General Data Protection Regulation (GDPR)
Általános Adatvédelmi rendelet

ADATVÉDELMI SZABÁLYZAT

TARTALOMJEGYZÉK

ÁLTALÁNOS ADATVÉDELEM

1. AZ ADATVÉDELMI ÉS ADATKEZELÉSI SZABÁLYZAT ALKALMAZÁSA

A szervezet megnevezése:	Agro-World Egyesület
A szervezet székhelye:	3300 Eger Vitkovics u. 8/a
A szabályzat tartalmáért felelős személy:	Dr. Horváth Ágnes elnök
A szabályzat hatályba lépésének dátuma:	2018. 11. 21.

Ez a szabályzat a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a személyes adatok szabad áramlására vonatkozó szabályokat állapít meg. A szabályzatban foglaltakat kell alkalmazni a konkrét adatkezelési tevékenységek során, valamint az adatkezelést szabályozó utasítások és tájékoztatások kiadásakor.

Abban az esetben, ha a fő tevékenységek olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé, vagy az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelésére vonatkoznak, adatvédelmi tisztviselőt kell kinevezni. Az adatvédelmi tisztviselő kinevezése az adatbiztonság megerősítését célozza.

A szervezet fő tevékenysége □ ilyen jellegű □ nem ilyen jellegű
A szervezet adatvédelmi tisztviselőt □ alkalmaz □ nem alkalmaz

Adatvédelmi tisztviselő alkalmazása esetén:

Neve:	-
Beosztása:	-
Elérhetősége:	-

Az adatvédelmi tisztviselő fenti adatait az adatkezelő köteles a felügyeleti Hatósággal is közölni!

2. A SZABÁLYZAT CÉLJA

Az adatvédelmi és adatbiztonsági szabályzat célja a Agro-World Egyesület (a továbbiakban: Szervezet) tevékenységével összefüggésben a személyes adatok védelméhez fűződő jog

érvényesülésének biztosítása, a Szervezet által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása, a személyes adatok kezelése során irányadó adatvédelmi és adatbiztonsági előírások meghatározása, az adatkezelési tevékenységek tekintetében a Szervezet egyéb belső szabályzati előírásainak harmonizálása a természetes személyek alapvető jogainak és szabadságainak védelme érdekében, valamint a személyes adatok megfelelő kezelésének a biztosítása. A szabályozás kiterjed az adatkezelő hatáskörére és felelősségére.

A Szervezet tevékenysége során teljes mértékben meg kíván felelni a személyes adatok kezelésére vonatkozó jogszabályi előírásoknak, különösen az Európai Parlament és a Tanács (EU) 2016/679 rendeletében foglaltaknak, ezért amennyiben szükséges, a jelen Szabályzaton túl további belső adatvédelmi szabályokat alkalmaz. A szabályokat az adatkezelés jellegének, hatókörének, körülményeinek és céljainak, valamint a természetes személyek jogait és szabadságait érintő kockázatnak a figyelembevételével kell meghozni.

A szabályozás az alábbi jogszabályokra, ajánlásokra és irányelvekre, belső szabályozásokra alapozva, azokkal teljes összhangban került kialakításra:

- 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 rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)
- Magyarország Alaptörvényének VI. cikke,
- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.),
- 2013. évi LXXVII. törvény a felnőttképzésről,
- 2011. évi CLXXXVII. törvény a szakképzésről;
- a Polgári Törvénykönyvről szóló 2013. évi V. törvény,
- a személy és vagyonvédelmi, valamint magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII törvény (a továbbiakban: vagyonvédelmi tv.),
- a munka törvénykönyvéről szóló 2012. évi I. törvény (a továbbiakban: Mt.),
- az egyének védelméről és az ilyen adatok szabad áramlásáról szóló Európai Parlament és a Tanács 1995. október 24-i 95/46/EK irányelve,
- az elektronikus hírközlésről szóló 2003. évi C. törvény,
- a fogyasztóvédelemről szóló 1997. évi CLV. törvény,
- a Nemzeti Adatvédelmi és Információszabadság Hatóság 2013. január 23-án kiadott ajánlása a munkahelyen alkalmazott elektronikus megfigyelőrendszer alapvető követelményeiről.

3. HATÁLY- ÉS FELELŐSSÉG MEGHATÁROZÁSA

3.1. SZEMÉLYI HATÁLY

A szabályzat személyi hatálya kiterjed a Szervezet szervezeti egységeire, munkavállalóira, valamint a Szervezettel szerződéses jogviszonyban álló természetes és jogi személyre, jogi személyiséggel nem rendelkező szervezetre, a velük kötött szerződésben, illetve titoktartási nyilatkozatokban rögzített mértékben.

3.2. TÁRGYI HATÁLY

Tárgyi hatálya kiterjed a Szervezet szervezeti egységeinél folytatott minden olyan adatkezelésre és adatfeldolgozásra, amely személyes adatra vonatkozik, függetlenül attól, hogy az adatkezelés, illetve adatfeldolgozás teljesen, vagy részben elektronikus informatikai eszközzel, vagy manuális módon történik.

3.3. A SZABÁLYZAT MÓDOSÍTÁSA

A szabályzat elkészítése és szükség szerinti módosítása a Szervezet belső adatvédelmi kapcsolattartójának (a továbbiakban: adatvédelmi kapcsolattartó) a feladata.

4. FOGALMAK MEGHATAROZÁSA

A szabályzat alkalmazása során – összhangban a GDPR, az Infotv., valamint az Mt. előírásaival – a következőkben meghatározott fogalmak irányadók:

adat: valamilyen jelrendszerben ábrázolt jelek, vagy elemi jelek sorozata, amelyeknek jelentésük, értelmük van, valamire vonatkoznak, valamit leírunk velük. Az adatok teljes információtartalmát adat-környezetük határozza meg, így az adat jelentésétől megfosztott információ.

adatállomány: az egy nyilvántartásban kezelt adatok összessége.

adatbázis: az adatok szervezett gyűjteménye, amelyet egy – az adatok tárolására, lekérdezésére és szerkesztésére alkalmas – szoftvereszköz kezel. Az adatbázis lényege, hogy az adatok mellett az adatok között lévő kapcsolatokat is tárolja. Az adatbázis fogalmát meg kell különböztetni az adatbázis-kezelőtől, amely az adatbázis működtetésére, rendszerszintű és felhasználói folyamatok szervezésére szolgáló szoftver eszköz (program).

adatcsoport: adatok, (azaz tények, koncepciók vagy utasítások formalizált megjelenítése, rögzített jelsorozat, beszéd vagy technikai eszközökkel történő közlés, értelmezés és feldolgozás számára. Jelen Szabályzatban írásban vagy elektronikus úton készített – bármilyen adathordozón tárolt – szöveg, számadatsor, tény, információ, vázlat, grafikon, kép és ábra) és adatkörök összefoglaló elnevezése, általában nyilvántartási funkció alapján.

adatbiztonság: az informatikai (adattároló és feldolgozó) rendszer azon állapota, amelyben az adatok elvesztésének illetve megsemmisülésének kockázata a megfelelő intézkedésekkel

elviselhető mértékűre csökkenthető. Ez az állapot olyan nemzetközi szabványokon alapuló előírások és megelőző biztonsági intézkedések betartásának eredménye, amelyek az információk elérhetőségét, sérthetetlenségét és megbízhatóságát érintik.

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

adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján – beleértve a jogszabály rendelkezése alapján kötött szerződést is – adatok feldolgozását végzi.

adathordozó: az adat fizikai megjelenési formája, tárolási helye, ide értve az iratokat is.

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.

az adatkezelés korlátozása: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából.

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.

adatkör: az adatfajták nevesített felsorolása. A felhasználás szempontjából funkcionálisan összetartozó üzleti adatok, azaz olyan halmaz, amely logikai szinten egységesen kezelhető, illetve kezelendő és a halmaz elemeinek védelmi igénye közel egy szinten van. (Pl.: Kassza Rendszer adatok, készpénz átutalási adatok).

adatmegsemmisítés: Az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése.

adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele.

adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges.

adatmegjelölés: az adat azonosító jelzéssel ellátása annak megkülönböztetése céljából.

adatkezelés korlátozása: a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából.

adatvédelem: a személyes adat jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.

