ADATVÉDELMI SZABÁLYZAT

MSZ EN ISO 9001:2015

MSZ ISO/IEC 27001:2014

MSZ EN ISO 14001:2015

IS-SZ-38
Verzió: 2.0
Oldalszám: 16

Jelen szabályzat hatályba lép

2021. július 27-én

elektronikusan aláírva
Dr. Karlócai Balázs
Vezérigazgató

Belső információ

Jelen dokumentált információ az IdomSoft Zrt. tulajdona.
A Vezérigazgató előzetes jóváhagyása nélkül üzleti vagy más célra nem használható fel.

1. Dokumentum kontroll

1.1. Módosítások jegyzéke

Kiadás	Dátum	Változtatás rövid leírása, módosítás elvégzője
1.0	2018.05.25.	Első kiadás az általános adatvédelmi rendelet hatályba lépésével egyidejűleg
1.1	2020.01.01	Adatvédelmi incidenskezelés módosítása
2.0	2021.07.27.	Adatvédelmi szabályzat átfogó módosítása, a szervezeti átalakulásnak és megváltozott szerepköröknek megfelelően.

Tartalom

2. Alkalmazás

Az IdomSoft Zrt. (a továbbiakban: Szervezet) a jogszabályi előírások és belső működési elvei alapján kiemelt figyelemmel kezeli az adatvédelmi előírásokat.
A Szervezet munkavállalóinak személyes adatai és a működéséhez kapcsolódó egyéb személyes adatok esetében adatkezelőnek minősül, míg az általa fejlesztett, illetve üzemeltetett elektronikus információs rendszerek esetében – jogszabályi kijelölés vagy az adatkezelővel kötött szerződés alapján – adatfeldolgozónak. A Szervezet tehát ezen a két területen – munkavállalók személyes adatainak kezelése és személyes adatok kezelése adatfeldolgozóként – különös figyelemmel jár el az adatvédelmi feladatok ellátása érdekében.

Az adatvédelem áthatja a Szervezet valamennyi működési mechanizmusát, így az adatvédelemre vonatkozó egyes területi részletszabályokat a Szervezet egyéb, belső szabályzói tartalmazzák. Jelen szabályzat ezen további szabályzókban követendő elveket és az adatvédelem biztosításának általános mechanizmusait rögzíti.

A folyamat szabályozása a minőségirányítási rendszerekről és követelményekről szóló MSZ EN ISO 9001:2015, az információbiztonság irányítási rendszerről szóló MSZ ISO/IEC 27001:2014, továbbá a környezetközpontú irányítási rendszerről szóló MSZ EN ISO 14001:2015 szabványok követelményrendszerein alapul.

Alkalmazási terület: a teljes Szervezet.

2.1. szabályzat személyi hatálya

A szabályzat személyi hatálya kiterjed a Szervezettel foglalkoztatási jogviszonyban álló személyekre, valamint a szabályzatban érintett folyamatok végrehajtásában közreműködő alvállalkozókra és a Szervezettel, a személyi adatokkal kapcsolatban bármilyen jogviszonyban álló további természetes és jogi személyekre.

2.2. A szabályzat tárgyi hatálya

A Szabályzat tárgyi hatálya kiterjed:

- a Szervezet bármely szervezeti egységénél és munkatársánál nyilvántartott valamennyi személyes adatra, a velük végzett adatkezelési műveletek teljes körére, keletkezésük, felhasználásuk, feldolgozásuk helyétől, valamint megjelenési formájuktól függetlenül;
- a személyes adatok kezelésének alapvető elveire a Szervezet működésére vonatkozóan;
- az adatvédelem biztosításának, fenntartásának módjára és eszközeire, annak felügyeletére.

2.3. A szabályzat időbeli hatálya

Jelen Szabályzat rendelkezéseit a hatálybalépését követően kell alkalmazni felmenő rendszerben

2.4. Az adatvédelemhez kapcsolódó folyamatok bemenete és kimenete

A folyamat bemenete: a Szervezet által kezelt személyes adatok jelenléte a működésben – ideértve a Szervezet működéséhez szükséges személyes adatokat és a Szervezet, mint adatfeldolgozó által kezelt személyes adatokat.

