A 17/2021. (IX.15.) POLGÁRMESTERI-JEGYZŐI EGYÜTTES UTASÍTÁSSAL KIADOTT

BUDAPEST FŐVÁROS XVIII. KERÜLET PESTSZENTLŐRINC-PESTSZENTIMRE ÖNKORMÁNYZATA ÉS BUDAPEST FŐVÁROS XVIII. KERÜLET PESTSZENTLŐRINC-PESTSZENTIMREI POLGÁRMESTERI HIVATAL ADATVÉDELMI ÉS ADATKEZELÉSI SZABÁLYZATA

1. BEVEZETÉS

1.1 A szabályzat célja

A Budapest Főváros XVIII. kerület Pestszentlőrinc-Pestszentimre Önkormányzata és a Budapest Főváros XVIII. kerület Pestszentlőrinc-Pestszentimrei Polgármesteri Hivatal (a továbbiakban együtt: **Hivatal**) jelen szabályzat megalkotásával és hatályba léptetésével a **személyes adatok** törvényi követelményeknek és a Hivatal szervezeti és működési szabályzatában megfogalmazottaknak megfelelő **kezelését biztosító szabályrendszert** hoz létre.
A Hivatal a szabályzat által meghatározott rendszer működtetésével a természetes személyek alapvető jogait és szabadságait és különösen a személyes adatok védelméhez való jogukat védi.
A szabályzat célja, hogy alkalmazásával a Hivatal megfeleljen az **EU 2016/679 számú Általános Adatvédelmi Rendelet**ének (a továbbiakban: **GDPR**) és a személyes adatok kezelését érintő magyar jogszabályoknak.
Ezeknek megfelelően célja a Szabályzatnak, hogy az érintettek megfelelő tájékoztatást kaphassanak a Hivatal által kezelt, valamint az általa megbízott adatfeldolgozó által feldolgozott személyes adatokról, azok forrásáról, az adatkezelés céljáról, időtartamáról, az adatkezelésbe esetlegesen bevont adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, továbbá – az érintett személyes adatainak továbbítása esetén – az adattovábbítás jogalapjáról és címzettjéről.
Jelen szabályzattal a Hivatal biztosítani kívánja a nyilvántartások működésének törvényes rendjét, az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, meg kívánja akadályozni az adatokhoz való jogosulatlan hozzáférést és azok jogosulatlan megváltoztatását, valamint nyilvánosságra hozatalát.

1.2 A szabályzat kezelése

1.2.1 A szabályzat karbantartása

Jelen szabályzatot **legalább évente**, vagy jogszabályi változásokat, valamint jelentős szervezeti változásokat követően át kell vizsgálni és aktualizálni kell.
A GDPR változása és/vagy a magyarországi vonatkozó jogszabályok változása esetén a szabályzat aktualizálását teljeskörűen és késedelem nélkül el kell végezni.

A szabályzat elkészítéséért és rendszeres felülvizsgálatáért a felelős: ***Adatvédelmi manager***
Az ellenőrzést elvégzi: ***Adatvédelmi tisztviselő***

2. A SZABÁLYZAT HATÁLYA

2.1 Személyi hatály

Jelen szabályzat hatálya a Hivatal irányítása alatt tevékenységet végző természetes személyekre, köztisztviselőkre, munkavállalókra, valamint a Hivatal számára/megbízásából adatfeldolgozói tevékenységet végző természetes személyekre, jogi személyekre terjed ki, valamint a Hivatali szolgáltatásokat igénybe vevő természetes személyekre vagy jogi személyek nevében eljáró természetes személyekre.

2.2 Tárgyi hatály

Ezt a szabályzatot kell alkalmazni a személyes adatok részben vagy egészben automatizált módon történő kezelésére, valamint azoknak a személyes adatoknak a nem automatizált módon történő kezelésére, amelyek valamely nyilvántartási rendszer részét képezik vagy a későbbiekben részévé kívánják tenni.
A szabályzat tárgyi hatálya kiterjed a Hivatal minden szervezeti egységénél folytatott valamennyi olyan folyamatra, amely során a GDPR 4. cikk 1. pontjában meghatározott személyes adat kezelése megvalósul.

2.3 Jogszabályok

2.3.1 A személyes adatok kezelésére vonatkozó törvényi előírások

GDPR

- 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)

Info tv.

- **2011. évi CXII. törvény** az információs önrendelkezési jogról és az információszabadságról

További törvények

- **2001. évi CVIII. törvény** az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről
- **2005. évi CXXXIII. törvény** a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól
- **2008. évi XLVIII. törvény** a gazdasági reklámtevékenység alapvető feltételeiről és egyéb korlátairól
- **2013. évi CLXV. törvény** a panaszokról és a közérdekű bejelentésekről
- **2013. évi L. törvény** az állami és önkormányzati szervek elektronikus információbiztonságáról
- **2012. évi I. törvény** a munka törvénykönyvéről
- **2011. évi CXCIX. törvény** a közszolgálati tisztviselőkről
- **2013. évi V. törvény** a polgári törvénykönyvről
- **2000. évi C. törvény** a számvitelről

3. FOGALOM MEGHATÁROZÁSOK ÉS RÖVIDÍTÉSEK

A szabályzat a GDPR-ban meghatározott fogalmakat használja a következők szerint:

„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, valamint 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 előre jelzésére 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 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 végrehajtására, 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 a GDPR szerint meghatározott kötelezettségek vonatkoznak;

„képviselő”: az az Unióban tevékenységi hellyel, valamint lakóhellyel rendelkező és az adatkezelő vagy adatfeldolgozó által a GDPR 27. cikke alapján írásban megjelölt természetes vagy jogi személy, aki, valamint amely az adatkezelőt vagy adatfeldolgozót képviseli az adatkezelőre vagy adatfeldolgozóra a GDPR értelmében háruló kötelezettségek vonatkozásában;

„vállalkozás”: gazdasági tevékenységet folytató természetes vagy jogi személy, függetlenül a jogi formájától, ideértve a rendszeres gazdasági tevékenységet folytató személyegyesítő társaságokat 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 a GDPR 51. cikkének megfelelően létrehozott független közhatalmi szerv;
Az Info tv. 38. § (2a) bekezdése alapján a GDPR-ban a felügyeleti hatóság részére megállapított feladat- és hatásköröket a Magyarország joghatósága alá tartozó jogalanyok tekintetében a GDPR-ban, valamint az Info tv.-ben meghatározottak szerint a Nemzeti Adatvédelmi és Információszabadság Hatóság gyakorolja.

„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 a GDPR-t megsértették-e, valamint, hogy az adatkezelőre vagy az adatfeldolgozóra vonatkozó tervezett intézkedés összhangban van-e a GDPR-ral; 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. 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.

„Adatvédelmi tisztviselő”: az Hivatal legfelső vezetésének direktben felelősséggel tartozó, a Hivatal adatkezelési tevékenységet ellenőrző, az adatkezelés tevékenységhez szaktanácsadással a Hivatal számára rendelkezésre álló, a Hivatal munkavállalója vagy külső szerződött partnere. A szerepkört betöltőt a Hivatal bejelenti az adatvédelmi hatósághoz (NAIH)

„Adatvédelmi manager”: a Hivatalon belül az az operatív személy, aki az adatkezelési tevékenységeket nyilvántartja, szervezi, kezeli, a hatásvizsgálatot elvégzi, az adatkezelési tevekénységéhez szakértőként kikérhető a vélemény. Amennyiben a Hivatal nem rendelkezik adatvédelmi tisztviselővel, az Adatvédelmi felelős látja le a kapcsolattartási szerepet az adatvédelmi hatósággal (NAIH)

„**Adatkezelési folyamatgazda”**: Azok az üzleti/szakterületi vezetők, aki üzleti folyamataik működtetése során személyes adatokat kezelnek és az adatkezelési tevékenységek nyilvántartásában meghatározott **konkrét adatkezelési tevékenységekhez vannak rendelve, mint felelősök**.

