KOVÁCS ÜGYVÉDI IRODA ADATVÉDELMI, ADATKEZELÉSI ÉS BEJELENTŐVÉDELMI SZABÁLYZATA

Hatályos 2023. július 24-től

1. Preambulum

A Kovács Ügyvédi Iroda – a továbbiakban: „Iroda" vagy „Adatkezelő" vagy „Vállalkozás" - a gazdasági tevékenységével összefüggő valamennyi adatkezelése, adatfeldolgozása során a jelen Adatvédelmi, Adatkezelési Bejelentővédelmi Szabályzat (továbbiakban: „Szabályzat") szerint jár el. Az Iroda főtevékenységként jogi illetve kiegészítőként ingatlanközvetítői szolgáltatást nyújt. Ennek során kiemelten fontosnak tartja az érintett személyek személyes adatainak védelmét, az információs önrendelkezési joguk és magánszférájuk tiszteletben tartását továbbá, hogy az Irodánál zajló adatkezelés, adatfeldolgozás során biztosítsa az adatvédelem alkotmányos elveinek érvényre juttatását, valamint az adatbiztonság, így különösen az Európai Parlament és Tanács 2016/679 rendeletének – „GDPR" – és a panaszokról és a közérdekű bejelentésekről szóló 2013. évi CLXV. törvényben foglalt rendelkezéseinek való megfelelést és visszaélés-bejelentési rendszert is üzemeltet

Iroda az adatkezelés során a személyes adatokat bizalmasan kezeli, a biztonságos adatkezelést elősegítő minden intézkedést megtesz, amelynek során a személyes adatok védelme körében kiemelt hangsúlyt fektet a legmodernebb informatikai megoldások alkalmazására.

2. Szabályzat hatálya – alkalmazandó normák

Jelen Szabályzat hatálya kiterjed az Iroda által az Európai Unió területén folytatott valamennyi adatkezelésre, adatfeldolgozásra, adattovábbításra, illetve az ezekkel kapcsolatos adatvédelmi tevékenységre, továbbá az Iroda és más adatkezelők között lezajló személyes adatokat érintő adattovábbításra, valamint kommunikációra. A Szabályzat hatálya a GDPR hatály alá nem, tartozó jogi személyek adataival kapcsolatos adatkezelésre, adatfeldolgozásra nem terjed ki.

Jelen szabályzat a hatályos Európai Uniós és magyar jogszabályok, a vonatkozó ajánlások és az Iroda belső szabályzatival együttesen értelmezendő és kezelendő.

A Szabályzat jogszabályi alapját különösen, de nem kizárólagosan az alábbi jogszabályok jelentik: a) Magyarország Alaptörvénye (továbbiakban: Alaptörvény) b) Polgári Törvénykönyvről szóló 2013. évi V. törvény (továbbiakban: Ptk.) c) az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Info tv.), d) Munka törvénykönyvéről szóló 2012. évi I. törvény (továbbiakban: Mt.) fogyasztóvédelemről szóló 1997. évi CLV. törvény (továbbiakban Fgy tv.) e) Európai Parlament és Tanács 2016/679 számú rendeletek (továbbiakban: GDPR); f) az ügyvédi tevékenységről szóló 2017. évi LXXVIII. törvény g) a panaszokról és a közérdekű bejelentésekről szóló 2013. évi CLXV. törvény

Jelen Szabályzat személyi hatálya kiterjed az Irodával szerződéses vagy egyéb jogviszonyban álló, adatkezelést illetve feldolgozást végző valamennyi személyre.

Jelen Szabályzat időbeli hatálya a hatálybalépésétől (lásd első oldal) visszavonásig áll fenn.

Jelen Szabályzatban foglaltak szakszerű végrehajtásáról a vállalkozás irodavezetőjének kell gondoskodnia.

3. Értelmező rendelkezések

Jelen Szabályzat során a 2. pontban írt normák alkalmazása mellett az Iroda elsődlegesen alkalmazza GDPR szerinti alábbi fogalom-meghatározásokat és érti alatta az ott, alábbiakban megjelölt tartalmat:

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

„*adatkezelés*": a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés;

„*az adatkezelés korlátozása*": a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából;

„*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;

„*álnevesítés*": a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni;

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

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

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

„*címzett*": az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e. Azon közhatalmi szervek, amelyek egy 2016.5.4. HU Az Európai Unió Hivatalos Lapja L

119/33 egyedi vizsgálat keretében az uniós vagy a tagállami joggal összhangban férhetnek hozzá személyes adatokhoz, nem minősülnek címzettnek; az említett adatok e közhatalmi szervek általi kezelése meg kell, hogy feleljen az adatkezelés céljainak megfelelően az alkalmazandó adatvédelmi szabályoknak;

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

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

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

„*genetikai adat*": egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered;

„*biometrikus adat*": egy természetes személy testi, fiziológiai vagy viselkedési jellemzőire vonatkozó minden olyan sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat;

„*egészségügyi adat*": egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;