A folyamat kimente: Környezettudatos, ésszerű gazdálkodásnak, jogszabályi és egyéb követelményeknek megfelelő adatvédelmi folyamatok eredménye, kockázatokkal és lehetőségekkel kapcsolatos intézkedések kezelése, amellyel a Szervezet külső és belső forrásból biztosított folyamatai, termékei és szolgáltatásai megfelelnek a tulajdonosi, megrendelői és valamennyi érdekelt fél követelményeinek.

Az adatvédelmi folyamat eredménye lehet:

- az adatvédelem megfelelő szintje,
- adatvédelmi incidens kezelése,
- belső szabályozó, oktatás vagy egyéb intézkedés kiadása az adatvédelem szintjének emelése és az adatvédelmi tudatosság növelése érdekében.

2.5. Kockázatok és lehetőségek

Az adatvédelem kapcsán fel kell mérni a bizonytalanság pozitív és negatív hatásait a kockázatközpontúság jegyében és a folyamatos fejlesztés biztosítása érdekében. A kockázatból eredő pozitív eltérés lehetőséget teremthet jó eredmény eléréséhez, míg a negatív kockázatok hatásának kiküszöbölését folyamatosan tervezni kell.

Az adatvédelem kapcsán valamennyi részfolyamat esetében kiemelt figyelemmel kell lenni a számba vehető kockázatokra és azok hatásaira, kiemelten kezelve a következő kockázati tényezőket:

- az érintetteket kiemelten negatívan érintő adatvédelmi incidensek előfordulása,
- információbiztonság sértése a Szervezet adatfeldolgozói tevékenysége kapcsán,
- súlyos adatvédelmi incidens esetén a Szervezetre kiszabható bírság felmerülése.

A kockázatmenedzsment az ***IS-E-18 Kockázatok és lehetőségek*** című folyamatleírásban meghatározott kockázatok felmérésével és kezelésével kapcsolatos keretrendszer alapján folyik.

2.6. Kapcsolódó jogszabályok és szabályozók

Jogszabályok:

- *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) (a továbbiakban: GDPR);

- *az információs önrendelkezési jogról és az információszabadságról 2011. évi CXII. törvény (a továbbiakban: Infotv.);*
- *az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről;*
- *az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.*

Szabályozók:

- *IS-SZ-2 Szervezeti és működési szabályzat,*
- *IS-E-18 Kockázatok és lehetőségek eljárási utasítás,*
- *IS-SZ-31 Incidenskezelési szabályzat,*
- *IS-SZ-36 Folyamatszervezési szabályzat.*

3. Cél

Jelen Szabályzat célja, hogy biztosítsa a Szervezet által kezelt adatok vonatkozásában az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését – beleértve a Szervezet adatfeldolgozó tevékenységét –, megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát, valamint meghatározza a Szervezet által vezetett, adatvédelemmel kapcsolatos nyilvántartások kezelésének rendjét. Ennek megfelelően a szabályzat tartalmazza:

- az adatvédelem kapcsán a Szervezet tevékenységében követett alapelveket,
- az Adatvédelmi tisztviselő feladatait az adatvédelmi tevékenységek megfelelő szintjének biztosítása érdekében.

4. Értelmező rendelkezések

4.1. Fogalmak

Jelen Szabályzat alkalmazásában az alábbi fogalmakat, szerepköröket a következő értelemben kell alkalmazni:

- **Adatfeldolgozás:** az adatkezelő nevében végzett adatkezelési tevékenység.

- **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.

- **Adatkezelést végző szervezeti egység:** a Szervezet – az ***IS-SZ-2 Szervezeti és működési szabályzat***a alapján önállóan azonosítható – azon szervezeti egysége, amely a Szervezet adatkezelési (adatfeldolgozási) tevékenységét belső kijelölés alapján közvetlenül végzi.

- **Adatkezelő:** az a természetes vagy jogi személy, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza.

- **Adatvédelem:** személyes adatok jogszerű kezelése, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége.

- **Adatvédelmi tisztviselő:** a Vezérigazgató által a GDPR 37. cikke alapján kijelölt személy.

- **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.

- **Érintett:** élő természetes személy, akinek az adatát a Szervezet adatkezelői vagy adatfeldolgozói minőségben kezeli.

- **Személyes adat:** azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható.