4. A HIVATAL ADATKEZELÉSI TEVÉKENYSÉGEI

4.1 A Hivatal adatkezelési tevékenysége

A Hivatal a GDPR meghatározása alapján **Adatkezelő**nek minősül alkalmazottai, szolgáltatásait igénybe vevői, egyéb szerződéses partnerei alkalmazottainak adatainak kezelésének tekintetében, ugyanakkor bizonyos adatfeldolgozási tevékenységek kapcsán **Adatfeldolgozó**ként működik.

A Hivatal az adatkezelési tevékenységeit az ***„ASZ-01-1 Adatkezelési tevékenység nyilvántartás”*** megnevezésű dokumentumban határozza meg és rögzíti, elektronikusan vezetve azt. Az adatkezelési tevékenység nyilvántartás mintáját az **1. függelék** tartalmazza.

4.2 A Hivatal adatfeldolgozói tevékenysége

A Hivatal a GDPR meghatározása alapján **Adatfeldolgozónak** minősül a megrendelői által a számára átadott vagy a megrendelők nevében kezelt adatok tekintetében.

A Hivatal az adatfeldolgozói tevékenységeit az ***„ASZ-01-2 Adatfeldolgozói adatkezelések nyilvántartása”*** megnevezésű dokumentumban határozza meg és rögzíti, elektronikusan vezetve azt. Az adatfeldolgozói adatkezelések nyilvántartásának mintáját a **2. függelék** tartalmazza.

5. VEZETÉS

5.1 Vezetői elkötelezettség

A Hivatal vezetése elkötelezett abban, hogy megfelelő intézkedéseket tegyen a természetes személyek személyes adatainak védelmében.
Ezen elkötelezettség jegyében a Hivatal vezetése a Hivatal Szervezeti és Működési Szabályzatával összhangban **adatvédelmi szabályrendszert** alakít ki, vezet be és működtet.
A Hivatal vezetése biztosítja az adatvédelmi szabályrendszer céljainak megvalósulásához szükséges erőforrásokat, közvetlenül támogatja az adatvédelmi szabályrendszer működését biztosító személyek munkáját és a szabályrendszer folyamatos fejlesztését.
A Hivatal vezetése ezen felül rendszeresen, de minimálisan évente egy alkalommal ellenőrzi a Hivatalban a személyes adatkezelés folyamatait.

5.2 Hivatali szerepek, felelősségek és hatáskörök

5.2.1 Hivatal Jegyzője

A Hivatal jegyzője mindent megtesz annak érdekében, hogy a Hivatal megfeleljen a jogszabályi előírásoknak és a jelen szabályzatban meghatározott vállalati elvárásoknak. A Hivatal jegyzője biztosítja a Hivatal számára az 1.1 pontban meghatározott cél eléréséhez szükséges erőforrásokat.

5.2.1.1 Hivatal Jegyzőjének feladatai

- Rendszeresen ellenőrzi az adatvédelmi folyamatokat a Hivatalban
- Döntést hoz az Adatvédelmi manager vagy az Adatvédelmi tisztviselő által előkészített adatvédelemmel kapcsolatos kérdésekben
- Aktív részese az Adatvédelmi incidens kezelési eljárásnak
- Biztosítja a szükséges erőforrásokat a Hivatalon belüli személyes adatkezeléshez
- Kinevezi az Adatvédelmi managert és tisztviselőt
- Bevonja az Adatvédelmi tisztviselőt a személyes adatkezeléssel kapcsolatos ügyekbe

5.2.2 Adatvédelmi tisztviselő

A Szervezet a GDPR 37. cikk (1) bekezdés a) pontja alapján adatvédelmi tisztviselőt jelöl ki.

Az adatvédelmi tisztviselő hatáskörét, felelősségét és feladatait a munkaköri leírása vagy megbízási szerződése tartalmazza. A feladatmeghatározást a **7. függelék** szerinti ***„ASZ-04 Adatvédelmi tisztviselő feladatai és jogállása”*** megnevezésű dokumentum minta alapján kell elkészíteni.

Legfontosabb feladatai:

- Ellenőrzi a Hivatalban a GDPR elvárásainak és a belső adatvédelemmel kapcsolatos szabályozásoknak való megfelelést, a feladatkörök kijelölését, az adatkezelésben résztvevők képzését és az auditokat,
- Kérésre szakmai tájékoztatást és tanácsot ad adatkezelési kérdésekben, így különösen az adatvédelmi hatásvizsgálatra vonatkozóan, és nyomon követi annak elvégzését,
- Kapcsolatot tart, konzultál és együttműködik az adatvédelmi hatósággal,
- Tájékoztat és szakmai tanácsot ad a Hivatalban adatkezelést végző alkalmazottak részére a GDPR és a hatályos magyar jogszabályok szerinti kötelezettségeikkel kapcsolatosan,
- Kezeli az adatvédelmi incidenseket,
- Érintetti igényérvényesítési kéréseket intézi.

5.2.2.1 Az Adatvédelmi tisztviselő jogállása

A Hivatal biztosítja, hogy az Adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon.
A Hivatal támogatja az Adatvédelmi tisztviselőt feladatai ellátásában azáltal, hogy biztosítja számára azokat a forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az Adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükségesek.
A Hivatal biztosítja, hogy az Adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne fogadjon el.

Az Adatvédelmi tisztviselő feladatai ellátásával összefüggésben nem bocsátható el és szankcióval nem sújtható.
Az Adatvédelmi tisztviselő közvetlenül a Hivatal legfelső vezetésének tartozik felelősséggel.

Az Adatvédelmi tisztviselőt feladatai teljesítésével kapcsolatban uniós vagy tagállami jogban meghatározott titoktartási kötelezettség (ha van ilyen) vagy a személyes adatok kezelésére vonatkozó titoktartási kötelezettség köti. Ez utóbbit az **5. függelék** szerinti ***„ASZ-02 Titoktartási nyilatkozat”*** megnevezésű dokumentum minta alapján kell elkészíteni.

Amennyiben az Adatvédelmi tisztviselő más feladatokat is ellát, a Hivatal biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

- Ez különösen azt jelenti, hogy az Adatvédelmi tisztviselő nem tölthet be olyan pozíciót a Hivatalon belül, amelynek keretében ő határozza meg a személyes adatok kezelésének céljait és eszközeit, azaz a Hivatalon belül nem tölthet be felsővezetői pozíciót (például vezérigazgató, ügyvezető igazgató, pénzügyi igazgató, főorvos, marketing osztályvezető, humán erőforrás vezető vagy informatikai osztályvezetők).

5.2.2.2 Hatósági bejelentés, közzététel

A Hivatal az Adatvédelmi tisztviselő kinevezését követően késedelem nélkül
- bejelentést teszt a területileg illetékes adatvédelmi hatóságnál a kinevezésről,
- a Hivatal által kiadott adatvédelmi tájékoztatókban közzéteszi az Adatvédelmi tisztviselő nevét és elérhetőségét.