„*tevékenységi központ*": a) az egynél több tagállamban tevékenységi hellyel rendelkező adatkezelő esetében az Unión belüli központi ügyvitelének helye, ha azonban a személyes adatok kezelésének céljaira és eszközeire vonatkozó döntéseket az adatkezelő egy Unión belüli másik tevékenységi helyén hozzák, és az utóbbi tevékenységi hely rendelkezik hatáskörrel az említett döntések végrehajtatására, az említett döntéseket meghozó tevékenységi helyet kell tevékenységi központnak tekinteni; b) az egynél több tagállamban tevékenységi hellyel rendelkező adatfeldolgozó esetében az Unión belüli központi ügyvitelének helye, vagy ha az adatfeldolgozó az Unióban nem rendelkezik központi ügyviteli hellyel, akkor az adatfeldolgozónak az az Unión belüli tevékenységi helye, ahol az adatfeldolgozó tevékenységi helyén folytatott tevékenységekkel összefüggésben végzett fő adatkezelési tevékenységek zajlanak, amennyiben az adatfeldolgozóra e rendelet szerint meghatározott kötelezettségek vonatkoznak;

„*képviselő*": az az Unióban tevékenységi hellyel, illetve lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által a 27. cikk alapján írásban megjelölt természetes vagy jogi személy,

aki, illetve amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra az e rendelet értelmében háruló kötelezettségek vonatkozásában;

„*vállalkozás*”: gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő Irodaokat és egyesületeket is;

„*vállalkozáscsoport*”: az ellenőrző vállalkozás és az általa ellenőrzött vállalkozások;

„*kötelező erejű vállalati szabályok*”: a személyes adatok védelmére vonatkozó szabályzat, amelyet az Unió valamely tagállamának területén tevékenységi hellyel rendelkező adatkezelő vagy adatfeldolgozó egy vagy több harmadik országban a személyes adatoknak az ugyanazon vállalkozáscsoporton vagy közös gazdasági tevékenységet folytató vállalkozások ugyanazon csoportján belüli adatkezelő vagy adatfeldolgozó részéről történő továbbítása vagy ilyen továbbítások sorozata tekintetében követ;

„*felügyeleti hatóság*”: egy tagállam által az 51. cikknek megfelelően létrehozott független közhatalmi szerv; L 119/34 HU Az Európai Unió Hivatalos Lapja 2016.5.4.

„*érintett felügyeleti hatóság*”: az a felügyeleti hatóság, amelyet a személyes adatok kezelése a következő okok valamelyike alapján érint: a) az adatkezelő vagy az adatfeldolgozó az említett felügyeleti hatóság tagállamának területén rendelkezik tevékenységi hellyel; b) az adatkezelés jelentős mértékben érinti vagy valószínűsíthetően jelentős mértékben érinti a felügyeleti hatóság tagállamában lakóhellyel rendelkező érintetteket; vagy c) panaszt nyújtottak be az említett felügyeleti hatósághoz;

„*személyes adatok határokon átnyúló adatkezelése*”: a) 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 b) 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;

„*releváns és megalapozott kifogás*”: a döntéstervezettel szemben benyújtott, azzal kapcsolatos kifogás, hogy ezt a rendeletet megsértették-e, illetve hogy az adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a rendelettel; a kifogásban egyértelműen be kell mutatni a döntéstervezet által az érintettek alapvető jogaira és szabadságaira, valamint adott esetben a személyes adatok Unión belüli szabad áramlására jelentett kockázatok jelentőségét;

„*az információs társadalommal összefüggő szolgáltatás*”: az (EU) 2015/1535 európai parlamenti és tanácsi irányelv (1) 1. cikke (1) bekezdésének b) pontja értelmében vett szolgáltatás;

„*nemzetközi szervezet*”: a nemzetközi közjog hatálya alá tartozó szervezet vagy annak alárendelt szervei, vagy olyan egyéb szerv, amelyet két vagy több ország közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre.

4. Adatkezelő adatai

Cégnév: Kovács Ügyvédi Iroda
A szabályzat tartalmáért és betartásáért felelős személyek: Dr. Kovács Csaba irodavezető kovacs@cklawyers.hu (cklawyers.hu)
Székhely: 2484 Gárdony, Balatoni út 55.
Adószám: 18180262-2-07
Nyilvántartó szerv: Fejér Megyei Ügyvédi Kamara

5. Alapelvek

A személyes adatok kezelése során az Iroda az alábbi alapelvek figyelembevételével jár el:

(„**jogszerűség, tisztességes eljárás és átláthatóság**") - Személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni;

(„**célhoz kötöttség**") – Személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; a GDPR 9. cikk (1) bekezdésének megfelelően nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés

(„**adattakarékosság**") - az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk;

(„**pontosság**") - pontosnak és szükség esetén naprakésznek kell lenniük; minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék;

(„**korlátozott tárolhatóság**") – személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a GDPR 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az e rendeletben az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel;

(„**integritás és bizalmas jelleg**") - 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.

(„**elszámoltathatóság**") - Az adatkezelő felelős a fentieknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.

6. Általános adatkezelési szabályok

Az Iroda összesítette a nála kezelt adatok körét („Adatvagyon"). Az Adatvagyon kapcsán megállapítható, hogy ahhoz az EU-n kívül nem férhetnek hozzá, megváltoztatásuk, törlésük és továbbításuk az Iroda vezetősége által van kontrollálva.