4.2. Az adatvédelem és kapcsolódó folyamataiba bevont szervezeti egységek és személyek felelősségi rendje

Felelős szervezeti egység / személy	Felelősségi kör
Adatfeldolgozási szerződésben megjelölt kapcsolattartó	• Haladéktalanul értesíti az adatkezelőt, ha úgy véli, hogy annak valamely utasítása jogszabállyal ellentétes.
Adatkezelést végző szervezeti egység munkatársa	• Az *1. számú melléklet: Hatásvizsgálati lap minta* szerinti dokumentum felhasználásával hatásvizsgálatot végez arra vonatkozóan, hogy a

	tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik; • a hatásvizsgálat elvégzésekor kikéri az Adatvédelmi tisztviselő szakmai tanácsát; • ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése a korábban lefolytatott adatvédelmi hatásvizsgálatnak megfelelően történik-e; • kikéri az Adatvédelmi tisztviselő álláspontját az adatkezelési műveletek által jelentett kockázatok megváltozása esetén; • adatkezelési tevékenység nyilvántartása.
Adatkezelést végző szervezeti egység vezetője	• További adatfeldolgozó alkalmazása esetén felelős azért, hogy az adatfeldolgozási tevékenyég megkezdése előtt, illetve azalatt folyamatosan vizsgálja az adatfeldolgozó, a jelen szabályzóban rögzített elvárásoknak és a vonatkozó jogszabályi előírásoknak való, maradéktalanul megfelelését.
Adatvédelmi tisztviselő	• Az adatvédelemmel kapcsolatos feladatok megfelelőségének biztosítása a Vezérigazgató kijelölése alapján; • tájékoztat és szakmai tanácsot ad a Szervezet, továbbá az adatkezelést végző munkavállalók részére a GDPR, az Infotv, valamint egyéb vonatkozó jogszabályok szerinti kötelezettségeikkel kapcsolatban; • a tudomására jutott adatvédelmi incidens indokolatlan késedelem nélküli bejelentése a Nemzeti Adatvédelmi és Információszabadság Hatóság (továbbiakban: NAIH) felé – ha a Szervezet adatkezelőként jár el; • haladéktalanul tájékoztatja a Szervezet Vezérigazgatóját az adatvédelmi incidens tényéről, valamint a kivizsgálásról, kezelésre tett intézkedésekről; • nyilvántartja az adatvédelmi incidenseket; • javaslatokat tesz a Szervezet és a munkatársak számára az incidensmentes adatkezelési gyakorlat erősítése és a személyes adatok védelmének (adatbiztonsági) biztosítása érdekében; • tájékoztat és szakmai tanácsot ad a Szervezet adatkezelő vagy az adatfeldolgozó tevékenysége kapcsán felmerülő adatvédelmi kérdésekben; • ellenőrzi az adatvédelmi jogszabályoknak való megfelelést a Szervezet belső szabályalkotó tevékenységében; • igény esetén szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi annak elvégzését – szükség szerint részt vesz a vizsgálatban; • együttműködik és tartja a kapcsolatot a Nemzeti Adatvédelmi és Információszabadság Hatósággal; • adatkezeléssel kapcsolatos nyilvántartások kialakítása és vezetése; • adatvédelmi incidens észlelése vagy bejelentése esetén szóban és írásban is értesíti a Vezérigazgatót;

	• jelentést készít az adatvédelmi incidens kivizsgálását követően; • a vonatkozó jogszabályok figyelemmel kísérése, jogszabályváltozás esetén a megfelelőségre vonatkozó intézkedések kezdeményezése; • az adatvédelemmel kapcsolatos oktatási anyagok elkészítése, gondoskodás az oktatásokról.
A Szervezet minden munkatársa	• Adatvédelmi alapelvek ismerete és az adatvédelmi rendelkezések betartása; • amennyiben bevonásra kerül, a szükséges adatvédelmi hatástanulmányok elkészítése; • adatvédelmi incidensek haladéktalan jelentése az adatvédelmi tisztviselőnek; • adatszolgáltatás a szükséges, adatvédelemmel kapcsolatos nyilvántartások vezetéséhez az Adatvédelmi tisztviselő számára; • adatvédelmi incidensről az adatkezelő haladéktalan tájékoztatása – a Szervezet adatfeldolgozói minőségében –, illetve az érintett haladéktalan tájékoztatása – a Szervezet adatkezelői minőségében; • adatvédelmi oktatásokon való részvétel.
Folyamatszervezési csapat	• Az adatvédelmi elvek képviselete a folyamatszervezési tevékenység során; • az Adatvédelmi tisztviselő bevonása a folyamatok kialakításába, ellenőrzésébe.
Vezérigazgató	• Adatvédelmi tisztviselő munkatárs kijelölése vagy megbízási jogviszonyban való foglalkoztatása; • az adatvédelem megfelelő szintjének biztosítása a Szervezet tevékenységében; • Adatvédelmi tisztviselő munkájának elvégzéséhez szükséges feltételek biztosítása.