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.

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.

adatvédelmi kapcsolattartó: az adatkezelő által megbízott, az adatvédelmi ismeretek terén kellő tájékozottsággal rendelkező munkavállaló, aki részt vesz az adatkezelést érintő feladatok végrehajtásában és kapcsolatot tart az adatvédelmi kapcsolattartóval.

adatzárolás: az adat azonosító jelzéssel ellátása további kezelésének végleges vagy meghatározott időre történő korlátozása céljából.

anonimizálás: olyan technikai eljárás, amely biztosítja az érintett és az adat közötti kapcsolat helyreállítási lehetőségének végleges kizárását.

bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően, a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat.

cookie (süti): rövid adatfájl, melyek a meglátogatott honlap helyez el a felhasználó számítógépén, abból a célból, hogy az adott infokommunikációs, internetes szolgáltatást megkönnyítse, kényelmesebbé tegye. Számos fajtája létezik, de általában két nagy csoportba sorolható. Az egyik az ideiglenes cookie, amelyet a honlap csak egy adott munkamenet során (pl.: egy internetes bankolás biztonsági azonosítása alatt) helyez el a felhasználó eszközén, a másik fajtája az állandó cookie (pl. egy honlap nyelvi beállítása), amely addig a számítógépen marad, amíg a felhasználó le nem törli azt. Tekintve, hogy a cookie segítségével nyomon követhetők a felhasználó böngészési szokásai, ezért azt kizárólag a felhasználó engedélyével lehet a felhasználó eszközén elhelyezni.

direkt marketing (közvetlen üzletszerzési) tevékenység: azoknak a közvetlen megkeresés módszerével végzett tájékoztató tevékenységeknek és kiegészítő szolgáltatásoknak az összessége, amelyeknek célja az érintett részére termékek vagy szolgáltatások ajánlása, hirdetések továbbítása, a fogyasztók vagy kereskedelmi partnerek tájékoztatása, üzletkötés (vásárlás) előmozdítása érdekében.

érintett: bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül vagy közvetve – azonosítható természetes személy. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több, fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.

harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel vagy az adatfeldolgozóval.

személyes adatok határokon átnyúló adatkezelése:

- személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó több tagállamban található tevékenységi helyein folytatott tevékenységekkel összefüggésben kerül sor; vagy
- személyes adatoknak az Unióban megvalósuló olyan kezelése, amelyre az adatkezelő vagy az adatfeldolgozó egyetlen tevékenységi helyén folytatott tevékenységekkel összefüggésben kerül sor úgy, hogy egynél több tagállamban jelentős mértékben érint vagy valószínűsíthetően jelentős mértékben érint érintetteket.

harmadik ország: minden olyan ország, amely az Info tv. alapján nem (Európai Gazdasági Térség) EGT-állam.

hozzájárulás: az érintett akaratának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok – teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez. A hozzájárulás – a különleges adatok kezelésére adott hozzájárulást kivéve – nincs alakszerűséghez kötve, történhet kifejezett nyilatkozattal és ráutaló magatartással is, azonban a hozzájárulásnak minden esetben bizonyíthatónak kell lennie.

informatikai eszköz: bármely feladat ellátására létrehozott, informatikai technológia felhasználásával működtetett (pl. vezérelt) telepített, vagy mobil eszközök, továbbá rendszerek, eljárások összessége, vagy ezek alkotó elemei. (Pl.: számítógép, hordozható informatikai eszköz és adattároló, nyomtató, operációs rendszer, felhasználói programok [irodai alkalmazások, adatbáziskezelő, vezérlő programok, beágyazott informatikai rendszerek és egyéb egyedi fejlesztésű célprogramok stb.], továbbá az informatikai alapokra épülő távközlési rendszerek [pl. IP telefon rendszer és végberendezései, hálózati aktív és passzív eszközök], valamint a hálózatmenedzsment elemei)

informatikai eszközök ellenőrzésének indokolt esetei különösen:

- a munkavállaló mobiltelefon használatánál a számára engedélyezett költségkeretet indokolatlanul túllépi,
- a munkavállaló munkaköre gyakorlása során tudomására jutott védendő információt arra illetéktelen személlyel, vagy szervezettel megosztja,
- a munkavállaló munkáltatója felé fennálló együttműködési kötelezettségét megszegve jár el,

- amennyiben az érintett munkavállaló nyilatkozatának beszerzése lehetetlen és azt a közeli hozzátartozója írásban, indokai megjelölésével kéri, továbbá alappal feltehető, hogy az adatok kiadása az érintett munkavállaló létfontosságú érdekei védelméhez szükséges, valamint az adatok kiadását az adatvédelmi kapcsolattartó, szükség szerint a Jogi Igazgatóság véleményének kikérését követően, indokoltnak, az információs önrendelkezési jog korlátozásával arányosnak tartja,
- minden olyan körülmény, amely alapján alappal feltételezhető, hogy a munkavállaló az általában elvárható etikai normák súlyos megszegésével járt el, és azt az adatvédelmi kapcsolattartó is indokoltnak, az információs önrendelkezési jog korlátozásával arányosnak tartja.

irat: valamely szerv működésével, illetve személy tevékenységével kapcsolatban írásban vagy elektronikus úton készített szöveg, számadatsor, vázlat, grafikon és ábra.

kötelező adatkezelés: a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelés időtartamát, valamint az adatkezelő személyét az adatkezelést elrendelő törvény vagy önkormányzati rendelet határozza meg.

közterület: a közhasználatra szolgáló olyan állami vagy önkormányzati tulajdonban álló terület, amelyet rendeltetésének megfelelően mindenki korlátozás nélkül igénybe vehet, ideértve a közterületnek közútként szolgáló részét is.

különleges adat:

- a faji eredetre, a nemzeti és etnikai kisebbséghez tartozásra, a politikai véleményre vagy pártállásra, vallásos vagy más világnézeti meggyőződésre, érdekképviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,
- az egészségi állapotra, a kórós szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat.

megfelelő tájékoztatás: az érintettel az adatkezelés megkezdése előtt közölni kell, hogy az adatkezelés a hozzájárulásán alapul-e vagy kötelező, továbbá egyértelműen és részletesen tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről, az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is.

Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH): Nemzeti Adatvédelmi és Információszabadság Hatóság: Jogállását és feladatait az Info tv. 38.§-a határozza meg (a továbbiakban: Hatóság).

nyilvános adat: minden olyan tény, adat, információ, amelyek bárki számára hozzáférhetők. Személyes adat nyilvánosságáról kizárólag törvény rendelkezhet.

nyilvánosságra hozatal: az adat bárki számára hozzáférhetővé tétele.

személyes adat: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy

szociális azonosságára jellemző ismeret –, valamint az adatból levonható, az érintettre vonatkozó következtetés. A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható, tehát az adatkezelő rendelkezik azokkal a feltételekkel, amelyek a helyreállításhoz szükségesek.

személyes adat-gazda: egy adott szervezeti egységnél kezelt személyes adatok tekintetében a szervezeti egységet irányító vezető, áruházak esetében az áruházvezető, aki felelős a szervezeti egysége által kezelt valamennyi személyes adat jelen szabályzatnak megfelelő kezelésért (továbbiakban: adatgazda). Amennyiben IT rendszerben kezelt személyes adattal kapcsolatos döntés meghozatala szükséges, és az érinti az adatgazda felelősségét, akkor a személyes adatgazda a Szabályzat alapján kijelölt vezető egyetértésével hozza meg döntését.