Az Iroda nem végez sem hírlevél, sem más internetes kereső, adatgyűjtő szolgáltatást és nincs közösségi weboldalon bejegyzett fiókja sem. Az Irodánál tiltott a személyes adattartalom létesítése és továbbítása a cég elektronikus (e-mail illetve külső internetes) felületein illetve manuális (papír alapú, postai) rendszerén keresztül. Amennyiben mégis személyes adat kerül a rendszerbe, úgy az haladéktalanul anonimizálásra illetve törlésre kerül.

A személyes adatok jogszerű kezelését az Iroda kiemelten kezeli és jelen Szabályzat szerint az EU szabályozással összhangban maradéktalanul biztosítja. A személyes adatok kezelése akkor jogszerű, ha az alábbiak valamelyike teljesül:

a. az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;

b. az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;

c. az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;

d. az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;

e. az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;

f. az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

A fentiek értelmében az adatkezelés jogszerűnek minősül, ha arra valamely szerződés vagy szerződéskötési szándék keretében van szükség. Ha az adatkezelésre az adatkezelőre vonatkozó jogi kötelezettség teljesítése keretében kerül sor, vagy ha az közérdekű feladat végrehajtásához, illetve közhatalmi jogosítvány gyakorlásához szükséges, az adatkezelésnek az uniós jogban vagy valamely tagállam jogában foglalt jogalappal kell rendelkeznie. Az adatkezelést jogszerűnek kell tekinteni akkor, amikor az az érintett életének vagy más fent említett természetes személy érdekeinek védelmében történik. Más természetes személy létfontosságú érdekeire hivatkozással személyes adatkezelésre elvben csak akkor kerülhet sor, ha a szóban forgó adatkezelés egyéb jogalapon nem végezhető.

A **személyes adatkezelés alapjául szolgáló alapvető és általános jogalap az Irodánál a szerződéses kötelezettségek teljesítése és az ügyvédi tevékenységre vonatkozó szabályok által előírt felhatalmazás, ügyvédi titok és érdekvédelem.**

Az adatkezelő – ideértve azt az adatkezelőt is, akivel a személyes adatokat közölhetik – vagy valamely harmadik fél jogos érdeke jogalapot teremthet az adatkezelésre. Az ilyen jogos érdekről lehet szó például 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.

Az érintett adatkezelő jogos érdekének minősül a közhatalmi szervek, számítástechnikai vészhelyzetekre reagáló egység, hálózatbiztonsági incidenskezelő egységek, elektronikus hírközlési hálózatok üzemeltetői és szolgáltatások nyújtói, valamint biztonságtechnológiai szolgáltatók által végrehajtott olyan mértékű személyes adatkezelés, amely a hálózati és informatikai biztonság garantálásához feltétlenül szükséges és arányos.

A személyes adatoknak a gyűjtésük eredeti céljától eltérő egyéb célból történő kezelése csak akkor megengedett, ha az adatkezelés összeegyeztethető az adatkezelés eredeti céljaival.

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

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.

A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése tilos, kivéve, ha az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez.

A büntetőjogi felelősség megállapítására vonatkozó határozatokra és a bűncselekményekre, illetve a kapcsolódó biztonsági intézkedésekre vonatkozó személyes adatok kezelésére kizárólag abban az esetben kerülhet sor, ha az közhatalmi szerv adatkezeléséhez tartozóan történik.

Ha azok a célok, amelyekből az adatkezelő a személyes adatokat kezeli, nem vagy már nem teszik szükségessé az érintettnek az adatkezelő általi azonosítását, az adatkezelő nem köteles kiegészítő információkat megőrizni.

Ha az adatkezelő bizonyítani tudja, hogy nincs abban a helyzetben, hogy azonosítsa az érintettet, erről lehetőség szerint őt megfelelő módon tájékoztatja.

A tisztességes és átlátható adatkezelés elve megköveteli, hogy az érintett tájékoztatást kapjon az adatkezelés tényéről és céljairól.

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.

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, minden évben május 1-től 31-éig tart.

Az adatkezelő kötelessége, hogy megfelelő és hatékony intézkedéseket hajtson végre, valamint hogy képes legyen igazolni azt, hogy az adatkezelési tevékenységek a hatályos jogszabályoknak megfelelnek.

Ezt a szabályozást az adatkezelés jellegének, hatókörének, körülményeinek és céljainak, valamint a természetes személyek jogait és szabadságait érintő kockázatnak a figyelembevételével kell meghozni.

Az adatkezelő 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 hajt végre. E szabályzat alapján az egyéb belső szabályzatokat felülvizsgálja és szükség esetén naprakésszé teszi.

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.

Amennyiben az Iroda olyan adatkezelést kíván végezni, amely ebben a szabályzatban nem szerepel, előzetesen ezen belső szabályzatát kell megfelelően kiegészíteni, illetve az új adatkezelési célnak megfelelő részletszabályokat hozzákapcsolni.

