Budapest Főváros XII. kerület Hegyvidéki Polgármesteri Hivatal és Budapest Főváros XII. kerület Hegyvidéki Önkormányzat Adatvédelmi és Adatkezelési Szabályzata

1. Bevezetés és a Szabályzat célja

Jelen szabályzat célja, hogy meghatározza a Budapest Főváros XII. kerület Hegyvidéki Polgármesteri Hivatal (a továbbiakban: Hivatal) és Budapest Főváros XII. kerület Hegyvidéki Önkormányzat (a továbbiakban: Önkormányzat) által végzett adatkezelések során alkalmazandó adatvédelmi és adatbiztonsági elveket és szabályokat. Célja továbbá az információs önrendelkezési jog és az adatbiztonság érvényesítése, a személyes adatok védelme, valamint elsősorban az Európai Parlament és a Tanács (EU) 2016/679 természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló rendelete (általános adatvédelmi rendelet, a továbbiakban: GDPR), az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.), és a további jogszabályok előírásainak való megfelelés biztosítása.

2. Értelmező rendelkezések

Személyes adat: az érintettel kapcsolatba hozható adat – különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés.

Adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolás vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése.

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.

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

Érintett: bármely információ alapján azonosított vagy azonosítható természetes személy.

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

Adatvédelmi tisztviselő: az a személy, akit az adatkezelő jelölt ki a GDPR 37. cikkével összhangban, és akinek feladata az adatvédelmi jogszabályoknak való megfelelés ellenőrzése és tanácsadás nyújtása.

3. Az adatkezelés alapelvei

A Hivatal és az Önkormányzat a személyes adatok kezelése során az alábbi alapelveket érvényesíti:

Jogszerűség, tisztességes eljárás és átláthatóság: a 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 történhet.

Adattakarékosság: az adatkezelés céljai szempontjából megfelelő és releváns, és a szükségesre korlátozódik.

Pontosság: az adatoknak pontosnak és naprakésznek kell lenniük. A pontatlan személyes adatokat haladéktalanul törölni vagy helyesbíteni kell.

Korlátozott tárolhatóság: a személyes adatok tárolása olyan formában, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé.

Integritás és bizalmas jelleg: a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelem, ideértve az adatok titkosságát is.

Elszámoltathatóság: az adatkezelő felelős a fenti alapelveknek való megfelelésért, és képesnek kell lennie e megfelelés igazolására.

4. Az Adatkezelők

Adatkezelő megnevezése: Budapest Főváros XII. kerület Hegyvidéki Polgármesteri Hivatal

Székhelye: 1126 Budapest, Böszörményi út 23–25.

Képviselője: dr. Bitskey Botond, jegyző

Adatkezelő megnevezése: Budapest Főváros XII. kerület Hegyvidéki Önkormányzat

Székhelye: 1126 Budapest, Böszörményi út 23–25.

Képviselője: Kovács Gergely, polgármester

Adatvédelmi tisztviselő: dr. Zsille Katalin Lenke

Elérhetősége: gdpr@hegyvidek.hu

5. Az adatkezelések jogszerűsége és céljai

Az Adatkezelők kizárólag olyan személyes adatokat kezelnek, amelyek kezelésére jogszerű jogalappal rendelkezik. Az adatkezelés jogalapja lehet:

- jogszabályi kötelezettség: (pl. kötelező feladatellátás, adózás, szociális juttatások),

- szerződés teljesítése: (pl. munkaviszony, bérleti szerződés),

- érintett hozzájárulása: (pl. hírlevél feliratkozás, rendezvényekre jelentkezés),

- létfontosságú érdek védelme: (pl. vészhelyzet esetén),

- közérdek vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása,

- az Adatkezelők jogos érdeke.

6. Az adatkezelés folyamata és az adatok kezelése

Az Adatkezelők biztosítják, hogy az adatkezelés minden fázisa jogszerű és az adatvédelmi elveknek megfelelő legyen.

Adatgyűjtés: csak a szükséges adatok gyűjtése, megfelelő jogalap alapján, az érintettek megfelelő tájékoztatása mellett.

Adattárolás:

- személyes adatok tárolása biztonságos, zárt helyen (fizikai adatok) vagy védett informatikai rendszereken (digitális adatok),

- az adatokhoz való hozzáférés korlátozása, csak az arra jogosult munkatársak részére,

- adatok rendszeres mentése.

Adatfelhasználás: az adatok kizárólag a meghatározott célra használhatók fel.

Adattovábbítás: személyes adatok csak akkor továbbíthatók harmadik fél részére, ha arra jogszabály kötelez, az érintett hozzájárul, vagy az adatkezelés céljához elengedhetetlen (pl. adatfeldolgozó részére, szerződés alapján). Az adatátadásról nyilvántartást kell vezetni.

Adatok törlése, megsemmisítése: az adatok törlése vagy megsemmisítése az adatkezelés céljának megszűnésével vagy a jogszabályban előírt tárolási idő lejártával.

7. Adatfeldolgozók

Amennyiben az Adatkezelők adatfeldolgozót vesznek igénybe (pl. informatikai szolgáltató, könyvelő), az adatfeldolgozással kapcsolatos jogokat és kötelezettségeket írásbeli szerződésben kell rögzíteni a GDPR 28. cikkének megfelelően. Az adatfeldolgozó kizárólag az Adatkezelők utasításai szerint járhat el, és köteles biztosítani az adatok megfelelő biztonságát.