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 használják.

távolról végzett munka/távmunka: a Szervezet informatikai rendszerének biztonsági zónáján kívül eső (nem védett) környezetből végzett tevékenység, amely során a Szervezet a felhasználó számára olyan informatikai erőforrások elérését biztosítja (jellemzően VPN-en keresztül), amellyel a munkahelyén egyébként rendelkezhet. Ide nem értendők azoknak a technológiáknak, illetve mobil informatikai megoldásoknak alkalmi felhasználása, amellyel eseti információcserét lehet megvalósítani. E szabályzat alkalmazása során a távolról végzett munka tartalmában nem azonos a Munka Törvénykönyvében szabályozott távmunka fogalommal.

tiltakozás: az érintett nyilatkozata, amellyel személyes adatának kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adat törlését kéri.

munkahelyi azonosítószám: a Szervezet munkavállalóját az adatkezelés során egyértelműen azonosító, belső azonosítási célokat szolgáló számjegysor.

üzleti titok: a Szervezet gazdasági tevékenységéhez kapcsolódó minden nem közismert vagy az érintett gazdasági tevékenységet végző személyek számára nem könnyen hozzáférhető olyan tény, tájékoztatás, egyéb adat és az azokból készült összeállítás, amelynek illetéktelenek által történő megszerzése, hasznosítása, másokkal való közlése vagy nyilvánosságra hozatala a Szervezet jogos pénzügyi, gazdasági vagy piaci érdekeit sértené vagy veszélyeztetné, feltéve, hogy a titok megőrzésével kapcsolatban a Szervezetet felróhatóság nem terheli.

VPN: (Virtual Private Network – virtuális magánhálózat): olyan informatikai hálózat, amely nyilvános kommunikációs csatornák és eszközök segítségével valósul meg, de az azokon zajló egyéb forgalomtól logikailag elkülönülő, mások számára nem hozzáférhető egységet képez. A VPN az adatok védelmére, a hitelesítés mellett, titkosítást is alkalmaz, miáltal lehetőséget biztosít a Szervezet számára, hogy a belső hálózat meghatározott elemeit

kívülről elérhetővé tegye az erre feljogosított (pl. zárt felhasználói csoport, illetve távmunkát végző) felhasználók számára.

védendő információ: a minősített adat, az üzleti titok, a know-how (védett ismeret), a személyes adat (zártan kezelendő), a nem nyilvánossá, vagy belső használatúvá nyilvánított adat, a döntés-előkészítő dokumentum, továbbá a munkakör betöltésével összefüggésben a munkavállaló tudomására jutott egyéb olyan információ, amelynek illetéktelen személy számára történő hozzáférhetővé tétele törvényi előírást sért, a munkáltató, vagy más személy számára hátrányos következményeket hordozhat, továbbá a Szervezet által kezelt azon adatok, amelyek bizalmasságához, sértetlenségéhez, rendelkezésre állásához a Szervezetnek érdeke fűződik, kivéve, ha a nyilvánosságra hozatalt jogszabály, illetve belső utasítás írja elő, továbbá azt az arra jogosult korábban már nyilvánosságra hozta.

zártan kezelendő: a személyes adatot tartalmazó dokumentumok általános védelmi előírása. Amennyiben az adathordozóról nem állapítható meg egyértelműen adattartalmának védendő jellege, vagy az adatkezelő külön ki kívánja emelni a kezelés zártságának követelményét, abban az esetben ezt kezelési utasításként kell a dokumentumon feltüntetni.

5. A SZEMÉLYES ADATOK KEZELÉSE ÉS VÉDELME

5.1. ALAPELVEK ÉS ALAPVETŐ RENDELKEZÉSEK

A Szervezetnél a személyes adatok kezelését jogszerűen és tisztességesen kell végezni, az érintett számára átláthatóan, nyomon követhetően. **(„jogszerűség, tisztességes eljárás és átláthatóság")**

A személyes adatok gyűjtése csak előre megfogalmazott, egyértelmű és jogszerű célból történhet, és az adtakezelés célja szempontjából megfelelőek, pontosak és relevánsak legyenek, és csak annyi adatot kezeljen, ami a cél eléréséhez szükséges. **(„célhoz kötöttség")**

A Szervezetnél a személyes adatoknak az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell lenniük, és a gyűjtésüknek csak a szükségesre kell korlátozódniuk. **(„adattakarékosság")**

A Szervezet által kezelt adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tennünk annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljük vagy helyesbítsük. **(„pontosság")**

A felvett személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé, így minden adatkezelési időtartam lejárta után az adatokat törölni kell. **(„korlátozott tárolhatóság")**

A személyes adatok kezelését a Szervezetnél oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyenek a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve. **(„integritás és bizalmas jelleg")**

A célhoz kötöttség elve megvalósulásának vizsgálata minden esetben az illetékes adatkezelő szervezeti egység feladata és felelőssége. Az adat kiadására – ideértve a Szervezet szervezeti egységei közötti adatátadásokat is – vonatkozó kérések esetében az adatkérőnek az adatkérés célját minden esetben meg kell jelölni, az adatszolgáltató pedig köteles mérlegelni, hogy a kért adatok a megjelölt cél eléréséhez elengedhetetlenül szükségesek-e. Az adatkérőnek kizárólag olyan adat adható át, ami a cél eléréséhez elengedhetetlenül szükséges. Amennyiben az adatkezelés célhoz kötöttsége kétséges, az adatgazda köteles a kérdésben a belső adatvédelmi kapcsolattartó állásfoglalását beszerezni.

A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha a Szervezet rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.

Az adatvédelem elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell.

A szervezet adatkezelést végző alkalmazottja fegyelmi, kártérítési, szabálysértési és büntetőjogi felelősséggel tartozik a személyes adatok jogszerű kezeléséért. Amennyiben az alkalmazott tudomást szerez arról, hogy az általa kezelt személyes adat hibás, hiányos, vagy időszerűtlen, köteles azt helyesbíteni, vagy helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni.

A gyermekek személyes adatai különös védelmet érdemelnek, mivel ők kevésbé lehetnek tisztában a személyes adatok kezelésével összefüggő kockázatokkal, következményeivel és az ahhoz kapcsolódó garanciákkal és jogosultságokkal. Az adatkezelő kötelessége, hogy megfelelő és hatékony intézkedéseket hajtson végre, valamint hogy képes legyen igazolni azt, hogy az adatkezelési tevékenységek a hatályos jogszabályoknak megfelelnek.

Az adatkezelő vagy az adatfeldolgozó megfelelő nyilvántartást vezet a hatásköre alapján végzett adatkezelési tevékenységekről. Minden adatkezelő és adatfeldolgozó köteles a felügyeleti hatósággal együttműködni és ezeket a nyilvántartásokat kérésre hozzáférhetővé tenni az érintett adatkezelési műveletek ellenőrzése érdekében

Annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, az adatkezelő törlési vagy rendszeres felülvizsgálati határidőket állapít meg. A szervezet vezetője által megállapított rendszeres felülvizsgálati határidő: 1 év.

5.2. AZ ADATKEZELÉSSEK KAPCSOLATOS JOGOK

A tájékoztatáskéréshez való jog: bármely személy a megadott elérhetőségeken keresztül tájékoztatást kérhet arról, hogy a szervezet milyen adatait, milyen jogalapon, milyen adatkezelési cél miatt, milyen forrásból, mennyi ideig kezeli. A kérelmére haladéktalanul, de legfeljebb 30 napon belül, a megadott elérhetőségre tájékoztatást kell küldeni.

A helyesbítéshez való jog: bármely személy a megadott elérhetőségeken keresztül kérheti bármely adatának módosítását. Erről kérelmére haladéktalanul, de legfeljebb 30 napon belül intézkedni kell és a megadott elérhetőségre tájékoztatást kell küldeni.

A törléshez való jog: bármely személy a megadott elérhetőségeken keresztül kérheti adatának törlését. Kérelmére ezt haladéktalanul, de legfeljebb 30 napon belül meg kell tenni és a megadott elérhetőségre tájékoztatást kell küldeni.

A zároláshoz, korlátozáshoz való jog: bármely személy a megadott elérhetőségeken keresztül kérheti adatának zárolását. A zárolás addig tart, amíg a megjelölt indok szükségessé teszi az adatok tárolását. A kérelemre ezt haladéktalanul, de legfeljebb 30 napon belül meg kell tenni és a megadott elérhetőségre tájékoztatást kell küldeni.