7. Speciális adatkezelési részletszabályok kezelt adattípusonként

A) TÖRVÉNYI FELHATALMAZÁS ALAPJÁN TÖRTÉNŐ ADATKEZELÉSEK

Ezen adatok kezelése az előírt rendben a jogszabályi keretek között a hatóságok illetve a hatóságok felé eljáró más adatfeldolgozók felé történik a jogszabályi kötelezettségeknek történő megfelelés céljából.

Az adatkezelés során kizárólag olyan adatfeldolgozók kerülnek bevonásra, akik szerződésben vállalják GDPR szabályok megfelelőségét és az adatkezelési szabályzatot elfogadják.

Ezen adatkezelési kör az alábbi elsődleges adattartalmakra terjed ki: *Magánszemély ügyfelek számviteli jogszabályok által meghatározott adatai*: Jogalap és adatkezelési kör a hatályos számviteli jogszabályok által meghatározott.

B) SZERZŐDÉSES ADATKEZELÉS

Az Iroda jogi tevékenysége keretében az ügyvédi tevékenységről szóló 2017. évi LXXVIII. törvény („törvény") rendelkezéseinek megfelelően jár el és adatot kizárólag ennek megfelelően az ügyfél érdekében az adott szerződésben vállalt feladat szerint kezel.

Ügyvédi titoknak minősül minden olyan tény, információ és adat, amelyről az ügyvédi tevékenység gyakorlója e tevékenysége gyakorlása során szerzett tudomást. Ha e törvény eltérően nem rendelkezik, az ügyvédi tevékenység gyakorlója köteles az ügyvédi titkot megtartani. E titoktartási kötelezettség kiterjed az ügyvédi titkot tartalmazó iratra vagy más adathordozóra is.

Az ügyvédi tevékenység gyakorlója az ügyvédi titokról való tanúvallomás tételét és adatszolgáltatás teljesítését bármely hatósági és bírósági eljárásban köteles megtagadni, kivéve, ha a titoktartási kötelezettsége alól felmentést kapott az ügyvédi titokról rendelkezni jogosulttól, azzal, hogy - a törvény 12. § (4) bekezdésében meghatározott kivétellel - a védőként megismert ügyvédi titokról való tanúvallomás tételre és adatszolgáltatás teljesítésére felmentés érvényesen nem adható.

Az ügyvédi tevékenység gyakorlójának titoktartási kötelezettsége független az ügyvédi tevékenység folytatására létrejött jogviszony fennállásától, és az ügyvédi tevékenység gyakorlásának a befejezése vagy a jogviszony megszűnése után is határidő nélkül fennmarad.

Ha a törvény eltérően nem rendelkezik, az ügyvédi tevékenység gyakorlóját nem terheli titoktartási kötelezettség azon ügyfél irányába, akinek a javára végzett ügyvédi tevékenység keretében az ügyvédi titok a tudomására jutott. Ha az ügyvédi titok tárgya másik ügyvédi tevékenységet gyakorló személytől kapott információ, ezt az ügyvédi tevékenység gyakorlója az ügyben érintett saját ügyfele számára akkor nem tárhatja fel, ha az információt átadó ezt kifejezetten megtiltotta. A kamarai jogtanácsost és a jogi előadót nem terheli titoktartási kötelezettség azon munkáltatója irányába sem, amellyel fennálló munkaviszonya keretében az ügyvédi titok a tudomására jutott, továbbá e munkáltatója, illetve az ügyfele által meghatározott személyek irányába sem.

Az ügyvédi iroda titoktartási kötelezettsége az iroda tagjaira is kiterjed, azonban a tagokat egymással szemben nem terheli titoktartási kötelezettség. Ha törvény az ugyanazon ügyfél vagy egymással ellenérdekű ügyfelek számára együttesen végezhető tevékenységeket korlátozza, de ügyvédi iroda megbízása esetében megengedi, hogy a megbízásokat az iroda különböző tagjai ellássák, e tagok egymással szemben is titoktartásra kötelesek, és

biztosítaniuk kell, hogy az iroda ugyanazon alkalmazottja vagy megbízottja az érintett ügyek közül csak az egyikkel kapcsolatosan vehessen részt a feladat ellátásában.

Az ügyvédi tevékenység gyakorlóját nem terheli titoktartási kötelezettség alkalmazottjával szemben. Az ügyvédi tevékenység gyakorlóját nem terheli titoktartási kötelezettség a helyettes ügyvédjével szemben, valamint - az általuk nyújtott szolgáltatás nyújtásához szükséges mértékben - az alábbi személyek irányában:
a) az ügyvédi titkot tartalmazó adathordozó tárolását, archiválását, őrzését vagy az abban foglalt adatok feldolgozását végző személy, valamint az ügyvédi tevékenység gyakorlója által adatfeldolgozóként igénybe vett más közreműködő,
b) az ügyvédi tevékenység gyakorlója számára számviteli szolgáltatást nyújtó személy,
c) azok az ügyvédi megbízás teljesítésében közreműködő személyek, illetve a megbízás teljesítéséhez kapcsolódóan igénybe vett egyéb személyek, akiknek közreműködését, illetve igénybevételét az ügyfél jóváhagyta.