5. A személyes adatok kezelésére irányadó alapelvek

A Szervezet minden munkatársa, aki bármilyen okból adatkezelési tevékenységet végez, ezen tevékenysége során az alábbi elveknek megfelelően kell eljárnia:

- **Jogszerűség, tisztességes eljárás és átláthatóság:** a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.
- **Célhoz kötöttség:** a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, adatkezelésre a célokkal össze nem egyeztethető módon nem kerülhet sor.
- **Adattakarékosság:** az adatkezelés céljai megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk.

- **Pontosság:** a kezelt vagy feldolgozott személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.
- **Korlátozott tárolhatóság:** a személyes adatok tárolására olyan formában kerülhet sor, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé.
- **Integritás és bizalmas jelleg:** a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

6. A Szervezet, mint adatkezelő

a. A Szervezet az *5. A személyes adatok kezelésére irányadó alapelvek* fejezetben meghatározott alapelvekre tekintettel végez adatkezelést és jár el minden olyan folyamatban, amely személyes adatok kezelését érinti. A Szervezet közös adatkezelés során is köteles megfelelni a jogszabályban és a jelen szabályzóban leírtaknak.

b. A Szervezet az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázatok figyelembevételével megfelelő technikai és szervezési intézkedéseket (pl. hozzáférési jogosultságok kiosztása, nyilvántartáshoz való hozzáférés módjának kialakítása, stb.) hajt végre annak biztosítása és bizonyítása céljából, hogy a személyes adatok kezelése a Szervezetnél a GDPR előírásaival összhangban történik.

c. A jelen fejezet b. pontja szerinti intézkedéseket a Szervezet évente, külső vagy belső vizsgálat megállapításaira és javaslataira tekintettel, továbbá minden adatkezelési incidenst követően felülvizsgálja és szükség esetén naprakésszé teszi.

d. A Szervezet a jelen fejezet b. pontja szerinti intézkedések részeként az adatkezelési tevékenységgel arányos és megfelelő belső adatvédelmi szabályokat alkot.

e. A Szervezet az adatkezelést érintő kockázatok elemzésekor figyelemmel van a tudomány és a technológia állására, a megvalósítás költségeire, az adatkezelés jellegére, hatókörére, körülményeire és céljaira, valamint az érintettek jogaira.

f. A Szervezet biztosítja, hogy a személyes adatok kezelésére feljogosított munkavállalói, vagy egyéb jogviszonyban foglalkoztatott személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak.

g. A Szervezet biztosítja, hogy a GDPR, az Infotv. és egyéb vonatkozó jogszabályok, továbbá jelen szabályozó vonatkozó rendelkezéseit illetően a Szervezet munkavállalói naprakész ismeretekkel rendelkezzenek. Ennek érdekében belépéskor és a munkaviszony ideje alatt évi rendszerességgel, a megfelelő ismeretek megszerzésére irányuló oktatást biztosít, melynek megtartásáért az Adatvédelmi tisztviselő felelős.

h. A Szervezet munkavállalója köteles az általa észlelt adatkezelési incidenst haladéktalanul bejelenteni az Adatvédelmi tisztviselőnek és saját közvetlen felettesének.

