekezdése alapján az adatkezelő szerv alaposan megvizsgálta működésének körülményeit és az alábbi következtetésekre jutott.

A a) pont értelmében közhatalmi szervek, illetve egyéb, közfeladatot ellátó szervek kötelesek az adatvédelmi tisztviselő kijelölésére. Tekintettel arra, hogy a Közös Önkormányzati Hivatal és a szabályzat hatálya alá tartozó helyi önkormányzatok a Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény 13.§ alapján, a szabályzat hatálya alá tartozó nemzetiségi önkormányzatok a nemzetiségek jogairól szóló 2011. évi CLXXIX. törvény 115. § értelmében közfeladatot ellátó szervnek (bizonyos feladatai körében közhatalom gyakorlásának) minősülnek, a GDPR 37.cikk (1) bekezdés a) pontja alapján kötelesek adatvédelmi tisztviselő kijelölésére.