Az ügyvédi titoktartási kötelezettség a törvény 10. § (3) és (4) bekezdése alapján az ügyvédi titok megismerésére jogosult személyekre is kiterjed. A kamarai szervek és tisztségviselők az e törvényben meghatározott feladat- és hatáskörük gyakorlása során megismert ügyvédi titkot kötelesek megtartani. A bíróságok és hatóságok az eljárásuk során megismert ügyvédi titkot - az eljárásukra vonatkozó törvényben meghatározott keretek között - kezelhetik és használhatják fel.

Az ügyvédi titokkal az ügyfél vagy jogutódja jogosult rendelkezni. A törvény szerinti fegyelmi és hatósági ügyben, az eljárás lefolytatásához szükséges körben az ügyvédi tevékenység gyakorlója az eljáró kamarai szervek és bíróság előtt az ügyvédi titkot feltárhatja. Az ügyvédi tevékenység gyakorlója az ellene indult büntetőeljárásban a védekezéshez való jogának érvényesüléséhez szükséges mértékben az ügyvédi titkot feltárhatja. Az ügyvédi tevékenység gyakorlója a nem az ügyfele által a sérelmére vagy az ügyfele sérelmére elkövetett bűncselekmény felderítéséhez és bizonyításához szükséges mértékben - az ügyfele sérelmére elkövetett bűncselekmény esetében az ügyfele hozzájárulásával - az ügyvédi titkot feltárhatja.

Az ügyvédi titokról rendelkezni jogosult kérelmére, kezdeményezésére az ügyvédi titoktartásra kötelezett ellen indult bírósági, hatósági vagy más közhatalmi eljárásban az ügyvédi titoktartásra kötelezett a védekezéshez szükséges mértékben az ügyvédi titkot feltárhatja.

Az ügyvédi titoktartásra kötelezett a nála folytatott hatósági ellenőrzés, szemle vagy helyszíni kutatás során nem tárhatja fel az ügyvédi titkot tartalmazó iratokat és adatokat, az ügyvédi titokkal kapcsolatosan tanúvallomásra és adatszolgáltatás teljesítésére nem kötelezhető, de a hatóság eljárását nem akadályozhatja. Ezen bekezdéstől eltérően, a védekezés céljából készült irat hatósági, bírósági és más közhatalmi eljárásban bizonyítékként nem használható fel és - az ezen alcímben meghatározott esetek kivételével - közhatalmi szervek által nem vizsgálható meg, nem foglalható le, illetve nem másolható le, annak felmutatása, átadása, az ahhoz való hozzáférés adása megtagadható. E jogairól az érintett lemondhat, kivéve, ha az irat büntetőügyben való védelemhez kapcsolódik.

Védekezés céljából készült irat az olyan irat vagy iratrész, amely az ügyfélnek közhatalmi eljárásokban a védekezéshez való jogának gyakorlása érdekében, illetve annak keretében, az ügyvédi tevékenység gyakorlója és ügyfele közötti kommunikáció során keletkezett, vagy az ilyen kommunikáció során elhangzottakat rögzíti, és e jellege magából az iratból is kitűnik. Nem minősül védekezés céljából készült iratnak az az irat, amely nincs az ügyfél vagy az

ügyvédi tevékenység gyakorlója birtokában, kivéve, ha bizonyítják, hogy az irat jogellenesen vagy büntetőeljárás keretében került ki a birtokukból.

A hatóság jogosult az iratba - az e §-ban védett jog sérelme nélkül, a feltétlenül szükséges mértékig - betekinteni, annak megállapítása céljából, hogy a védekezés céljából készült iratként minősülésére való hivatkozás nem nyilvánvalóan alaptalan-e.
Ha az irat minősítése az ügyfél és a hatóság között vitatott, a szemle vagy helyszíni kutatás során a hatóság birtokba veheti az érintett iratot, azzal, hogy az iratot olyan tárolóeszközben kell elhelyezni, amely kizárja az adatok megismerhetőségét és utólagos megváltoztathatóságát. Az irat minősítése kérdésében a hatóság kérelme alapján az érintett ügyfél meghallgatásával a közigazgatási ügyben eljáró bíróság nemperes eljárásban dönt. Az iratot a hatóság csatolja a kérelméhez.

Ha a bíróság azt állapítja meg, hogy az irat, iratrész nem minősül védekezés céljából készült iratnak, azt a hatóság számára kiadja. Ellenkező döntés esetében a bíróság az iratot, iratrészt az érintett ügyfélnek adja ki. Ezen rendelkezéseket a büntetőeljárásról szóló törvényben meghatározott eltérésekkel kell alkalmazni.

8. Adatkezeléssel kapcsolatos jogosultságok

A rá vonatkozó adatok kapcsán jelen Szabályzat hatálya alatt a jogosultakat az alábbi jogok illetik meg a jogszabályok által megadott korlátozások figyelembevételével:

A tájékoztatás kéréshez való jog

Bármely személy a 4. pontban 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. Az érintett személynek nyújtott tájékoztatás tömör, könnyen hozzáférhető és könnyen érthető legyen, ezért azt világos és közérthető nyelven kell megfogalmazni és megjeleníteni.

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.

Adathordozhatósághoz való jog

Bármely személy a megadott elérhetőségeken keresztül kérheti, hogy a rá vonatkozó, általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa.

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.