5.2.2.3 A Hivatal Adatvédelmi tisztviselőjének elérhetőségei:

Az Adatvédelmi tisztviselő elérhetőségeit a 3. függelék tartalmazza.

5.2.3 Adatvédelmi manager

A Hivatal tekintettel az adatvédelmi feladatok menedzselésének fontosságára és az operatív feladatok ellátására **Adatvédelmi managert** nevez ki.
Az Adatvédelmi manager jogállása és feladatköre **nem** azonos a GDPR 38. és 39. cikkében megadott, jelen szabályzat 5.2.2 pontjában definiált Adatvédelmi tisztviselő jogállásával, még akkor sem, ha azokat a feladatokat elvégzi.
Az Adatvédelmi manager hatáskörét, felelősségét és feladatait a munkaköri leírása vagy megbízási szerződése tartalmazza. A feladatmeghatározást a **6. függelék** szerinti ***„ASZ-03 Adatvédelmi manager feladatai és jogállása”*** megnevezésű dokumentum minta alapján kell elkészíteni.

5.2.3.1 Az Adatvédelmi manager jogállása

A Hivatal biztosítja, hogy az Adatvédelmi manager a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon.
A Hivatal támogatja az Adatvédelmi managert feladatai ellátásában azáltal, hogy biztosítja számára azokat a forrásokat, amelyek e feladatok végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az Adatvédelmi manager szakértői szintű ismereteinek fenntartásához szükségesek.
Az Adatvédelmi manager a Hivatal jegyzőjének tartozik felelősséggel.
Az Adatvédelmi manager kifejezetten a személyes adatok kezelésére vonatkozó titoktartási kötelezettséget vállal az **5. függelék** szerinti ***„ASZ-02 Titoktartási nyilatkozat”*** megnevezésű dokumentum mintában meghatározottak alapján.
Amennyiben az Adatvédelmi manager más feladatokat is ellát, a Hivatal biztosítja, hogy e feladatokból ne fakadjon összeférhetetlenség.

5.2.3.2 A Hivatal Adatvédelmi managerének elérhetőségei:

Az Adatvédelmi manager elérhetőségeit a 3. függelék tartalmazza.

5.2.4 Adatkezelési folyamatgazda

A Hivatal az adatkezelési folyamatok nyilvántartásában minden azonos céllal rendelkező adatkezelési tevékenységhez egy adatkezelési folyamatgazdát jelöl ki.

5.2.4.1 Adatkezelési folyamatgazda

Az Adatkezelési folyamatgazda felelős az általa felügyelt adatkezelési tevékenység során

- kezelt adatokhoz történő hozzáférés engedélyezéséért, a hozzáférés visszavonása és a hozzáférések rendszeres, legalább évente egy alkalommal történő felülvizsgálatáért,
- az egyes lépéseinek meghatározásáért, ezek dokumentálásáért,
- jelen szabályzat vagy a GDPR elvárásainak változása esetén a folyamaton belül a szükséges változtatások végrehajtásáért és dokumentálásáért,
- feltárt adatkezelési gyengeségek jelentéséért az Adatvédelmi managernek/tisztviselőnek.

5.2.5 Adatkezelésre feljogosított személyek

A Hivatal minden alkalmazottja kisebb-nagyobb mértékben kezel a munkája során személyes adatokat.
A Hivatal gondoskodik arról, hogy minden alkalmazottja a személyes adatok kezelésére vonatkozó titoktartási kötelezettséget vállaljon. A titoktartási nyilatkozatokat az **5. függelék** szerinti ***„ASZ-02 Titoktartási nyilatkozat”*** megnevezésű dokumentum minta alapján kell elkészíteni.

> *A titoktartási nyilatkozatok aláíratását a munkavállalókkal a belépéskor a beléptetést végző **HR munkatárs végzi.***
> *Az ellenőrzést elvégzi : **Adatvédelmi tisztviselő***

6. ADATKEZELÉSI FOLYAMATOK MENEDZSMENTJE

6.1 Beépített és alapértelmezett adatvédelem

A Hivatal az adatkezelés tervezésekor a kockázatokkal arányos technikai és szervezési védelmi intézkedéseket épít az adatkezelési folyamataiba, hogy biztosítsa az érintettek személyes adatainak védelmét.
A Hivatal végrehajtja a megfelelő **technikai és szervezési intézkedések**et annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek.

6.2 Adatkezelési tevékenységek kockázatértékelése

A személyes adatok kezelése kockázatokkal járhat a természetes személyek alapvető jogaira és szabadságaira és különösen a személyes adatok védelméhez való jogukra nézve, ezért a Hivatal a nem törvényi felhatalmazás alapján végzett adatkezelések tekintetében az **adatkezelés megkezdése előtt**, az adott adatkezelés vonatkozásában **mérlegeli a kockázatokat** és ennek megfelelően hoz döntést az adatkezelési tevékenységről.
Az adatkezelési tevékenységek kockázatértékelése az „***ASZ-05 Adatvédelmi hatásvizsgálat és kockázat menedzsment szabályzat”*** alapján történik, amely jelen szabályzat **1. mellékletét** képezi.
A bevezetésre kerülő adatkezelési tevékenységek esetében a kockázatértékelést az adatkezelés megkezdése előtt el kell végezni és az adatkezelést csak a kockázatértékelésből következő kockázatcsökkentő intézkedések bevezetését követően szabad megkezdeni.

A Hivatal a kockázatelemzést követően hozott **szervezési és a technikai** intézkedésekkel együttesen fedi le az adatkezelés teljes folyamatát, és így felel meg az adatvédelmi követelményeknek.

Az adatkezelési folyamatokra kockázatelemzés és kezelés, valamint a hatásvizsgálat elvégzésért a felelős: ***Adatvédelmi manager***
Az ellenőrzést elvégzi: ***Adatvédelmi tisztviselő***

6.2.1 Szervezési intézkedések

A szervezési intézkedések keretét jelen szabályzat és a hozzá kapcsolódó szabályzatok alkotják.
Az adatkezelési tevékenységhez kapcsolódó adatkezelési folyamatlépések tervezése, működtetése és folyamatos fejlesztése során a következőket kell figyelembe venni:

- jelen adatvédelmi szabályrendszert,
- az adatvédelmi hatásvizsgálatból következő intézkedéseket,
- az adatvédelmi incidensek elemzéséből következő intézkedéseket,
- a belső ellenőrzések során feltárt vagy az adatkezelésben résztvevő által jelentett gyengeségek elemzéséből származó javító intézkedéseket.

Az adatkezelési folyamatok alatt az alábbi tevékenységeket azonosítjuk:

- az adatkezelési tevékenységre feljogosított **személyek által végzett munka**,
- az **informatikai rendszerek**ben megvalósított automatizált vagy kezelői beavatkozással megvalósuló **folyamatok**.

Az adatkezelési folyamatok megtervezése során meghatározásra kerülnek a következő szervezési intézkedések:

- **adatkezelési szerepkörök** meghatározása,
- **Adatvédelmi manager** kinevezése és a munkaköri feladatainak meghatározása,
- a személyes adatok kezeléséhez kapcsolódó jogosultságok és felelősségek pontosítása kerülnek,
- a **munkautasítások**, amelyek az adatkezelési tevékenységek pontos lépéseit határozzák meg,
- az informatika rendszerrel szembeni elvárások.