A tiltakozáshoz való jog: bármely személy a megadott elérhetőségeken keresztül tiltakozhat az adatkezelés ellen. A tiltakozást a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 15 napon belül meg kell vizsgálni, annak megalapozottsága kérdésében döntést kell hozni és a döntésről a megadott elérhetőségre tájékoztatást kell küldeni.

Az adatkezeléssel kapcsolatos jogérvényesítési lehetőség:

Nemzeti Adatvédelmi és Információszabadság Hatóság
Postacím: 1530 Budapest, Pf.: 5.
Cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/c
Telefon: +36 (1) 391-1400
Fax: +36 (1) 391-1410
E-mail: ugyfelszolgalat@naih.hu
URL https://naih.hu

Az érintett a jogainak megsértése esetén az adatátvevő az adatkezelő ellen bírósághoz fordulhat. A bíróság az ügyben soron kívül jár el. A pert az érintett – választása szerint – a lakóhelye vagy tartózkodási helye szerint illetékes törvényszék előtt is megindíthatja.

5.3. AZ ADATKEZELÉS JOGALAPJA

Személyes adatot a Szervezet akkor kezelhet, ha

1. az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
2. azt törvény vagy – törvény felhatalmazása alapján, az abban meghatározott körben – helyi önkormányzat rendelete közérdeken alapuló célból elrendeli (a továbbiakban: kötelező adatkezelés),
3. az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
4. az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
5. az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
6. az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges; utóbbi esetben azonban csak akkor, ha a szóban forgó adatkezelés egyéb jogalapon nem végezhető.
7. az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan

érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Jogos érdekről lehet szó olyankor, amikor releváns és megfelelő kapcsolat áll fenn az érintett és az adatkezelő között, például olyan esetekben, amikor az érintett az adatkezelő ügyfele vagy annak alkalmazásában áll. Személyes adatoknak a csalások megelőzése céljából feltétlenül szükséges kezelése szintén az érintett adatkezelő jogos érdekének minősül. Személyes adatok közvetlen üzletszerzési célú kezelése szintén jogos érdeken alapulónak tekinthető.

A jogos érdek fennállásának megállapításához mindenképpen körültekintően meg kell vizsgálni többek között azt, hogy az érintett a személyes adatok gyűjtésének időpontjában és azzal összefüggésben számíthat-e ésszerűen arra, hogy adatkezelésre az adott célból kerülhet sor. Az érintett érdekei és alapvető jogai elsőbbséget élvezhetnek az adatkezelő érdekével szemben, ha a személyes adatokat olyan körülmények között kezelik, amelyek közepette az érintettek nem számítanak további adatkezelésre.

Ha az érintett cselekvőképtelensége folytán vagy más elháríthatatlan okból nem képes hozzájárulását megadni, akkor a saját vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges mértékben a hozzájárulás akadályainak fennállása alatt az érintett személyes adatait a Szervezet kezelheti.

A 16. életévét be nem töltött kiskorú érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása szükséges.

Különleges adatot a Szervezet az érintett kifejezett hozzájárulása, törvény elrendelése alapján, meghatározott esetekben kezelhet.

Kétség esetén azt kell vélelmezni, hogy az érintett a hozzájárulását nem adta meg. Amennyiben az érintett a Szervezetnél írásban kötött szerződés teljesítése érdekében adja hozzájárulását az adatkezeléshez, a szerződésnek tartalmaznia kell minden olyan információt, amelyet a személyes adatok kezelése szempontjából az érintettnek ismernie kell, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, a felhasználás célját, az adatok továbbításának tényét, címzettjeit, adatfeldolgozó igénybevételét. A szerződésnek félreérthetetlen módon tartalmaznia kell, hogy az érintett aláírásával hozzájárul az adatai szerződésben meghatározottak szerinti kezeléséhez.

Mivel a természetes személyek összefüggésbe hozhatók az általuk használt készülékek, alkalmazások, eszközök és protokollok által rendelkezésre bocsátott online azonosítókkal, például IP-címekkel és cookie-azonosítókkal, ezért ezek az adatok egyéb információkkal összekapcsolva alkalmasak és felhasználhatók a természetes személyek profiljának létrehozására és az adott személy azonosítására.

Az adatkezelésre csak akkor kerülhet sor, ha az érintett személy egyértelmű megerősítő cselekedettel, például írásbeli - ideértve az elektronikus úton tett - vagy szóbeli nyilatkozattal önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulását adja az adatok kezeléséhez.

Az adatkezeléshez való hozzájárulásnak minősül az is, ha az érintett személy az internetes honlap megtekintése során bejelöl egy erre vonatkozó négyzetet. A hallgatás, az előre bejelölt négyzet vagy a nem cselekvés nem minősül hozzájárulásnak.

Hozzájárulásnak minősül az is, ha valamely felhasználó az elektronikus szolgáltatások igénybevétele során erre vonatkozó technikai beállításokat hajt végre, vagy olyan nyilatkozatot illetve cselekedet tesz, amely az adott összefüggésben az érintett személy hozzájárulását személyes adatainak kezeléséhez egyértelműen jelzi.

Amennyiben az adatkezelés hozzájáruláson alapul, az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult.

Ha az érintett a hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell közölni.

Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.

Annak megállapítása során, hogy a hozzájárulás önkéntes-e, a lehető legnagyobb mértékben figyelembe kell venni azt a tényt, egyebek mellett, hogy a szerződés teljesítésének – beleértve a szolgáltatások nyújtását is – feltételéül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez.

Közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában végzett személyes adatok kezelése akkor jogszerű, ha a gyermek a 16. életévét betöltötte. A 16. életévét be nem töltött gyermek esetén, a gyermekek személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte.

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

5.4. AZ ÉRINTETT ELŐZETES TÁJÉKOZTATÁSÁNAK KÖVETELMÉNYE

A tisztességes és átlátható adatkezelés elve megköveteli, hogy az érintett tájékoztatást kapjon az adatkezelés tényéről és céljairól, valamint arról, hogy az adatkezelés milyen jogalappal történik.

Az érintettre vonatkozó személyes adatok kezelésével összefüggő tájékoztatást az adatgyűjtés időpontjában kell az érintett részére megadni, illetve ha az adatokat nem az érintettől, hanem más forrásból gyűjtötték, az ügy körülményeit figyelembe véve, ésszerű határidőn belül kell rendelkezésre bocsátani.

Ha a személyes adatokat az érintettől gyűjtik, az érintettet arról is tájékoztatni kell, hogy köteles-e a személyes adatokat közölni, valamint hogy az adatszolgáltatás elmaradása milyen következményekkel jár. Ezeket az információkat szabványosított ikonokkal is ki lehet egészíteni annak érdekében, hogy az érintett a tervezett adatkezelésről jól látható, könnyen érthető és jól olvasható formában általános tájékoztatást kapjon.

Az érintett jogosult, hogy hozzáférjen a rá vonatkozóan gyűjtött adatokhoz, valamint arra, hogy egyszerűen és ésszerű időközönként, az adatkezelés jogszerűségének megállapítása és ellenőrzése érdekében gyakorolja e jogát. Minden érintett számára biztosítani kell a jogot arra, hogy megismerje különösen a személyes adatok kezelésének céljait, továbbá ha lehetséges, azt, hogy a személyes adatok kezelése milyen időtartamra vonatkozik.

Az érintett jogosult különösen arra, hogy személyes adatait töröljék és a továbbiakban ne kezeljék, ha a személyes adatok gyűjtésére vagy más módon való kezelésére az adatkezelés eredeti céljaival összefüggésben már nincs szükség, vagy ha az érintettek visszavonták az adatok kezeléséhez adott hozzájárulásukat.

Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett számára biztosítani kell a jogot arra, hogy bármikor díjmentesen tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen.