A jogosultak azonban a fenti jogaikat gyakorlása során kötelesek figyelemmel lenni az ügyvédi tevékenység sajátosságára és kiemelt bizalmi jellegére és arra, hogy az adatkezelés milyen jogi alapokon történik. A jogok gyakorlása során figyelemmel kell lenni a jogszabályi korlátozásokra és adatkezelő jogaira, jogos érdekeire is, amely alapján a jogok érvényesítése visszaélésszerű joggyakorlást nem valósíthat meg.

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.

9. Adatvédelmi tisztviselő

Az adatkezelő és az adatfeldolgozó adatvédelmi tisztviselőt jelöl ki minden olyan esetben, amikor:

a) az adatkezelést közhatalmi szervek vagy egyéb, közfeladatot ellátó szervek végzik, kivéve az igazságszolgáltatási feladatkörükben eljáró bíróságokat;

b) az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek jellegüknél, hatókörüknél és/vagy céljaiknál fogva az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé;

c) az adatkezelő vagy az adatfeldolgozó fő tevékenységei a személyes adatok GDPR 9. cikk szerinti különleges kategóriáinak és a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó adatok nagy számban történő kezelését foglalják magukban.

A GDPR által meghatározottak szerint belső adatvédelmi tisztviselő („DPO") kinevezése a Irodánál nem kötelező és ennek megfelelően az iroda nem is jelöl ki DPO-t.

10. Információbiztonsági és iratkezelési (IBSZ) szabályok

Az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és 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 hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

a) a személyes adatok álnevesítését és titkosítását;

b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;

c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;

d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

Az adatkezelő és az adatfeldolgozó intézkedéseket hoz annak biztosítására, hogy az adatkezelő vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek kizárólag az adatkezelő utasításának megfelelően kezelhessék az említett adatokat, kivéve, ha az ettől való eltérésre uniós vagy tagállami jog kötelezi őket.

Irodánál elvégzésre került az információ biztonsági és technológiai belső vizsgálat, amely alapján megállapítható, hogy az elektronikus információbiztonság tekintetében folyamatos, zárt és a kezelt adatok sajátosságára tekintettel teljes körű-arányos védelem valósul meg.

Az információbiztonság és technológiai biztonság felelőse az irodavezető. Az irattárhoz hozzáférési joggal rendelkezik az irodavezető.

Az Iroda az általa kezelt személyes adatokat **fizikai védelemmel ellátott szerverén** és **irattárában tárolja, amelynek felelőse az irodavezető.**

A papír alapú és az elektronikus információik kezelése, módosítása során jelen Szabályzat szerint (különösen tekintettel a 7. pontban foglaltakra) kell eljárni.

Az IBSZ szabályozás célja:

- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
- az üzemeltetett informatikai és irattározási rendszerek rendeltetésszerű használata,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- a munkaállomásokon lekérdezhető adatok körének meghatározása,
- az adatállományok biztonságos mentése,
- az informatikai és irattározási rendszerek zavartalan üzemeltetése,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatvédelem és adatbiztonság feltételeinek megteremtése.

Az adatokat megfelelő intézkedésekkel védeni 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 nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban tárolt adatok közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

Az adatbiztonság megtervezésekor 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.

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.

Az informatikai rendszerre az alábbi tényezők hatnak: a környezeti infrastruktúra, a hardver elemek, az adathordozók, a dokumentumok, a szoftver elemek, az adatok, a rendszerelemekkel kapcsolatba kerülő személyek.

A védelmi intézkedések kiterjednek: az alkalmazott hardver eszközökre és azok működési biztonságára, az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra, az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig, az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírásszerű felhasználására, reprodukálhatóságára,

Az információhoz való hozzáférést lehetőség szerint a tevékenység naplózásával dokumentálni kell, ezáltal bármely számítógépen végzett tevékenység – adatbázisokhoz való hozzáférés, a fájlba vagy mágneslemezre történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet – utólag visszakereshető.

A naplófájlokat rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét a vállalkozás vezetőjének jelenteni kell.

A naplófájlok áttekintéséért, értékeléséért az informatikai vezető és a rendszergazdák a felelősek.

Az adatok védelmét, a feldolgozás – az adattovábbítás, a tárolás - során az operációs rendszerben és a felhasználói programban alkalmazott logikai matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftver, hardver adatvédelem).

Biztonságvédelmi előírások:

a) az irattár és a géptermek külső és belső helyiségeit biztonsági zárakkal kell felszerelni,

b) be- és kilépés rendjét szabályozni kell,

c) az illetéktelen behatolás tényét az iroda vezetőjének azonnal jelenteni kell,

d) az informatikai, irattározási és selejtezési eszközöket csak az Iroda vezetője használhatja,

Az adathordozókat könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak, a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni. A használni kívánt adathordozót a tárolásra kijelölt helyről kell kivenni, és oda kell vissza is helyezni. A munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz szükségesek. Az adathordozót másnak átadni csak engedéllyel szabad és a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

Elemi csapás (vagy más ok) esetén a számítógépekben vagy szerverekben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni: menteni a még használható anyagot, biztonsági mentésekről, háttértárakról a megsérült adatok visszaállítása, archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

A berendezések hibátlan és üzemszerű működését biztosítani kell. A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése.