A szervezési intézkedések részét képező, jelen szabályzathoz kapcsolódó dokumentumok felsorolását a **4. függelék** szerinti ***„ASZ-01-4 Adatvédelmi és adatkezelési szabályzathoz kapcsolódó dokumentumok listája”*** megnevezésű dokumentum tartalmazza.

Az adatkezelési dokumentumlista napra készen tartásáért a felelős: ***Adatvédelmi manager***
Az ellenőrzést elvégzi: ***Adatvédelmi tisztviselő***

6.2.2 Technikai intézkedések

A Hivatal a személyes adatok védelmével kapcsolatos technikai intézkedések megvalósítása érdekében bevezette, és rendszeresen karbantartja az ***Információbiztonsági Szabályzatát***

(IBSZ). A Hivatal az Információbiztonsági szabályzatban dokumentált információkat tárol az információbiztonsági technikai intézkedésekről.

6.2.2.1 Informatikai rendszerrel szembeni elvárások

Az informatikai rendszerre vonatkozó technikai intézkedések megtervezésének kiindulópontjaként a szervezési intézkedések tervezése során figyelembe kell venni minimálisan az alábbiakat:
Az informatikai rendszer képes legyen:

- biztosítani a benne kezelt személyes adatok bizalmasságát, sértetlenségét és rendelkezésre állását,
- a kockázatokkal arányos titkosítási eljárások alkalmazására,
- teljesíteni az üzletmenet folytonossági eljárásokat és incidens esetén az adatok hozzáférését képes legyen a megfelelő időn belül visszaállítani.

További elvárás az informatikai rendszer üzemeltetőjétől a technikai és szervezési intézkedések rendszeres, de legalább évente egy alkalommal történő tesztelése.

6.2.3 Információbiztonsági intézkedések

Az információbiztonsági intézkedések azok a technikai és szervezési intézkedések, amelyek a Hivatal információs vagyonának, és ezen belül kiemelten a személyes adatoknak a **bizalmas jellegét**, a **sértetlenségét** és a **rendelkezésre állását** biztosítják.
A Hivatal információbiztonsági intézkedéseit a Hivatal ***Információbiztonsági Szabályzata*** tartalmazza.

6.3 Adatkezelési tevékenységek azonosítása és nyilvántartása

A Hivatal a már megkezdett és a későbbiekben bevezetésre kerülő adatkezelési tevékenységekről teljes körű nyilvántartást vezet.
Az „adatkezelési tevékenység” azon adatkezelési műveletek összessége, **amelyeknek egy adott célja van**. Az Adatvédelmi tisztviselő az adatkezelés megkezdése előtt ellenőrzi, hogy az adatkezelés megfelelő a GDPR és jelen szabályzat elvárásainak.
Folyamat:

1. Azonosítja az adatkezelési tevékenységeket a Hivatalon belül.
2. Csoportosítja az azonos cél érdekében történő adatkezelési tevékenységeket.
3. Minden adatkezelési célhoz a 6.4 pontban megfogalmazott jogalapok közül társít egyet.
   Amennyiben nem társítható jogalap az adatkezelési célhoz úgy az adatkezelési tevékenységet nem szabad elkezdeni vagy azonnal meg kell szakítani.
4. Meghatározza a 6.3.1 és 6.3.2 pontban meghatározott paramétereket.
5. Adatkezelési folyamatgazdát jelöl ki minden azonos céllal megjelölt adatkezelési tevékenységcsoporthoz.
6. Megvizsgálja, hogy az adatkezelési cél megszűnése estén vagy a hozzá kapcsolódó határidő lejáratakor a Hivatal befejezi-e az adatkezelési tevékenységet vagy másik adatkezelési cél mentén kezeli tovább az adatokat.

6.3.1 Adatkezelési tevékenységek azonosítása

A Hivatal azonosítja az adatkezelőként vagy adatfeldolgozóként végzett adatkezelési tevékenységeit. Az adatkezelési tevekénységek azonosításának célja, hogy a Hivatal tisztában legyen a személyes adatok kezelési folyamatainak Hivatalon belüli megvalósításával annak érdekében, hogy megfelelő kontroll alatt tarthassa azokat.

Az adatkezelési tevekénységek azonosításáért a felelős : ***Adatvédelmi manager***
Az ellenőrzést elvégzi: ***Adatvédelmi tisztviselő***

A Hivatal adatkezelési tevékenységeinek azonosításánál az alábbi paramétereket határozza meg a Hivatal:

Adatkezelési folyamat	A Hivatal által végzett adatkezelési tevekénységek csoportba foglalva, azonos adatkezelési cél mentén.
Adatkezelési folyamatgazda	Az a hivatali egység vezető, akinek a hivatali egységében kezelik az azonosított adatkezelési tevekénységeket.
Adatkezelési cél	Az adatkezelési tevékenységek összefoglaló célja.
Jogalap	A 6.4.3.-6.4.8 pontokban definiált jogalapok közül egy.
Érintettek kategóriái	Azon természetes személyek összefoglaló csoportjai, akik adatait az adatkezelési folyamatban kezeli a Hivatal.
Kezelt személyes adatok kategóriái	A kezelt személyes adatok összefoglaló megnevezése.
Címzettek kategóriái	Azon szervezetek összefoglaló megnevezése melyeknek továbbítják a személyes adatokat, vagy hozzáférési lehetőséget biztosít a Hivatal az adatkezelési tevékenység során.
3. Országba továbbítás címzettje	Az EGT tagállamain kívüli szervezetbe vagy címzettjének történő adattovábbítás esetén a címzett megnevezése.
Továbbítás garanciái	A 3. Országba történő adattovábbítás biztonsági garanciának dokumentálása.
Tervezett adattárolási határidő	Az adatok kezelésének tárolásának tervezett határideje, vagy annak kiszámítási módja vagy definíciója. (pl.: visszavonásig)
Adatbiztonság leírása	Az adatkezelés során alkalmazott információbiztonsági megoldások.
Elfogadás /tudomásul vétel bizonyítása	Hozzájárulásos jogalap esetén az adatkezelő milyen módon bizonyítja a hozzájárulást/tudomásul vételt.

A Hivatal a GDPR 30. cikk (1) bekezdése alapján elkészíti az adatkezelési tevékenységek nyilvántartását, amelyet az „***ASZ-01-1 Adatkezelési tevékenység nyilvántartás”*** táblázatban rögzít.

Az adatkezelési tevekénységek dokumentálásáért a felelős: ***Adatvédelmi manager***
Az ellenőrzést elvégzi: ***Adatvédelmi tisztviselő***

6.3.2 Adatfeldolgozói tevékenységek nyilvántartása

A Hivatal a GDPR 30. cikk (2) bekezdése alapján elkészíti az **adatfeldolgozóként** végzett adatkezelési tevékenységek nyilvántartását, amelyet az „***ASZ-01-2 Adatfeldolgozói adatkezelések nyilvántartása”*** táblázatban rögzít.

Az adatkezelési tevékenységek nyilvántartása csak azokat az adatokat tartalmazza, amelyek a GDPR 30. cikke szerint szükséges, minden további nyilvántartást a Hivatal ettől elkülönítve kezel.