Kötelező adatkezelés esetén nem szükséges az érintett hozzájárulásának a beszerzése és nem kell az érintettel adatvédelmi nyilatkozatot aláíratni, mert az adatkezelés jogalapja a törvényi felhatalmazás és nem az érintett hozzájárulása. Ebben az esetben is az érintettet tájékoztatni kell az adatkezelés jogalapjáról, tehát arról, hogy melyik jogszabály felhatalmazása alapján történik a személyes adatainak kezelése.

Az adatkezelés megkezdése előtt az adatkezelést végzőnek az érintettet - kérés nélkül is - előzetesen tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva tájékoztatni kell az adatai kezelésével kapcsolatos minden tényről, így különösen

- az adatkezelő kilétéről, elérhetőségéről;
- az adatkezelés céljáról és jogalapjáról;
- a személyes adatok címzettjeiről, illetve a címzettek kategóriáiról;
- az adatfeldolgozó kilétéről,
- az adatkezelés időtartamáról,
- az adattovábbítás címzettjeiről,
- érintetti jogokról;
- visszavonás lehetőségéről, amennyiben hozzájáruláson alapult;
- jogorvoslati lehetőségeiről: adatvédelmi hatósághoz, bírósághoz fordulás,
- kik ismerhetik meg az adatokat, valamint
- a szolgáltatás igénybevétele meghiúsulásáról, ha az ügyfél az ahhoz szükséges személyes
  nem adja meg, illetve nem járul hozzá azok kezeléséhez.

Kötelező adatkezelés esetén a tájékoztatás megtörténhet a jogszabályi rendelkezésekre való utalás nyilvánosságra hozatalával is.

5.5. AZ ADATBIZTONSÁG KÖVETELMÉNYE

A Szervezet az adatkezelés során mindvégig köteles gondoskodni a kezelt személyes adatok biztonságáról (adatbiztonság elve).

Az informatikai rendszerekben megvalósuló adatkezelések során a tudomány és technológia állása, a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket a Szervezet mindenkor hatályos jogszabályoknak megfelelően alkalmaz.

A Szervezet köteles az adatkezelési műveleteket úgy megtervezni és végrehajtani, hogy az biztosítsa az érintettek magánszférájának védelmét.

A Szervezet az adatbázisai védelme érdekében titkosítottan tárolja az általa kezelt személyes adatokat.

A Szervezet illetőleg tevékenységi körében az Informatikai rendszerének üzemeltetője, mint adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az Infotv., és a belső szabályzat, valamint az egyéb adat- és titokvédelmi szabályokban megfogalmazottak érvényre juttatásához szükségesek.

Ennek keretében a Szervezet az adott szervezeti egység által kezelt személyes adatok tekintetében kötelesek:

- Az adatkezelés időtartama alatt az adatok biztonságos tárolása, az időtartam lejártával az adatállomány törlése, fizikai megsemmisítése érdekében a szükséges intézkedéseket megtenni;
- Az adatokat megfelelő intézkedésekkel védeni kell a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés a véletlen megsemmisítés és sérülés, a Szervezet által alkalmazott technika megváltoztatásából fakadó hozzáférhetetlenné válás ellen.
- Gondoskodni arról, hogy a jelen Szabályzatot, valamint a feladatkörükben kiadott külön, a személyes adatok kezeléséről szóló rendelkezéseket az irányításuk alatt dolgozók megismerjék és betartsák, illetve azt folyamatosan ellenőrizni;
- Ellenőrizni, hogy a szervezeti egységében kezelt adatok továbbításukat követően is olyan adatkezelőhöz, adatfeldolgozóhoz kerülnek, aki vagy amely az adatok biztonságos kezeléséről megfelelően gondoskodni tud, ezzel összefüggő kérdésekben jogosult kérni az adatvédelmi kapcsolattartó állásfoglalását.

A Szervezet valamennyi munkavállalója köteles a személyes adatokat tartalmazó iratokat és a munkavégzéshez szükséges segédleteket a munkavégzés befejezését követően – ahol biztosított – zárható lemez- vagy páncélszekrényben, biztonsági zárral ellátott fiókban, szekrényben tárolni. Ahol ezek a feltételek nem biztosítottak ott is törekedni kell az adatok legalább zárral ellátott fiókban, szekrényben történő biztonságos tárolására. Az íróasztalokon a munkavégzés befejezését követően személyes adatokat tartalmazó iratok tárolása tilos.

Az adatokat a Szervezetnek megfelelő intézkedésekkel védenie kell, különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

A személyes adatok automatizált feldolgozása során biztosítania kell a jogosulatlan adatbevitel megakadályozását, annak ellenőrizhetőségét, hogy a személyes adatokat mely szerveknek továbbították, a személyes adatokat mikor és ki vitte be az adatfeldolgozó rendszerbe, a telepített rendszerek üzemzavara esetén az adatok helyreállíthatóságát, valamint azt, hogy a fellépő hibákról jelentés készüljön.

Az elektronikusan kezelt adatállományok védelme érdekében a Szervezet megfelelő technikai megoldással köteles biztosítani, hogy a különböző nyilvántartásokban tárolt adatok – kivéve, ha azt törvény lehetővé teszi – közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők. A Szervezet munkavállalóinak adatai, függetlenül attól, hogy egy közös, vagy osztott adatbázisban szerepelnek, a munkavállaló szempontjából egy nyilvántartásnak tekintendők.

A Szervezet szerződéses jogviszonyban áll adótanácsadó gazdasági szervezettel, aki a könyvelés ellenőrzését és megfelelését végzi.

A Szervezetnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.

Amennyiben az adatkezelő indokoltnak látja, az adatkezelést megelőzően adatvédelmi hatásvizsgálatot folytathat le. A hatásvizsgálat során meg kell vizsgálni, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Ha az adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az adatkezelőnek konzultálnia kell a felügyeleti hatósággal.

5.6. ADATFELDOLGOZÁS

A Szervezet a munkaviszonyból, illetve gazdasági tevékenységének ellátáshoz származó kötelezettségek teljesítése céljából, (számlázáshoz, bérszámfejtéshez, könyveléshez szükséges szoftverek) az adatszolgáltatás céljának megjelölésével, a munkavállalók, illetve az ügyfelek személyes adatait adatfeldolgozó számára átadhatja, amelyről a munkavállalókat, érintett oktatókat előzetesen tájékoztatni kell.

A Szervezet határozza meg az általa megbízott adatfeldolgozónak a személyes adatok feldolgozásával kapcsolatos jogait és kötelezettségeit az adatkezelésre vonatkozó jogszabályi előírások keretei között. Az adatkezelési műveletekre vonatkozó szabályzatok jogszerűségéért és jelen szabályzat előírásainak történő megfelelőségéért a Szervezet, illetve az adatkezelő szervezet vezetője a felelős.

Az adatfeldolgozó az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag a Szervezet rendelkezései szerint dolgozhatja fel, és ezek

felhasználásával saját céljára adatfeldolgozást nem végezhet, továbbá köteles a személyes adatokat a Szervezet rendelkezései szerint tárolni és megőrizni.

A Szervezet az adatfeldolgozásra vonatkozó szerződéseit írásba kell foglalnia. A szerződésnek tartalmaznia kell minden olyan információt, amely a személyes adatok kezelése szempontjából releváns, így különösen a kezelendő adatok meghatározását, az adatkezelés időtartamát, az adatfeldolgozás célját, a kezelendő adatok biztonságával kapcsolatos elvárásokat, az adatok kezelésének ellenőrzési lehetőségét. Az adatfeldolgozással nem bízható meg olyan szervezet, amely a feldolgozandó személyes adatokat felhasználó üzleti tevékenységben akár közvetett, akár közvetlen módon érdekelt. A szerződés kidolgozása során biztosítani kell az adatvédelmi kapcsolattartó véleményezési jogát.