6.1. A Szervezet által lefolytatott adatvédelmi hatásvizsgálat

a. Az adatkezelést végző szervezeti egység az **adatkezelést megelőzően** az *1. számú melléklet: Hatásvizsgálati lap minta* szerinti dokumentum felhasználásával hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.

b. A Szervezet adatkezelését végző szervezeti egységeinek kizárólag eredeti adatkezelői minőségükben kell adatvédelmi hatásvizsgálatot végezniük, minden más esetben az adatfeldolgozó köteles a hatásvizsgálatot végezni, de a Szervezet ebben az esetben segítséget nyújthat.

c. Egyetlen hatásvizsgálat keretei között is értékelhetőek az egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek.

d. A hatásvizsgálat elvégzésekor az adatkezelést végző szervezeti egység köteles kikérni az Adatvédelmi tisztviselő szakmai tanácsát.

e. Adatvédelmi hatásvizsgálatot az alábbi esetekben kell különösen elvégezni:
- ha új technológia alkalmazásával kerül sor az adatkezelésre, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, amennyiben valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve.
- 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;
- a GDPR 9. cikk (1) bekezdésében említett személyes adatok különleges kategóriái, vagy a GDPR 10. cikkében említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése;
- nyilvános helyek nagymértékű, módszeres megfigyelése.

f. A hatásvizsgálat legalább kiterjed:
- a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben a Szervezet által érvényesíteni kívánt jogos érdeket;
- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
- a jelen fejezet a. pontjában említett, az érintett jogait és szabadságait érintő kockázatok vizsgálatára;
- a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és a GDPR-ral való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

g. Jogszabály eltérő rendelkezés hiányában az adatvédelmi hatásvizsgálatot nem kell lefolytatni, amennyiben az adatkezelés jogalapját jogszabály határozza meg és a szóban forgó jogszabály elfogadásakor egy általános hatásvizsgálat részeként már végeztek adatvédelmi hatásvizsgálatot is.

h. A Szervezet adatkezelést végző szervezeti egységei szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése a korábban lefolytatott adatvédelmi hatásvizsgálatnak megfelelően történik-e.

i. Az adatkezelést végző szervezeti egység munkatársai kötelesek kikérni az Adatvédelmi tisztviselő álláspontját az adatkezelési műveletek által jelentett kockázatok jelen fejezet g. pontja szerinti megváltozása esetén.

7. A Szervezet, mint adatfeldolgozó

a. A Szervezet az adatkezelő nevében, a vele papíralapú vagy elektronikus formában kötött adatfeldolgozási szerződés alapján végez adatkezelési tevékenységet. Az adatfeldolgozási szerződésben meg kell határozni:
- az adatkezelés tárgyát, időtartamát, jellegét és célját;
- a személyes adatok típusát;
- az érintettek kategóriáit;
- az adatkezelő kötelezettségeit és jogait;
- az adatkezelő és az adatfeldolgozó részéről a szervezetek képviselőit, operatív kapcsolattartóit és adatvédelmi tisztviselőit, valamint ezek elérhetőségeit.

b. A Szervezet adatfeldolgozói minőségében kizárólag az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása alapján vehet igénybe további adatfeldolgozót.

c. A Szervezet (további) adatfeldolgozót kizárólag abban az esetben alkalmazhat, ha az adatfeldolgozó a jelen szabályzóban rögzített elvárásoknak és a vonatkozó jogszabályi előírásoknak maradéktalanul megfelel. Ennek előzetes és az adatfeldolgozási tevékenység ideje alatt megvalósuló folyamatos vizsgálata az adatkezelést végző szervezeti egység vezetőjének felelőssége.

d. Az adatfeldolgozási szerződésben megjelölt kapcsolattartó haladéktalanul köteles tájékoztatni az adatkezelőt, ha úgy véli, hogy annak valamely utasítása jogszabállyal ellentétes.

e. A 6. *A Szervezet, mint adatkezelő* fejezet rendelkezéseit értelemszerűen kell alkalmazni abban az esetben is, ha a Szervezet adatfeldolgozói minőségben jár el.

f. Az adatfeldolgozói minőségben észlelt adatvédelmi incidens kezelésének rendjét – ideértve különösen az azzal kapcsolatos kommunikációt és információmegosztást – a GDPR, az Infotv., és jelen szabályzó mellett az adatkezelővel kötött adatfeldolgozási szerződés határozza meg.