Az adatkezelési dokumentumlista nyilvántartásáért és napra készen tartásáért a felelős: ***Adatvédelmi manager***
Az ellenőrzést elvégzi: ***Adatvédelmi tisztviselő***

A Hivatal **adatfeldolgozóként** végzett adatkezelési tevékenységeinek nyilvántartásánál az alábbi paramétereket rögzíti a Hivatal:

Adatkezelő neve	Az a szervezet, akinek megbízása alapján, akinek, vagy amelynek a nevében történik az adatkezelés.
Az adatkezelő elérhetősége	Az előző sorban meghatározott adatkezelő elérhetősége.
Adatkezelési tevékenységek kategóriái	Az adatkezelési tevékenységek összefoglaló csoportosítása. Pl. IT üzemeltetés, bérszámfejtés, könyvelés, adattisztítás stb.
További adatfeldolgozók	Azon adatfeldolgozók megnevezése, akiket a Hivatal, mint alvállalkozó adatfeldolgozó bevon az adatkezelési tevékenységbe, vagy akik/amelyek hozzáférnek, tárolják vagy kezelik az adatkezelő adatait.
3. országba továbbítás címzettje	Az EGT tagállamai kívüli szervezetbe vagy címzettének történő adattovábbítás esetén a címzett megnevezése.
A 3. országba továbbítás garanciái	Azok a biztonsági garanciák megnevezése, melyek mentén a Hivatal az adatokat a 3. Országba továbbítja. pl.: EU Bizottsági megfelelőségi határozat, kötelező érvényű vállalati szabályok, az érintett kifejezett hozzájárulása stb.

6.4 Az adatkezelés jogszerűsége

A Hivatal a személyes adatok kezelését csak akkor végzi, ha a GDPR 6. cikk (1) bekezdésében megadott hat jogalap közül, legalább az egyik alkalmazható.

A jogalapok meghatározásának felelőse: ***Adatvédelmi manager***
Az ellenőrzést elvégzi: ***Adatvédelmi tisztviselő***

6.4.1 Gyermekek személyes adatainak kezelése

A Hivatal alaptevékenységét és szolgáltatásait kifejezetten NEM gyermek (16. életévét be nem töltött) korúak számára nyújtja, azonban törvényi felhatalmazás, vagy szülői felügyeleti jog gyakorlójának hozzájárulása alapján kezel gyermekekre vonatkozó személyes adatot.
Amennyiben az adatkezelés során a Hivatal számára egyértelművé válik, hogy a természetes személy még nem töltötte be a 16. életévét és nincs törvényi előírás az adatok kezelésére vonatkozóan, késedelem nélkül beszerzi a szülői felügyeleti jog gyakorlójától az adatkezeléshez a hozzájárulást a **10. függelék** szerinti „***ASZ-06 Szülői hozzájáruló nyilatkozat"*** megnevezésű dokumentum minta alapján vagy megszünteti az adatok kezelését.

Ha a Hivatal felügyelete alatt adatkezelést végzők számára egyértelművé válik, hogy egy kezelt adat 16 éven aluli természetes személyé és nincs törvényi előírás, vagy hozzájárulás az adatok

kezelésére vonatkozóan, késedelem nélkül kötelesek jelenteni az incidenskezelési szabályzatnak megfelelően.

6.4.2 A személyes adatok különleges kategóriáinak kezelése

Különleges adatok a következők: 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.

A Hivatal a **személyes adatok különleges kategóriáit** alapértelmezetten nem kezeli, kivéve a GDPR rendelet 9. cikk (2) bekezdésében megfogalmazott kivételek alapján, de legfőképpen:

a) az érintett kifejezett hozzájárulását adta az említett személyes adatok egy vagy több konkrét célból történő kezeléséhez, kivéve, ha az uniós vagy tagállami jog úgy rendelkezik, hogy a GDPR 9. cikk (1) bekezdésében említett tilalom nem oldható fel az érintett hozzájárulásával;
b) az adatkezelés az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében szükséges, ha az érintett alapvető jogait és érdekeit védő megfelelő garanciákról is rendelkező uniós vagy tagállami jog, valamint a tagállami jog szerinti kollektív szerződés ezt lehetővé teszi;
c) az adatkezelés megelőző egészségügyi vagy munkahelyi egészségügyi célokból, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, valamint egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében, továbbá a GDPR 9. cikk (3) bekezdésében említett feltételekre és garanciákra figyelemmel.

6.4.3 Hozzájárulás jogalap alkalmazása

GDPR 6. cikk (1) bekezdés a) pontja: „az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez”.

Az érintetti hozzájáruláson alapuló adatkezelést megelőzően az érintettet tájékoztatni kell a releváns adatkezelési tájékoztató rendelkezésre bocsátásával. A tájékoztatásnak ugyanazon a csatornán, a hozzájárulás kérésével egyidőben kell megtörténnie.
Annak megállapítása során, hogy a hozzájárulás önkéntes-e, a lehető legnagyobb mértékben figyelembe kell venni azt a tényt, hogy a szerződés teljesítésének feltételéül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez.

6.4.3.1 Hozzájáruló nyilatkozat

A hozzájáruló nyilatkozatnak – függetlenül annak megjelenési formájától – teljesítenie kell a következő feltételeket:

- legyen egyértelmű,
- más ügyektől elkülöníthető,
- érhető, világos, egyszerű nyelvezetű.

6.4.3.2 Hozzájárulás munkavállalók esetében

A hozzájárulás érvényességének feltétele az önkéntesség, ezért munkavállalók esetében a Hivatal különös körültekintéssel alkalmazza. A hozzájárulás munkavállalók esetében csak olyan adatkezelési tevékenységre vonatkozzon, ami nincs összefüggésben a munkaviszonnyal és a munkáltatói jogok gyakorlásával nem áll kapcsolatban. A Hivatal kifejezetten figyelmet fordít arra, hogy a munkavállalók esetében a hozzájárulásos jogalap mentén kezelt adatok esetében a hozzájárulás megtagadása esetén munkaviszonyával kapcsolatosan semmilyen hátrányos következmény ne érje a munkavállalót.

6.4.3.3 Hozzájárulás visszavonása

Az érintett az adatkezeléshez való hozzájárulását bármikor visszavonhatja, erről a jogáról, valamint a visszavonás módjáról a hozzájáruló nyilatkozatban vagy az ezzel egyidőben átadott adatkezelési tájékoztatóban kell tájékoztatni.
A hozzájárulás visszavonásának olyan egyszerűnek kell lenni, mint amilyen a hozzájárulás megadása.
A Hivatal a hozzájárulás visszavonásához alternatív csatornát is biztosít, az Adatvédelmi manager vagy Adatvédelmi tisztviselő elérhetőségén írásban bejelentett hozzájárulás visszavonási igényeket is elfogadja.
A Hivatal a hozzájárulások meglétét és a visszavonást követő intézkedéseket az **adatkezelési tevékenységek nyilvántartásában** adatkezelési tevékenységenként megadott módon igazolja és ennek megfelelően a szükséges szervezési és technikai intézkedéseket megteszi.

6.4.4 Szerződéses jogalap alkalmazása

GDPR 6. cikk (1) bekezdés b) pontja: „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”.

Jogi személyekkel (vállalkozások, céges ügyfelek) kötött szerződések esetében ez a jogalap **nem használható**.
Szerződéskötésre irányuló közvetlen cselekmények esetében (ajánlatkérés, ajánlatadás, szerződéses feltételek egyeztetése) ez a jogalap alkalmazandó.

6.4.5 Jogi kötelezettség jogalap alkalmazása

GDPR 6. cikk (1) bekezdés c) pontja: „az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges”.