Az adatfeldolgozó tevékenységének ellátása során további adatfeldolgozót a Szervezet rendelkezései alapján vehet igénybe. Amennyiben az adatfeldolgozó további adatfeldolgozót kíván megbízni egyes adatfeldolgozási műveletek elvégzésével, ehhez a Szervezet előzetes írásbeli hozzájárulására van szükség. Az adatkezelésben érintettek vonatkozásában olyan szerződéses kötelezettségeket kell meghatározni, amely az adatkezelés teljes folyamatában biztosítja a megfelelő védelmi szintet. A szerződés kidolgozása során biztosítani kell az adatvédelmi kapcsolattartó véleményezési jogát.

5.7. AZ ÉRINTETTEK JOGAI ÉS ÉRVÉNYESÍTÉSÜK

A Szervezet biztosítani köteles, hogy az érintett a róla kezelt adatokat megismerhesse, a kezelt adatokat tartalmazó iratokról másolatot vagy kivonatot kaphasson.

Az adatkezelő a személyes adatok megszerzésének időpontjában, annak érdekében, hogy a tisztességes és átlátható adatkezelést biztosítsa, az érintettet a következő kiegészítő információkról tájékoztatja:

- a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjairól;
- az érintett azon jogáról, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról;
- a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;
- a felügyeleti hatósághoz címzett panasz benyújtásának jogáról;
- arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása;
- amennyiben fennáll, az automatizált döntéshozatal ténye, ideértve a profilalkotást is, valamint legalább ezekben az esetekben az alkalmazott logikára és arra vonatkozóan érthető információk, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel bír.

Az érintett e kérdésével a Szervezet adatvédelmi kapcsolattartójához is fordulhat.
E-mail: forraspontgasztro@gmail.com
A Szervezetnek az érintett kérelmére legfeljebb 25 napon belül írásban, közérthető formában tájékoztatást kell adnia

- az általa kezelt, illetőleg az általa megbízott adatfeldolgozó által feldolgozott adatairól
- az adatkezelés
    - adatainak forrásáról
    - céljáról
    - jogalapjáról
    - időtartamáról
- az adatfeldolgozó
    - nevéről
    - címéről (székhelyéről)
- az adatkezeléssel összefüggő tevékenységéről
- adattovábbítás esetén annak jogalapjáról és címzettjéről,
- az adatvédelmi incidensekről.

A Szervezet köteles a személyes adatot törölni, amennyiben

- a személyes adatokra már nincsen szükség,
- az érintett kéri, illetve visszavonja hozzájárulását,
- az hiányos vagy téves és ez az állapot jogszerűen nem orvosolható – feltéve, hogy a törlést törvény nem zárja ki,
- az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben meghatározott határideje lejárt,
- az adatkezelés jogellenes,
- a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogi kötelezettség teljesítéséhez törölni kell;
- azt bíróság vagy a NAIH elrendelte.

A Szervezet törlési kötelezettsége nem vonatkozik azon személyes adatra, amelynek adathordozóját a levéltári anyag védelmére vonatkozó jogszabály értelmében levéltári őrizetbe kell adni.

A Szervezet a hibás személyes adatot, amennyiben a valóságnak megfelelő személyes adat a rendelkezésére áll, saját kezdeményezésre, illetve az érintett kérésére, az általa bemutatott dokumentumok, bizonyítékok alapján helyesbíti, illetve az adatfeldolgozónál helyesbítteti.

Az érintett jogosult arra, hogy korlátozza az adatkezelést, ha

- az érintett vitatja a személyes adatok pontosságát, ez esetben a korlátozás arra az időtartamra vonatkozik, amely lehetővé teszi, hogy az adatkezelő ellenőrizze a személyes adatok pontosságát;
- az adatkezelés jogellenes, és az érintett ellenzi az adatok törlését, és ehelyett kéri azok felhasználásának korlátozását,

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

A Szervezet megjelöli az általa kezelt személyes adatot, ha az érintett annak helyességét vagy pontosságát vitatja, de a rendelkezésre álló dokumentumok alapján nem állapítható meg egyértelműen annak helytelensége vagy pontatlansága.

Az adatok törlésről, a helyesbítésről, a zárolásról, a megjelölésről az érintettet, továbbá mindazokat értesíteni kell, akiknek korábban azt adatkezelés céljára továbbították. Az értesítés abban az esetben mellőzhető, ha az – tekintettel az adatkezelés céljára – nem sérti az érintett jogos érdekét.

A kérelem elutasítása esetén az adatkezelő a kérelem kézhezvételét követő 30 napon belül írásban közli az elutasítás indokait, továbbá tájékoztatja az érintettet a bírósági jogorvoslat, valamint a Hatósághoz fordulás lehetőségéről.

5.8. AZ ADATKEZELÉSBEN KÖZREMŰKÖDŐK ÉS FELADATAIK (PRIVACY BY DEFAULT- ALAPÉRTELMEZETT ADATVÉDELEM)

5.8.1. KÉPVISELETRE JOGOSULT

A Szervezet képviseletre jogosultja irányítja és ellenőrzi az adatvédelemmel kapcsolatos feladatok végrehajtását.

5.8.2. ADATVÉDELMI KAPCSOLATTARTÓ/ KOORDINÁTOR

Az adatvédelmi kapcsolattartó feladatai:

- ellenőrzi az Infotv. és az adatkezelésre vonatkozó más jogszabályok, valamint a jelen szabályzat rendelkezéseinek betartását; adatvédelmi incidens esetén feltárja annak körülményeit, hatását, javaslatot tesz az adatkezelő számára az intézkedésekre, amelyről nyilvántartást vezet;
- a megbízott adatvédelmi szakértő közreműködésével ellátja a Szervezet szervezeti egységei adatvédelmi tevékenységének szakirányítását és szakfelügyeletét;
- közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
- kivizsgálja a személyes adatkezeléssel összefüggésben hozzá érkezett bejelentéseket, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;
- vezeti a belső adatvédelmi nyilvántartást, amelynek alapján kezdeményezi a NAIH felé az adatkezelések jogszabály által előírt bejelentését;
- támogatja az adatkezelőt vagy adatfeldolgozót a jogszabályi előírások teljesítésében, a NAIH-nak a Szervezetet érintő intézkedése esetén;
- koordinál az egyes szervezeti egységek között az egységes szemlélet megvalósítása érdekében;
- a más vállalkozóval kötött szerződések keretein belül adatvédelmi kérdésekben koordináló, tanácsadó, ellenőrző tevékenységet végez;
- véleményezi a részére megküldött, adatvédelmi kérdéseket érintő belső szabályozási dokumentumok tervezetét;

- az adatvédelmi kérdésekkel összefüggésben az forraspontgasztro@gmail.com e-mail címen fogadja a Szervezet munkavállalóinak, illetve szerződéses partnereinek megkeresését, konzultációs kérdéseit és azzal érdemben foglakozik;
- az adatvédelmi kérdésekkel összefüggésben tájékoztatja a Szervezet vezetését;
- a tárgyévet követő év január 31-ig gondoskodik a NAIH számára az elutasított tájékozódási kérelmekről szóló tájékoztatás elkészítésétől és megküldéséről.

5.8.3. ADATKEZELÉST VÉGZŐ SZERVEZETI EGYSÉG VEZETŐJE

- gondoskodik az adatvédelmi szabályok végrehajtásának feltételrendszeréről,
- intézkedik az irányítása alá tartozó szervezet által kezelt rendszerben található személyes adatok védelméről,
- intézkedik a nem szabályszerű adatkezelési gyakorlat megszüntetéséről, az eset kivizsgálása érdekében értesíti az adatvédelmi kapcsolattartót és informatikai rendszer érintettsége esetén a rendszer tulajdonosát,
- új adatkezelés létrehozása esetén irányítja a feladatok végrehajtását,
- szervezeti egységénél irányítja és ellenőrzi a személyes adatok kezelésével, azok készítésével, továbbításával összefüggő adatvédelmi tevékenységet,
- kijelöli és megbízza a területi adatvédelmi szakértőt,
- intézkedik az adatkezelő felé az érintett által hozzá benyújtott, tiltakoztatási illetve tájékozódási jog teljesülése érdekében.