Az üzemeltetést, karbantartást és szervizelést az informatikusok végzik. A munkák szervezésénél figyelembe kell venni: a gyártó előírásait, ajánlatait, a tapasztalatokat. Alapgép megbontását (kivéve a garanciális gépeket) csak informatikus végezheti el.

Adatbevitel hibátlan műszaki állapotú berendezésen történjen és a tesztelt adathordozóra lehet csak adatállományt rögzíteni. A bizonylatokat és mágneses adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani. Az adatrögzítő szoftver védelme. Lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják a rögzített tételek visszakeresésének és javításának lehetőségét is.

Hozzáférési lehetőség: a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (alapelv: a tárolt adatokhoz csak az illetékes személyek férjenek hozzá). az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti. A szerverek rendszergazda jelszavát az informatikai vezető kezeli.

Az adathordozók tárolására műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

Az adathordozók megőrzési idejét a törvényekben meghatározott bizonylat őrzési kötelezettségnek megfelelően kell kialakítani

Az adatfeldolgozás után biztosítani kell az adatok mentését. A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó munkatársak (felhasználók) feladata. A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban az informatikusok segítséget nyújtanak. A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért az informatikai vezető illetve a rendszergazdák a felelősek.

A számvitelről szóló többször módosított 2000. évi C. törvény értelmében a vállalkozásoknak az üzleti évről készített beszámolót, valamint az azt alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá más, a számviteli törvény követelményeinek megfelelő nyilvántartást olvasható formában legalább 8 évig meg kell őrizni.

A bizonylat elektronikus formában is megőrizhető, ha az alkalmazott módszer biztosítja az eredeti bizonylat összes adatának késedelem nélküli előállítását, folyamatos leolvashatóságát, illetve kizárja az utólagos módosítás lehetőségét. A programok nyilvántartásáért és működőképes állapotban való tartásáért a vezetők a felelősek.

A központi gépek háttértárairól folyamatosan biztonsági mentést kell készíteni. Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni. A vásárolt szoftverekről biztonsági másolatot kell készíteni.

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal. Vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell. Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket. A vállalkozás informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein illetve az Szabályzaton kívüli esetekben nem szabad.

Az adatkezelést végző személy tevékenysége során: kezeli és megőrzi a feladata ellátása során birtokába került adatokat; ügyel a személyes adatokat tartalmazó nyilvántartások biztonságos kezelésére és tárolására; gondoskodik arról, hogy az általa kezelt adatokhoz illetéktelen személy ne férhessen hozzá; betartja az adatkezelésre vonatkozó jogszabályokat és belső utasításokat; részt vesz az adatkezeléssel, adatvédelemmel összefüggő oktatásokon.

11. Adatfeldolgozás

Ha az adatkezelést az adatkezelő nevében más végzi, az adatkezelő kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés e rendelet követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására.

Az adatfeldolgozó külön írásbeli jogi kötelezettségvállalás alapján nyilatkozik arról, hogy jelen Szabályzatban foglaltakat betartja és hogy

a) a személyes adatokat kizárólag az adatkezelő írásbeli utasításai alapján kezeli – beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is –, kivéve akkor, ha az adatkezelést az adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő; ebben az esetben erről a jogi előírásról az adatfeldolgozó az adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja;

b) biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;

c) meghozza a GDPR 32. cikkben előírt intézkedéseket;

d) tiszteletben tartja a további adatfeldolgozó igénybevételére vonatkozó feltételeket;

e) az adatkezelés jellegének figyelembevételével megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti az adatkezelőt abban, hogy teljesíteni tudja kötelezettségét az érintett III. fejezetben foglalt jogainak gyakorlásához kapcsolódó kérelmek megválaszolása tekintetében;

f) segíti az adatkezelőt a GDPR 32–36. cikk szerinti kötelezettségek teljesítésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;

g) az adatkezelési szolgáltatás nyújtásának befejezését követően az adatkezelő döntése alapján minden személyes adatot töröl vagy visszajuttat az adatkezelőnek, és törli a meglévő másolatokat, kivéve, ha az uniós vagy a tagállami jog az személyes adatok tárolását írja elő;

h) az adatkezelő rendelkezésére bocsát minden olyan információt, amely az e cikkben meghatározott kötelezettségek teljesítésének igazolásához szükséges, továbbá amely lehetővé teszi és elősegíti az adatkezelő által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

g) haladéktalanul tájékoztatja az adatkezelőt, ha úgy véli, hogy annak valamely utasítása sérti ezt a rendeletet vagy a tagállami vagy uniós adatvédelmi rendelkezéseket.

Ha az adatfeldolgozó bizonyos, az adatkezelő nevében végzett konkrét adatkezelési tevékenységekhez további adatfeldolgozó szolgáltatásait is igénybe veszi, uniós vagy tagállami jog alapján létrejött szerződés vagy más jogi aktus útján erre a további adatfeldolgozóra is ugyanazok az adatvédelmi kötelezettségeket kell telepíteni, mint amelyek az adatkezelő és az adatfeldolgozó között létrejött, a kötelezettségvállalásban szerepelnek, különösen úgy, hogy a további adatfeldolgozónak megfelelő garanciákat kell nyújtania a megfelelő technikai és szervezési intézkedések végrehajtására, és ezáltal biztosítania kell, hogy az adatkezelés megfeleljen e rendelet követelményeinek.