Tipikus jogszabályi kötelezettségeket ír elő többek között a számviteli törvény, az adó törvény, a munkajog. A jogi kötelezettségre hivatkozva csak azokat a személyes adat kategóriákat szabad tárolni, amelyeket az adott jogszabály előír, azokat viszont kötelező.
A jogi kötelezettség jogalap alkalmazása estében kötelező a Hivatal **jogi főosztályának egyetértését** megszerezni.

6.4.6 Létfontosságú érdek jogalap alkalmazása

GDPR 6. cikk (1) bekezdés d) pontja: „az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges”.

A Hivatal a létfontosságú érdek jogalapot jelenleg **nem alkalmazza** a személyes adatkezelési tevékenységei során.

6.4.7 Közhatalmi jogosítvány jogalap alkalmazása

GDPR 6. cikk (1) bekezdés e) pontja: „az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges”.

A Hivatal rendszerint a közhatalmi jogosítvány jogalapot **alkalmazza** a személyes adatkezelési tevékenységei során.

6.4.8 Jogos érdek jogalap alkalmazása

GDPR 6. cikk (1) bekezdés f) pontja: „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 érdek jogalap alkalmazását megelőzően a Hivatal **mérlegeli**, hogy az adott adatkezelés esetében az érintett alapvető jogai és szabadságai és különösen a személyes adatok védelméhez való joga milyen mértékben sérülhet, és ezt összeveti saját érdekével, amely az adatkezelést szükségessé teszi.

6.4.8.1 Közvetlen üzletszerzés

A GDPR preambulum (47) bekezdése alapján a személyes adatok közvetlen üzletszerzési célú kezelése jogos érdeken alapulónak tekinthető. A Hivatal a közvetlen üzletszerzés jogalapot **nem alkalmazza** a személyes adatkezelési tevékenységei során.

6.4.8.2 Más adatkezelési célok esetében

Más adatkezelési célok esetében, különösen a munkavállalók (vagy más érintettek) megfigyelése esetében, az „adatkezelő jogos érdeke” adatkezelési jogalap alkalmazhatóságáról a Hivatal az adatkezelési tevékenység megkezdése előtt elvégzett **érdekmérlegelés** eredménye alapján dönt.

6.5 Érintetti jogok érvényesítése

A Hivatal fokozott figyelmet fordít arra, hogy a GDPR-ban meghatározott érintetti jogok érvényesítése megfeleljen a jogszabályi követelmények és az érintettek elvárásinak.
Ennek érdekében az érintetti jogokhoz kapcsolódóan kidolgozásra került az ***„ASZ-07 Érintetti jogok érvényesítése szabályzat”***, amely jelen szabályzat **2. mellékletét** képezi**.**

6.6 Célhoz kötöttség és adattakarékosság

A Hivatal személyes adatokat csak tisztességes, jól meghatározott, egyértelmű és jogszerű célból kezel.

A Hivatal az adatkezelési tevékenységek megtervezése során gondoskodik arról, hogy a kezelt személyes adatok terjedelme (adatkategóriák számossága és típusa) csak a cél szempontjából releváns és szükséges mértékű legyen. Ezt többek között az **Adatvédelmi hatásvizsgálat és kockázat menedzsment szabályzat** következetes alkalmazásával biztosítja.

6.7 Pontosság és korlátozott tárolhatóság

6.7.1 Intézkedések a pontosság érdekében

A Hivatal az adatkezelési tevékenysége során folyamatba épített ellenőrzéseket végez a kezelt személyes adatok pontosságának biztosítása érdekében.
Ahol ez lehetséges, az informatikai rendszer a személyes adatok szintaktikai ellenőrzésével is támogatja a pontosságot.
A személyes adatokhoz való hozzáférés korlátozása és a hozzáférés ellenőrzése csökkenti az adatok véletlen vagy szándékos megváltoztatásának kockázatát.

6.7.2 Adatmegőrzés és adateltávolítás

Amíg a személyes adat kezelésének van **célja és** érvényes **jogalapja**, addig az adatot meg kell őrizni, ezt az időpontot követően az adatot törölni kell.
Az adatkezelési cél megváltozását vagy megszűnését az Adatkezelési folyamatgazdának kell figyelemmel kísérni és adott esetben ennek megfelelően intézkedni az adatok törléséről.
A jogalapok változási lehetőségei:

- jogszabályi változások,
- érintetti jogok gyakorlása (hozzájárulás visszavonása, tiltakozás, törlési kérelem),
- az idő múlása (letelik a jogalap által meghatározott idő).

A megőrzési idő leteltét lehetőség szerint jelezze az informatikai rendszer, de automatizált törlést nem szabad alkalmazni.
A törlést minden esetben az Adatkezelési folyamatgazdának **jóvá kell hagynia**, miután megvizsgálta nem áll-e fenn olyan körülmény, ami elsőbbséget élvező, jogszerű ok az adat további tárolására.

6.8 Integritás és bizalmas jelleg

6.8.1 Biztonsági intézkedések

A Hivatal által megtervezett és megvalósított információbiztonsági intézkedések biztosítják a személyes adatok **bizalmas jellegét**, **sértetlenségét** és **rendelkezésre állását.** Ezeket az intézkedéseket a Hivatal által kiadott és alkalmazott ***Információbiztonsági Szabályzat*** tartalmazza.

6.8.2 Adatvédelmi incidensek kezelése

A Hivatal az adatvédelmi incidensek kezelését, beleértve a felügyeleti hatósághoz való bejelentést és szükség esetén az érintettek tájékoztatását az „***ASZ-08 Adatvédelmi incidenskezelési szabályzat*”** alapján végzi, amely jelen szabályzat **3. mellékletét** képezi.

6.9 Adatfeldolgozók menedzselése

A Hivatal által megbízott **adatfeldolgozó** az adatkezelést érintő érdemi döntést nem hozhat, a tudomására jutott személyes adatokat kizárólag technikai feladatként a Hivatal rendelkezései szerint dolgozhatja fel, saját céljára a Hivatal adatain adatfeldolgozást nem végezhet, a

személyes adatokat a Hivatal rendelkezései szerint köteles tárolni és megőrizni vagy az adatkezelési folyamat végeztével a Hivatal döntése alapján visszaállíthatatlanul törölni.

6.9.1 Adatfeldolgozók az EU-n belül

Itt EU-n belülinek az **EGT tagállamai** tekintendők, ezen országok vonatkozásában nincs semmilyen korlátozás, azaz olyan mintha Magyarország területén belüli adattovábbításra kerülne sor.
A Hivatal csak olyan adatfeldolgozókat vesz igénybe, akik szervezési és technikai intézkedésekkel biztosítani tudják, hogy a Hivatal adatvédelmi követelményei teljesüljenek.
Az adatfeldolgozásra vonatkozó szerződést írásba kell foglalni. Az adatfeldolgozókkal kötött szerződésnek rendelkeznie kell a következőkről:

- az adatfeldolgozó a személyes adatokat kizárólag a Hivatal írásbeli utasításai alapján kezeli, beleértve a személyes adatoknak valamely harmadik ország vagy nemzetközi szervezet számára való továbbítását is;
- az adatfeldolgozó biztosítja azt, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak;
- az adatfeldolgozó meghozza az adatkezelés biztonságát szavatoló megfelelő technikai és szervezési intézkedéseket (GDPR 32. cikk);
- az adatfeldolgozó tiszteletben tartja a további adatfeldolgozó igénybevételére vonatkozóan a feltételeket, azaz
    - csak a Hivatal előzetesen írásban tett eseti vagy általános felhatalmazásának birtokában vesz igénybe további adatfeldolgozót,
    - biztosítja, hogy a további adatfeldolgozó megfelelő garanciákat nyújtson a megfelelő technikai és szervezési intézkedések végrehajtására,
    - ha a további adatfeldolgozó nem teljesíti adatvédelmi kötelezettségeit, az őt megbízó adatfeldolgozó teljes felelősséggel tartozik a Hivatal felé a további adatfeldolgozó kötelezettségeinek a teljesítéséért;
- az adatfeldolgozó megfelelő technikai és szervezési intézkedésekkel a lehetséges mértékben segíti a Hivatalt abban, hogy teljesíteni tudja kötelezettségét az érintett jogainak kapcsolódó kérelmek megválaszolása tekintetében;
- az adatfeldolgozó segíti a Hivatalt az adatvédelmi incidensek kezelésében, figyelembe véve az adatkezelés jellegét és az adatfeldolgozó rendelkezésére álló információkat;
- az adatfeldolgozó az adatkezelési szolgáltatás nyújtásának befejezését követően a Hivatal döntése alapján minden személyes adatot töröl vagy visszajuttat a Hivatalnak, és törli a meglévő másolatokat;
- az adatfeldolgozó a Hivatal rendelkezésére bocsát minden olyan információt, amely lehetővé teszi és elősegíti a Hivatal által vagy az általa megbízott más ellenőr által végzett auditokat, beleértve a helyszíni vizsgálatokat is.

Az adatfeldolgozók adatvédelmi szempontok menedzselésének a felelőse: ***az adatfeldolgozó partner kapcsolattartója.***

6.9.1.1 Adatátadás az Adatfeldolgozók részére

Az adatkezelő a jelen szabályzat **4. mellékletét** képező *„**ASZ-09 Adatátadási szabályzatban”*** rögzített szervezési és technikai feltételek mellett továbbíthat személyes adatokat az Adatfeldolgozóknak.

6.10 Adattovábbítás harmadik országokba

EU-n kívülinek, azaz harmadik országnak tekintendő minden olyan ország, ami az **EGT tagállamain** kívül van.
Amennyiben a címzett harmadik országban van, az EU-n belüli adattovábbítás feltételein felül további feltételek biztosítása szükséges:

1) Az adattovábbításhoz nem szükséges külön engedély azon országok esetében, ahol a Bizottság megállapította, hogy a harmadik ország, a harmadik ország valamely területe, vagy egy vagy több meghatározott ágazata, **megfelelő védelmi szintet** biztosít
   Ezen országok aktuális listája:
   https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
2) A felügyeleti hatóság által jóváhagyott megállapodás a Hivatal és a címzett között (GDPR 46. cikk (3) bekezdés).
3) Kötelező erejű vállalati szabályok vannak érvényben az adatfeldolgozó és a Hivatal között.
   Ezen országok aktuális listája:
   http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm
   4) Amennyiben az 1)-3) pontban megfogalmazott határozat és megfelelő garanciák nem állnak rendelkezésre az adattovábbításhoz a Hivatal tájékoztatja az Érintettet a 3. országba történő adattovábbítás veszélyeiről és kifejezett hozzájárulását kéri az adatok továbbításához a **21. függelék** szerinti *„**ASZ-10 3. országba való adattovábbítási nyilatkozat”*** megnevezésű dokumentum minta alapján.
5) A Hivatal által nyújtott szolgáltatás igénybevételéhez és a szerződés teljesítéséhez szükséges az 3. országba történő személyes adatok továbbítása. Erről a Hivatal az Adatvédelmi tájékoztatóban az érintettet értesíti, ezért ezekhez a tevékenységekhez az 1)-4) pontban meghatározott feltételeket nem kell teljesíteni.

A 3. országba történő adattovábbítási folyamat előtt a megfelelő biztonsági garanciák ellenőrzését elvégzi: ***Adatvédelmi tisztviselő***

7. OKTATÁS ÉS KÉPZETTSÉGI ELVÁRÁSOK

7.1 Felkészültség

Az Adatvédelmi tisztviselő, az Adatvédelmi manager és az Adatkezelési folyamatgazdák esetében a szükséges szakmai felkészültséget a munkatársak munkaköri leírásában vagy a megbízási szerződésükben kell meghatározni az alábbiak szerint:

Elvárás:

Adatvédelmi tisztviselő képzés:

Több napos, személyes oktatás, amely a felkészíti az Adatvédelmi tisztviselőt munkája elvégzésére.

- GDPR ismeret
- Kötelező adminisztráció elvárások
- Adatkezelési elvek
- Adatkezelés jogalapjai
- Érintett jogai
- Érinett jogainak teljesítési lehetőségei
- Adatvédelemi incidens bejelentése
- Kommunikációs képzés
- Hatósági kommunikáció
- Ellenőrzés, auditálási ismeretek

Adatvédelmi manager esetében:

- legalább két napos adatvédelmi oktatáson való részvétel, jogi diploma, adatvédelmi szakjogász, információbiztonsági, adatvédelmi szakirányú végzettség vagy releváns munkakörben szerzett szakmai tapasztalat,
- rendszeres képzés/önképzés.

Adatkezelési folyamatgazdák estében:

- Évente egy alkalommal a Hivatal által biztosított adatvédelmi oktatáson való részvétel,
- Jelen adatvédelmi szabályzat vonatkozó részeinek ismerete.

A feladatkört ellátó a felkészültséget igazoló dokumentumokat a Hivatal képviselője számára bemutatja.

> *A megfelelő szakirányú végzettség vagy szakmai tapasztalat ellenőrzését elvégzi:* ***HR vezető***

7.2 Tudatosság fenntartása a Hivatalban

A Hivatal felügyelete alatt munkát végző személyeknek tudatában kell lenniük a következőknek:

a) a Hivatal jelen szabályzatban rögzített adatvédelmi elvárásaival,
b) szerepükkel az adatvédelmi rendszer működtetésében,
c) az adatkezelésre vonatkozó szabályok megszegésének lehetséges következményeivel,
d) egy adatvédelmi incidens esetében a riasztási protokollal.

A Hivatal irányítása alatt munkát végző személyeknek rendszeres adatvédelmi tudatossági képzésben kell részesülniük a jelen szabályzat 8.3 pontjában részletezettek szerint.

A tudatosító képzések megszervezéséért felelős: ***Adatvédelmi manager***
Az ellenőrzést elvégzi: ***Adatvédelmi tisztviselő***

8. ADATKEZELÉSI FOLYAMATOK MŰKÖDTETÉSE

A Hivatal a jelen szabályzat hatálybalépésétől kezdődően a 6. pontban megtervezett adatkezelési tevékenységek mentén kezeli a személyes adatokat.

8.1 Adatkezelési tevékenységek feladatmeghatározása

A Hivatal az **Adatvédelmi hatásvizsgálat és kockázat menedzsment szabályzatban** határozza meg azokat az adatkezelési folyamatokat, amelyek magas kockázattal járnak a természetes személyek jogaira.