8. A Szervezet által végzett adatkezelési tevékenység nyilvántartása

A Szervezet adatkezelés végző szervezeti egységeinek erre kijelölt munkatársai nyilvántartást vezetnek az alábbi adatokkal:

a. a szervezet neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, a szervezet képviselőjének és az Adatvédelmi tisztviselőnek a neve és elérhetősége;

b. az adatkezelés céljai;

c. az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;

d. olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;

e. adott esetben a személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk, beleértve a harmadik ország vagy a nemzetközi szervezet azonosítását, valamint a GDPR 49. cikk (1) bekezdésének második albekezdés szerinti továbbítás esetében a megfelelő garanciák leírása;

f. ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidők;

g. a 6. *A Szervezet, mint adatkezelő* fejezet b. pontja szerinti technikai és szervezési intézkedések általános leírása;

h. a jogszabályi megfelelés érdekében törölt személyes adatok leírása, valamint a *2. számú melléklet: Jegyzőkönyv a kezelt személyes adatok törléséről minta* szerinti jegyzőkönyv a személyes adatok törléséről.

9. Az Adatvédelmi tisztviselő

a. A Szervezet munkavállalói közül szakmai rátermettsége, különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete alapján a Vezérigazgató Adatvédelmi tisztviselőt jelöl ki.

b. Az Adatvédelmi tisztviselő más feladatokat is elláthat, de feladatellátásával összefüggésben összeférhetetlenség nem merülhet fel.

c. A Vezérigazgató dönthet úgy, hogy az Adatvédelmi tisztviselő a *9.1 Adatvédelmi tisztviselő feladatai* fejezet szerinti feladatokat szolgáltatási szerződés keretében látja el, amennyiben a Szervezet munkavállalói közül senki nem felel meg a jelen fejezet a. pontjában meghatározott feltételeknek. A szolgáltatási szerződés megkötésekor a GDPR és az Infotv. mellett jelen szabályozó rendelkezéseire is figyelemmel kell lenni.

d. Az Adatvédelmi tisztviselő nevét és elérhetőségét (adatvedelem@idomsoft.hu) a NAIH) felé az Adatvédelmi tisztviselő, a Szervezet honlapján pedig a Kommunikációs csapat munkatársa teszi közzé.

e. Az Adatvédelmi tisztviselőt a személyes adatok védelmével összefüggő összes ügybe megfelelő módon és időben be kell vonni.

f. A Szervezet támogatja az Adatvédelmi tisztviselőt a *9.1 Adatvédelmi tisztviselő feladatai* fejezet szerinti feladatai ellátásában azáltal, hogy biztosítja számára azokat az forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az Adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek.

g. Az Adatvédelmi tisztviselő szervezeti hierarchiában elfoglalt helye biztosítja, hogy a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el. A Szervezet az Adatvédelmi tisztviselőt a jogszabályok és a vonatkozó szerződések szerinti feladatai ellátásával összefüggésben nem bocsáthatja el és szankcióval nem sújthatja.

h. Az Adatvédelmi tisztviselőt nem terheli személyes felelősség az adatvédelmi követelmények be nem tartásáért.

i. Az Adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban titoktartási kötelezettség köti.

j. Az Adatvédelmi tisztviselő közvetlenül a Vezérigazgató alárendeltségében látja el a *9.1 Adatvédelmi tisztviselő feladatai* fejezet szerinti feladatait.

9.1. Adatvédelmi tisztviselő feladatai

Az Adatvédelmi tisztviselő az adatkezelési műveletekhez fűződő kockázatok megfelelő figyelembevételével, az adatkezelés jellegére, hatókörére, körülményeire és céljaira is tekintettel az alábbi feladatokat látja el a Szervezetnél:

a. tájékoztat és szakmai tanácsot ad a Szervezet, továbbá az adatkezelést végző munkavállalók részére a GDPR, az Infotv., valamint egyéb vonatkozó jogszabályok szerinti kötelezettségeikkel kapcsolatban;

b. ellátja a 6. *A Szervezet, mint adatkezelő* fejezet g. pontja szerinti oktatást, amelynek során törekedni kell az elektronikus felületen történő oktatási-számonkérési forma (új belépőknek általános adatvédelmi, állományban lévő munkatársaknak ismétlő – általános vagy tematikus – oktatás) alkalmazására;