Ha a további adatfeldolgozó nem teljesíti adatvédelmi kötelezettségeit, az őt megbízó adatfeldolgozó teljes felelősséggel tartozik az adatkezelő felé a további adatfeldolgozó kötelezettségeinek a teljesítéséért.

Az adatfeldolgozó és bármely, az adatkezelő vagy az adatfeldolgozó irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező személy ezeket az adatokat kizárólag az

adatkezelő utasításának megfelelően kezelheti, kivéve, ha az ettől való eltérésre őt uniós vagy tagállami jog kötelezi.

12. Adatkezelési nyilvántartások

Az adatkezelő és az adatfeldolgozó a végzett adatkezelési tevékenységekről nyilvántartást vezet.

E nyilvántartás (beleértve jelen Szabályzatban foglaltakat is) a következő információkat tartalmazza:

a) az adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő 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) ha lehetséges, a GDPR 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.

Minden adatfeldolgozó nyilvántartást vezet az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról; a nyilvántartás a következő információkat tartalmazza:

a) az adatfeldolgozó vagy adatfeldolgozók neve és elérhetőségei, és minden olyan adatkezelő neve és elérhetőségei, amelynek vagy akinek a nevében az adatfeldolgozó eljár, továbbá – ha van ilyen – az adatkezelő vagy az adatfeldolgozó képviselőjének, valamint az adatvédelmi tisztviselőnek a neve és elérhetőségei;

b) az egyes adatkezelők nevében végzett adatkezelési tevékenységek kategóriái;

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

d) ha lehetséges, a 32. cikk (1) bekezdésében említett technikai és szervezési intézkedések általános leírása.

A fent említett nyilvántartást írásban kell vezetni, ideértve az elektronikus formátumot is.

Az adatkezelő vagy az adatfeldolgozó megkeresés alapján a felügyeleti hatóság részére rendelkezésére bocsátja a nyilvántartást.

Az Iroda **adattovábbítási nyilvántartást vezet**, amelyben ellenőrizhető az esetlegesen megtörténő adattovábbítás jogszerűsége. A nyilvántartásban rögzítésre kerül a továbbított személyes adatok körének meghatározása, az adattovábbítás időpontja, jogalapja, az

adattovábbítás címzettje, továbbá a jogszabályban meghatározott egyéb adatok. Az adattovábbítási adatok megőrzési ideje a továbbítástól számított 5 év.

13. Incidenskezelési szabályok

Az adatvédelmi incidenst 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.

A bejelentés megtételére köteles az irodavezető.

Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

Az adatfeldolgozó az adatvédelmi incidenst, az arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti az adatkezelőnek.

Az incidens bejelentése során a bejelentésben legalább:

a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

d) ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Ha és amennyiben nem lehetséges az információkat egyidejűleg közölni, azok további indokolatlan késedelem nélkül később részletekben is közölhetők.

Az adatkezelő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az e cikk követelményeinek való megfelelést.

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.

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 incidenst indokolatlan késedelem nélkül, legkésőbb 72 órán belül be kell jelenteni az illetékes felügyeleti hatóságnál, kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani lehet, hogy az adatvédelmi incidens valószínűleg nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve.

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.

14. Bejelentővédelmi rendszer

Az Iroda a panaszokról és a közérdekű bejelentésekről szóló 2013. évi CLXV. törvényben foglalt rendelkezéseknek megfelelően visszaélés-bejelentési rendszert üzemeltet.

A visszaélés-bejelentési rendszerbe az Irodával szerződéses viszonyban álló, vagy olyan külső személyek tehetnek bejelentést, akiknek a bejelentés megtételéhez vagy a bejelentés tárgyát képező magatartás orvoslásához méltányolható jogos érdeke fűződik.

A bejelentőt semmiféle hátrányos megkülönböztetés nem érheti, akkor sem, ha az általa jóhiszeműen tett bejelentés a vizsgálat során megalapozatlannak bizonyul.

A bejelentés a Magyar Ügyvédi Kamara által vezetett www.muk.hu weboldalon keresztül tehető meg.

A vonatkozó bejelentési rendszer keretei között kezelt személyes adatok kezelésére és továbbíthatóságára a panaszokról és a közérdekű bejelentésekről szóló 2013. évi CLXV. törvény rendelkezései irányadók.

15. Záró rendelkezések

Jelen Adatvédelmi, Adatkezelési és Bejelentővédelmi Szabályzatot a Kovács Ügyvédi Iroda vezetője hagyja jóvá.

Az Iroda fenntartja magának a jogot, hogy jelen Szabályzatot módosítsa.

Jelen Szabályzat 2023. július 24. napján lép hatályba és ezzel egyidejűleg a korábban tárgyban kiadott szabályzatok hatályukat vesztik.

Gárdony, 2023. július 23.

_____

Kovács Ügyvédi Iroda
dr. Kovács Csaba
irodavezető-ügyvéd