5.8.4. SZEMÉLYES ADATOKAT KEZELŐ MUNKAVÁLLALÓ

A Szervezet azon munkavállalója, aki személyes adatok kezelésével kapcsolatos tevékenységet végez, köteles gondoskodni arról, hogy

- az adatkezelés teljes folyamatában maradéktalanul érvényesüljenek az adatvédelmi előírások
- indokolt esetben a személyes adatot tartalmazó adathordozókon és dokumentumokon a „Zártan kezelendő” kezelési jelölés feltüntetésre kerüljön
- az informatikai eszközök adathordozóján tárolt személyes adatok törlése esetén azok a későbbiekben ne legyenek visszaállíthatók
- a személyes adat indokolt esetben törlésre, illetve zárolásra kerüljön.
- irányítja és ellenőrzi a személyes adatok kezelésével, azok készítésével, továbbításával összefüggő adatvédelmi tevékenységet.

5.9. HATÓSÁGI ADATSZOLGÁLTATÁSOK

A hivatalos szervektől – bíróság, közigazgatási szerv– érkezett, személyes adatokat érintő adatszolgáltatást az illetékes szervezeti egység a megkeresésben megadott határidőig, ennek hiányában 15 napon belül teljesíti, a Szervezet általi adatszolgáltatás folyamatáról szóló mindenkori hatályos szabályozásban foglaltaknak megfelelően.

A nyomozó hatósági adatkéréseket a hatósági adatkérésben illetékes szervezet munkavállalója teljesíti.

Ha a megkeresés alakisága, a megkereséssel érintett adatkör kiadhatósága aggályos, az illetékes szervezeti egység a belső adatvédelmi kapcsolattartó soron kívüli állásfoglalását kéri.

Ha a megkeresés jogszerűségét a belső adatvédelmi kapcsolattartó is aggályosnak tartja, köteles az ügyben a Hatóság sürgősségi eljárását kezdeményezni.

A megkeresés ez esetben a Hatóság állásfoglalásától függően teljesíthető, kivéve, ha az állásfoglalás a megkeresésben megadott határidő alatt nem érkezik meg a Szervezet részére. Ez esetben a megkeresést a megadott határidőben a Szervezet kijelölt szervezeti egysége teljesíti.

5.10. BELSŐ ADATVÉDELMI NYILVÁNTARTÁS

Az adatkezelést végző szervezeti egység vezetője nyilvántartásba vétel céljából, alapján köteles a Szervezet adatvédelmi kapcsolattartójának bejelenteni az adatkezelésre vonatkozó adatokat, továbbá az adatkezelésre vonatkozóan helyi adatvédelmi és adatkezelési szabályozást ad ki, amely az adatkezelésre vonatkozó bejelentésben szereplő adatokon túlmenően tartalmazza az adatokhoz hozzáféréssel rendelkezők körét, valamint az adatok elektronikus feldolgozása esetén az adatok mentésének, azok tárolásának rendjét is.

Az adatkezelésről szóló bejelentést, valamint a helyi adatvédelmi és adatkezelési szabályozást az adatkezelés megkezdését megelőzően legalább 15 nappal meg kell küldeni az adatvédelmi felelősnek a nyilvántartás napra készen történő tartása céljából.

Meglévő adatkezelésből történő legyűjtés eredményeként létrejövő adatkezelés új adatkezelésnek számít, amennyiben az adatkezelés célja eltérően kerül megfogalmazásra, vagy az adatkezelő személye megváltozik. Ilyen esetben erre vonatkozóan is bejelentési, illetve szabályzatkészítési kötelezettség lép életbe. Vitás esetben az adatvédelmi szakértő állásfoglalását kell kérni.

A belső adatvédelmi nyilvántartásba bejelentett adatok változását, vagy az adatkezelés megszűnését az adatkezelésért felelős szervezeti egység vezetője nyolc napon belül köteles bejelenteni a Szervezet adatvédelmi kapcsolattartójának, aki ennek megfelelően módosítja a belső adatvédelmi nyilvántartás adatait, és ha szükséges, kezdeményezi a NAIH szerinti bejegyzés módosítását.

Melléklet: Adatvédelmi nyilvántartás (elektronikus)

5.11. ADATTOVÁBBÍTÁSI NYILVÁNTARTÁS

A Szervezet adattovábbítást végző adatkezelőinek nyilvántartást kell vezetnie az általuk végrehajtott adattovábbítások jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából, amelynek tartalmaznia kell a kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét, a továbbított személyes adatok körének meghatározását. A nyilvántartás papír alapon, és elektronikus úton is vezethető.

A felállított adattovábbítási nyilvántartásról, annak papír alapú, vagy elektronikus jellegéről az adatvédelmi kapcsolattartót tájékoztatni kell. A tájékoztatás tartalmazza a létrehozás idejét, helyét, kezelőjét stb. Nem szükséges külön adattovábbítási nyilvántartás készítése amennyiben az adatok a rendszerből lekérdezés útján egyértelműen kimutathatók. A nyilvántartásban az adatokat öt évig, különleges adatok esetében húsz évig meg kell őrizni.

Melléklet: Adattovábbítási nyilvántartás (elektronikus)

5.12. ADATTOVÁBBÍTÁS

Személyes adatot továbbítani harmadik személy részére csak törvény alapján, vagy az érintett hozzájárulásával lehet, ha az adatkezelés feltételei minden egyes személyes adatra nézve teljesülnek.

Az adatfeldolgozásra irányuló adatátadás nem minősül adattovábbításnak. Az adattovábbítást megelőzően az adatgazda kötelessége megvizsgálni, hogy annak törvényi feltételei fennállnak-e, illetve a továbbítást követően az adatkezelés feltételei minden egyes személyes adatra megvalósulnak-e.

Ugyanazon adatkezelők számára történő, azonos érintettre vonatkozó, és azonos célú adattovábbítás előtt az adatvédelmi kapcsolattartót is be kell vonni a folyamatba. Az ezt követő adattovábbítások során külön vizsgálatot lefolytatni nem kell.

Az adattovábbításról a jelen Szabályzat – adattovábbítási nyilvántartás (elektronikus) szerinti formában adattovábbítási nyilvántartást köteles az adott szervezeti egység vezetni, amelynek egy példányát a tárgyévet követő év január 15-éig az irattárban kell elhelyezni. Az adattovábbítási nyilvántartást az adatátvétel, illetve az adattovábbítás évét követő ötödik év végéig (különleges adatok esetén húsz évig) kell megőrizni.

Az adattovábbítási nyilvántartás tartalmazza:

- az adattovábbító által kezelt/gyűjtött személyes adatok továbbításának időpontját,
- a továbbított adatköröket,
- az adattovábbítás jogalapját és címzettjét (név, cím, székhely),
- az adattovábbításért felelős nevét és telefonszámát.

5.13. AZ ADATKEZELÉS RÉSZLETES SZABÁLYAI, A SZERVEZET ÁLTAL KEZELT ADATCSOPORTOK

Személyes adatok a Szervezet szervezeti keretein belül a következő csoportokban kezelhetők:

- ügyfél adatok, beleértve a Szervezet szolgáltatásait igénybe vevő ügyfélkapcsolati adatokat is;
- a Szervezettel egyéb szerződéses kapcsolatban álló természetes személyek adatai (partnernyilvántartás);
- a Szervezet munkavállalóinak adatai (beleértve a toborzással kapcsolatban keletkező, nem munkavállalókhoz kapcsolódó adatokat, valamint az érintett munkavállaló kérelmére indult eljárásban;
- a Szervezet direkt marketing, piackutatási tevékenységével kapcsolatos adatok, adatnyilvántartások, tilalmi nyilvántartások;
- hatósági adatszolgáltatások;
- belső adatvédelmi nyilvántartás;
- adattovábbítási nyilvántartás.

5.14. AZ ADATVÉDELMI SZABÁLYOK MEGTARTÁSÁNAK ELLENŐRZÉSE

Az adatvédelmi és adatbiztonsági intézkedések betartásának, valamint jelen szabályzat rendelkezései érvényesülésének ellenőrzésére jogosultak:

- a Szervezet képviseletre jogosult vezetője
- az adatvédelmi kapcsolattartó
- a jogszabályban erre felhatalmazott személy (például a NAIH tisztviselői)
- a Szervezet által megbízott személy (pl. külső auditor).