c. ellenőrzi a GDPR, az Infotv., valamint egyéb vonatkozó jogszabályok előírásainak, továbbá a Szervezet személyes adatok védelmével kapcsolatos belső szabályozóinak való megfelelést, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben résztvevő munkatársak tudatosságnövelését és képzését, valamint a kapcsolódó auditokat is;

d. elvégzi a 6. *A Szervezet, mint adatkezelő* fejezet c. pontja szerinti feladatokat, együttműködve a Szervezet megfelelési tanácsadóival és a belső ellenőrökkel;

e. előkészíti, valamint elvégzi a 6. *A Szervezet, mint adatkezelő* fejezet d. pontja szerinti belső szabályozók rendszeres és szükségszerinti felülvizsgálatát, együttműködve a Szervezet megfelelési tanácsadóival, a belső ellenőrökkel, valamint a Folyamatszervezési csapattal;

f. kérésre szakmai tanácsot ad a *6.1. A Szervezet által lefolytatott adatvédelmi hatásvizsgálat* fejezet szerinti adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálatnak a GDPR 35. cikke alapján történő elvégzését;

g. a *9. Az Adatvédelmi tisztviselő* fejezet e. pontjára tekintettel részt vesz a személyes adatok kezelésére irányuló fejlesztések koncepcionális és stratégiai előkészítésében, támogatja a fejlesztési szakterület normakonformitását;

h. a *9. Az Adatvédelmi tisztviselő* fejezet e. pontja alapján bármely tevékenység esetében ellenőrizheti a GDPR szerinti megfelelőséget; az adatkezelési vagy adatfeldolgozási tevékenységek kapcsán információt gyűjthet a folyamatok működéséről, amelyeket elemez és összeveti a GDPR előírásaival;

i. adatvédelmi incidens észlelése vagy bejelentése esetén szóban, illetve írásban is tájékoztatja a Szervezet Vezérigazgatóját. A tájékoztatást követően az adatvédelmi incidens kivizsgálását és kezelésére tett intézkedéseket az Adatvédelmi tisztviselő saját hatáskörben végzi, szükség szerint a Vezérigazgató folyamatos tájékoztatása mellett.

j. észlelés vagy bejelentés alapján haladéktalanul, a lehető legrövidebb idő alatt, teljeskörűen, figyelemmel az *IS-SZ-31 Incidenskezelési szabályzat* rendelkezéseire, az alábbi szempontok alapján kivizsgálja az adatvédelmi incidenst:

   - bejelentésre induló vizsgálat esetében rögzíti a bejelentő azonosításához szükséges adatokat, az incidens bejelentő általi észlelésének idejét és körülményeit, valamint a bejelentés idejét;
   - észlelése alapján indított vizsgálat esetében rögzíti az észlelés idejét és körülményeit;
   - a vizsgálat ideje alatt lehetőség szerint javaslatot tesz az incidens által okozott károk enyhítésére, közvetlen és közvetett hatásainak korlátozására;
   - rögzíti az adatvédelmi incidens rövid leírását, a vizsgálat ideje alatt haladéktalanul megtett intézkedéseket, a vizsgálat lezárásának idejét és a vizsgálatot lefolytató azonosításához szükséges adatokat;
   - a vizsgálat során feltárja és rögzíti az adatvédelmi incidens körülményeit és előfordulásának okát;

k. az adatvédelmi incidens kivizsgálását (lezárását) követően a *3. számú melléklet: Adatvédelmi incidens vizsgálati jelentés minta* szerint jelentést készít, amelyben a fenti adatok és információk mellett az adatvédelmi incidenssel kapcsolatos következtetéseit és javaslatait is megfogalmazza;

l. a jelen fejezet k. pontban meghatározott jelentést haladéktalanul és közvetlenül felterjeszti a Vezérigazgató számára, egyúttal tájékoztatásul megküldi a Belső ellenőrzési divízió és a Megfelelési divízió részére;

m. együttműködik, illetve az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a NAIH irányába, valamint bármely egyéb kérdésben konzultációt folytat vele.

10. Mellékletek

1. számú melléklet: Hatásvizsgálati lap minta
2. számú melléklet: Jegyzőkönyv a kezelt személyes adatok törléséről minta
3. számú melléklet: Adatvédelmi incidens vizsgálati jelentés minta
4. számú melléklet: Folyamathoz kapcsolódó mérési pontok