8.2 Változáskezelés

A Hivatal folyamatosan figyelemmel kíséri az adatkezelési tevékenységeket érintő változásokat:

- Az **Adatvédelmi tisztviselő** feladata, hogy beazonosítsa azokat a **jogszabályi változások**at, valamint az **érdekelt felek elvárásaina**k azon **változásai**t, amelyek hatással lehetnek az adatkezelési tevékenységnek a természetes személyek jogait és szabadságait érintő kockázataira.
- Az adott adatkezelési tevékenységért felelős Adatkezelési folyamatgazda feladata, hogy beazonosítsa azokat a **szervezési és technikai változások**at, amelyek hatással lehetnek az adatkezelési tevékenységnek a természetes személyek jogait és szabadságait érintő kockázataira.
- Az **információbiztonsági felelős** feladata, hogy beazonosítsa azokat a **információbiztonságot érintő** szervezési és technológiai **változások**at, amelyek hatással lehetnek az adatkezelési tevékenységnek a természetes személyek jogait és szabadságait érintő kockázataira.

A Hivatalnak felügyelet alatt kell tartania a tervezett változásokat.

8.3 Adatvédelmi képzés

A Hivatal irányítása alatt munkát végző személyek rendszeres, differenciált adatvédelmi képzésben részesülnek az adatkezeléssel való kapcsolatuk és az ebben rejlő kockázatok alapján.

8.3.1 Képzési tematikák:

Adatvédelmi tisztviselő képzés
Több napos, személyes oktatás, amely a felkészíti az Adatvédelmi tisztviselőt munkája elvégzésére.

- GDPR ismeret
- Kötelező adminisztráció elvárások

- Adatkezelési elvek
- Adatkezelés jogalapjai
- Érintett jogai
- Érintett jogainak teljesítési lehetőségei
- Adatvédelemi incidens bejelentése
- Kommunikációs képzés
- Hatósági kommunikáció
- Ellenőrzés, auditálási ismeretek

Adatvédelmi manager képzés
Legalább két napos, személyes oktatás, amely felkészíti az Adatvédelmi managert munkája elvégzésére.

- GDPR ismeret
- Kötelező adminisztráció elvárások
- Adatkezelési elvek
- Adatkezelés jogalapjai
- Érintett jogai
- Érintett jogainak teljesítési lehetőségei
- Adatvédelemi incidens bejelentése
- Kommunikációs képzés

Adatvédelmi oktatás az Adatkezelési folyamatgazdáknak
Fél napos személyes oktatás, amely felkészíti az Adatkezelési folyamatgazdákat a személyes adatok kezelésével kapcsolatos feladataikra.

- Adatkezelési elvek
- Adatkezelés jogalapjai
- Érintett jogai
- Érintett jogainak teljesítési lehetőségei
- Adatvédelemi incidens hivatalon belüli eszkalációs rendje

Általános adatvédelmi tudatosító képzés
GDPR alapok – elektronikus oktatási anyag
Adatkezelési elvek

- Adatkezelési elvek, jogalapok
- Érintett jogainak teljesítési lehetőségei
- Adatvédelemi incidens Hivatalon belüli eszkalációs rendje

9. AZ ADATKEZELÉSI FOLYAMATOK ÉRTÉKELÉSE

9.1 Folyamatos megfigyelés

A Hivatal tervezett módon belső auditokat végez, annak ellenőrzésére, hogy az adatkezelési folyamatai megfelelnek-e az adatvédelmi szabályzatban foglaltaknak.

A Hivatal Adatvédelmi tisztviselője folyamatosan ellenőrzi az alábbi teljesítmény mutatókat:

- Az Adatkezelési folyamatgazda kollégák 1 hónapja nem fordultak kérdéssel az Adatvédelmi tisztviselőhöz.
- A Hivatal vezető beosztású kollégái 1 hónapja nem jelentettek adatkezelési folyamat változtatást.
- Fél éve nem volt érintetti panaszkezelési igény.
- 1 hónapja nem volt adatvédelmi incidens bejelentés (Notebook, USB eszköz elvesztése stb.).

9.2 Időszakos ellenőrzés

Az Adatvédelmi tisztviselő tervezett módon ellenőrzéseket hajt végre az adatvédelmi szabályozási rendszer működésének megfelelősége érdekében.
Amennyiben a 9.1 pontban megfogalmazott valamely teljesítmény mutató megfigyelésekor eléri a küszöbértéket, az Adatvédelmi tisztviselő késedelem nélkül ellenőrzi az érintett területen a jelen szabályzatban megfogalmazott elvárások teljesülését.
Ezen felül időszakos véletlenszerű mintavételezés alapján ellenőrzést végez negyedévente az alábbi területeken

- Ügyfél által megadott adatok kezelése
- Adatfeldolgozók menedzsmentje

9.3 Belső audit

A Hivatal tervezett módon belső auditokat végez, annak ellenőrzésére, hogy az adatkezelési folyamatai megfelelnek-e a jogszabályi elvárásoknak és a Hivatal saját követelményeinek.
Az adatkezelési folyamatok ellenőrzését, a belső auditot a Hivatal jelentős szervezeti átalakítását követően, a külső tényezők kockázatai, a szabályozási környezet változása esetén, de legalább évente egy alakalommal el kell végezni.
Az auditok elvégezhetők mind külső, mind belső erőforrásokkal. Az audit lebonyolítását vagy a külső erőforrás bevonásával való megvalósítását az Adatvédelmi tisztviselő végzi el.
A Hivatal a belső auditok során feltárt hiányosságokat jegyzőkönyvben rögzíti.
Az auditokat az auditálásra vonatkozó szakmai ajánlások szerint kell elvégezni, és az eredményeket dokumentált információként meg kell őrizni.

10.AZ ADATKEZELÉSI FOLYAMATOK BIZTONSÁGÁNAK FEJLESZTÉSE

Az adatvédelmi szabályozási rendszer működtetése során a Hivatal elvégzi a következő elemzéseket:

- adatvédelmi kockázatelemzés,
- információbiztonsági kockázatelemzés és
- az incidensek elemzése.

E tevékenységek során feltárt nem megfelelő működések kijavítására a Hivatal intézkedéseket hoz, felelőst rendel hozzá, meghatározza a teljesítési határidőt.
Az adatvédelmi szabályozási rendszer állapotáról, a fejlesztési lehetőségekről a következő forrásokból kap információt a Hivatal:

- belső auditok,
- belső ellenőri vizsgálat,
- harmadik fél auditja,

- jelentések az adatvédelmi és információbiztonsági gyengeségekről,
- hatósági iránymutatások,
- adatvédelmi incidensek.

A megszerzett információkat és a fejlesztési lehetőségeket a Hivatal évente legalább egy alkalommal egy vezetőségi vizsgálat keretében felülvizsgálja, és meghatározza a szükséges javító intézkedéseket, amelyek végrehajtását nyomon követi.

Az évenkénti vezetőségi felülvizsgálatra az Adatvédelmi tisztviselő a fenti információk alapján előterjesztést készít.

A vezetőségi felülvizsgálat évenkénti megszervezéséért a felelős: ***Adatvédelmi manager***
Az ellenőrzést elvégzi: ***Adatvédelmi tisztviselő***

11. ZÁRÓ RENDELKEZÉSEK

Jelen szabályzat a közzétételét követő napon lép hatályba.

Budapest, 2021. szeptember 15.

Szaniszló Sándor	**dr. Ronyecz Róbert**
polgármester	**jegyző**

A 17/2021. (IX.15.) polgármesteri-jegyzői együttes utasítással kiadott, 2021. szeptember 16-tól hatályos Adatvédelmi és adatkezelési szabályzat mellékletei és függelékei külön mappában megtalálhatóak