Az ellenőrzésnek különösen az alábbiakra kell kiterjednie:

- adatkezelési szabályzat
- adatkezelési tájékoztató és adatvédelmi nyilatkozat
- az adatvédelmi nyilvántartás vezetése
- feliratok, piktogramok megléte
- a munkavállalók betekintési- és hozzáférési jogosultságának naprakészsége
- a fizikai biztonsági előírások érvényesülése
- a jelszavak időszakonkénti cseréje
- az adattovábbítási nyilvántartás vezetése
- adathordozók meglétének szúrópróbaszerű ellenőrzése
- a selejtezés, megsemmisítés végrehajtására, dokumentálása
- a jelen szabályzat rendelkezéseinek betartása.

5.15. AZ ADATVÉDELMI RENDELKEZÉSEK MEGSÉRTÉSE ESETÉN KÖVETENDŐ ELJÁRÁS

Az adatvédelmi szabályok megsértése, vagy ennek közvetlen veszélye észlelése esetén, bárki közvetlenül az adatvédelmi kapcsolattartóhoz fordulhat. Az 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. Ilyen eset lehet, ha nagy mennyiségű személyes adatot tartalmazó adathordozó eltűnik, elveszik, a munkavállaló elhagyja azt. Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést.

Az adatvédelmi kapcsolattartó a bejelentés megalapozottsága, illetve az adatvédelmi előírások megsértésének észlelése esetén annak megszüntetésére szólítja fel az adatkezelőt, és azokkal a munkavállalókkal szemben, akik a Szervezet adatvédelmi és adatbiztonsági szabályzata előírásait megsértették, az érintett munkáltatói jogkörgyakorlójánál hátrányos jogkövetkezmény megállapítására vonatkozó munkáltatói intézkedést, esetlegesen tényfeltáró vizsgálatot kezdeményez. A megállapítás, illetve a tényfeltáró vizsgálat az adatvédelmi kapcsolattartó bevonásával történik.

Az adatvédelmi kapcsolattartó az eset valamennyi körülményére tekintettel mérlegeli, hogy az incidens be kell-e jelenteni a hatóságnak, és az adatvédelmi szakértőnek. A szakértő teljes egészében szakmai tanácsokkal látja el a kapcsolattartót, aki minden incidenst felvesz a belső nyilvántartásba.

Az adatvédelmi incidenst az adatvédelmi kapcsolattartó jelentésében foglalt javaslat alapján az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

Az érintettek esetleges értesítéséről külön jegyzőkönyvet kell felvenni.

A tényfeltáró vizsgálat lefolytatására, a vétkes kötelezettségszegés megállapítására, a hátrányos jogkövetkezmények és más munkajogi intézkedések alkalmazására a munkaviszonyra vonatkozó szabályok (Mt., belső szabályzatok, utasítások) irányadóak. A szankcióknak arányban kell állniuk a kötelezettségszegés súlyával és az okozott kárral.

5.16. ADATVÉDELMI INCIDENSEK KEZELÉSE

Az a munkavállaló, aki a Szervezet által kezelt vagy feldolgozott személyes adatokkal kapcsolatban adatvédelmi incidenst, észlel, az köteles a közvetlen vezetője útján haladéktalanul az adatvédelmi kapcsolattartónak bejelenteni, megadva a nevét, telefonszámát és/vagy e-mail címét, a szervezeti egységét, az incidens tárgyát, valamint azt, hogy az incidens informatikai rendszert érint-e.

A bejelentő további olyan információkat is megadhat, amelyeket az incidens beazonosítása, megvizsgálása szempontjából lényegesnek ítél.

A kapcsolattartó a bejelentést követően tájékoztatja az ügyvezetőt az adatvédelmi incidens bekövetkezéséről, megadva a bejelentő nevét, telefonszámát és/vagy e-mail címét, szervezeti egységét, továbbá a bejelentett adatvédelmi incidens tárgyát, azt, hogy az incidens informatikai rendszert érint-e, valamint a további, a bejelentő által tudomására hozott egyéb információkat.

Amennyiben a Szervezet ellenőrzésre jogosult szervezeti egységei a feladataik ellátása során adatvédelmi incidenst észlelnek, a belső adatvédelmi felelőst értesítik.

A bejelentés megvizsgálása és az incidens kezelése

A belső adatvédelmi kapcsolattartó – informatikai rendszert érintő incidens esetén az érintett szervezeti egységgel együttműködve – a bejelentést megvizsgálja, a bejelentőtől adatszolgáltatást kér, amelyet a bejelentő köteles haladéktalanul, de legkésőbb 2 munkanapon belül teljesíteni.

Az adatszolgáltatásnak tartalmaznia kell:

- az incidens bekövetkezésének időpontját és helyét,
- az incidens leírását, körülményeit, hatásait,
- az incidens során kompromittálódott adatok körét, számosságát,
- a kompromittálódott adatokkal érintett személyek körét,
- az incidens elhárítása érdekében tett intézkedések leírását,
- a kár megelőzése, elhárítása, csökkentése érdekében tett intézkedések leírását.

Amennyiben az adatszolgáltatás alapján az adatvédelmi incidens vizsgálatot igényel, annak végrehajtására az adatvédelmi kapcsolattartó felkéri az adatvédelmi szakértőt. A belső adatvédelmi kapcsolattartó szaktanácsadóként közreműködik a vizsgálat lefolytatásában.

A javaslat alapján a megvalósítandó további intézkedésekről az adatok kezelését vagy feldolgozását végző szakterület vezetője, – informatikai rendszerben bekövetkezett adatvédelmi incidens esetében az adatgazda egyetértésével dönt.

Az adatvédelmi incidens elhárítása érdekében megvalósított egyes intézkedésekről az adatok kezelését vagy feldolgozását végző szakterület vezetője, kijelölt adatgazda esetében az adatgazda az adott intézkedések végrehajtását követő 2 munkanapon belül köteles az adatvédelmi kapcsolattartót tájékoztatni.

Az érintett személyt késedelem nélkül tájékoztatni kell, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személy jogaira és szabadságára nézve, annak érdekében, hogy megtehesse a szükséges óvintézkedéseket.

5.17. AZ INCIDENS NYILVÁNTARTÁSA

Az adatvédelmi incidensről az adatvédelmi kapcsolattartó nyilvántartást vezet.
A nyilvántartásba rögzíteni kell:

- az érintett személyes adatok körét,
- az adatvédelmi incidenssel érintettek körét és számát,
- az adatvédelmi incidens időpontját,
- az adatvédelmi incidens körülményeit, hatásait,
- az adatvédelmi incidens elhárítására megtett intézkedéseket,
- az adatkezelést előíró jogszabályban meghatározott egyéb adatokat.

A nyilvántartásban szereplő adatvédelmi incidensekre vonatkozó adatokat személyes adatokat érintő incidens esetében 5 évig, különleges adatokat érintő incidens esetében 20 évig köteles az adatvédelmi kapcsolattartó megőrizni.

Melléklet: incidenskezelési nyilvántartás

HATÁLYBA LÉPTETŐ RENDELKEZÉS

A szabályzat a 2018. november 21. napján lép hatályba és visszavonásig érvényes. A Szervezet képviseletre jogosult vezetője gondoskodik arról, hogy munkavállalóik a szabályzatban szabályozott – tevékenységükhöz kapcsolódó – ismereteket elsajátítsák.

A jelen szabályzatban foglalt előírásoknak történő megfelelés érdekében az adatkezelést végző szervezeti egységek vezetői gondoskodjanak az irányításuk alá tartozó adatkezelők felé az adatkezelések áttekintésére.

Kelt: Eger, 2018. november 21

…….
.
Dr. Horváth Ágnes
elnök

Mellékletek jegyzéke:

1. Adatvédelmi nyilvántartás (elektronikus)
2. Adattovábbítási nyilvántartás (elektronikus)
3. Incidenskezelési nyilvántartás