8. Az érintettek jogai

Az Adatkezelők biztosítják az érintettek GDPR-ban foglalt jogainak gyakorlását:

Tájékoztatáshoz való jog: Az érintett kérésére tájékoztatást ad az érintett általa kezelt, illetve az általa vagy rendelkezése szerint megbízott adatfeldolgozó által feldolgozott adatairól, azok forrásáról, az adatkezelés céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, címéről és az adatkezeléssel összefüggő tevékenységéről, továbbá – az érintett személyes adatainak továbbítása esetén – az adattovábbítás jogalapjáról és címzettjéről.

Hozzáférés joga: Az érintett jogosult visszajelzést kapni arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha igen, hozzáférést kapni a személyes adatokhoz és a kapcsolódó információkhoz.

Helyesbítés joga: Az érintett kérheti a pontatlan személyes adatok helyesbítését, vagy a hiányos adatok kiegészítését.

Törléshez való jog: Az érintett jogosult arra, hogy kérésére az Adatkezelők indokolatlan késedelem nélkül töröljék a rá vonatkozó személyes adatokat bizonyos feltételek fennállása esetén.

Adatkezelés korlátozásához való jog: Az érintett jogosult arra, hogy kérésére az Adatkezelők korlátozzák az adatkezelést bizonyos feltételek fennállása esetén.

Adathordozhatósághoz való jog: Az érintett jogosult arra, hogy a rá vonatkozó, általa az Adatkezelők rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formában megkapja, és ezeket az adatokat egy másik adatkezelőnek továbbítsa.

Tiltakozáshoz való jog: Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból bármikor tiltakozzon személyes adatainak kezelése ellen.

Automatizált döntéshozatal egyedi ügyekben, beleértve a profilalkotást: Az érintett jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntés hatálya, amely rá nézve joghatással járna vagy őt hasonlóképpen jelentős mértékben érintené.

Panaszjog: Az érintett panaszt tehet a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (cím: 1055 Budapest, Falk Miksa utca 9–11., postacím: 1363 Budapest, Pf.: 9., telefon: +36 1 391 1400, fax: +36 1 391 1410, e-mail: ugyfelszolgalat@naih.hu, web: www.naih.hu).

Bírósági jogorvoslathoz való jog: Az érintett jogosult bírósági jogorvoslatra, ha úgy ítéli meg, hogy a személyes adataival kapcsolatos jogait megsértették.

Az Adatkezelő indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról az adatkezelő a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet.

9. Adatbiztonság

Az Adatkezelő az adatkezelés biztonságát szolgáló technikai és szervezési intézkedéseket hoz az adatok jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

Technikai intézkedések (példák):

Jelszavas védelem (komplex jelszavak, rendszeres változtatás).

Hálózati biztonság (tűzfalak, vírusvédelem).

Hozzáférési jogosultságok kezelése (csak a szükséges hozzáférés biztosítása a munkatársaknak).

Rendszeres biztonsági mentések.

Titkosítás (érzékeny adatok esetén).

Fizikai biztonság (zárható irodák, irattárak).

Szervezési intézkedések (példák):

Adatkezelési feladat- és felelősségi körök pontos meghatározása.

Adatvédelmi incidens kezelési eljárás.

Rendszeres felülvizsgálat és audit.

10. Adatvédelmi incidensek kezelése

Az Önkormányzat az adatvédelmi incidenseket haladéktalanul kezeli a következő eljárásrend szerint:

Incidens észlelése: Bármely munkatárs köteles haladéktalanul jelenteni az adatvédelmi tisztviselőnek az észlelt incidenst.

Incidens kivizsgálása: Az incidens körülményeinek, hatásainak és az érintettek körének felmérése.

Bejelentés a NAIH felé: Ha az incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Adatkezelő 72 órán belül bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnál (NAIH). A NAIH felé tett bejelentés az alábbi információkat tartalmazza:

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

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

c) az adatvédelmi incidensből eredő, valószínűsíthető következmények ismertetését;

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

Amennyiben az összes információt nem lehetséges egyidejűleg szolgáltatni, azok indokolatlan késedelem nélkül, szakaszosan is közölhetők.

Érintettek tájékoztatása: Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Önkormányzat indokolatlan késedelem nélkül tájékoztatja az érintetteket az incidensről. Nem szükséges az érintetteket tájékoztatni, amennyiben a következő feltételek bármelyike teljesül:

a) az Adatkezelő megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;

b) az Adatkezelő az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;

c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé.

Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását

Incidens kezelése és intézkedések: Az incidens elhárítása, a további incidensek megelőzése érdekében szükséges intézkedések megtétele.

Nyilvántartás vezetése: Az Adatkezelő nyilvántartást vezet az adatvédelmi incidensekről. z incidensekről vezetett nyilvántartás tartalmazza az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket, lehetővé téve ezáltal a felügyeleti hatóság számára az e cikk követelményeinek való megfelelés ellenőrzését.

11. Adatvédelmi hatásvizsgálat

Amennyiben egy tervezett adatkezelési művelet – különösen új technológiák alkalmazása, vagy jellegére, hatókörére, körülményeire és céljaira tekintettel – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Adatkezelő az adatkezelés megkezdése előtt adatvédelmi hatásvizsgálatot (a továbbiakban: hatásvizsgálat) végez. A magas kockázat fennállását különösen a GDPR 35. cikk (3) bekezdésében, valamint a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) által közzétett, kötelezően hatásvizsgálat-köteles műveletek listájában foglaltak alapján kell besorolni.

A hatásvizsgálatnak a GDPR 35. cikk (7) bekezdése alapján legalább az alábbiakat kell tartalmaznia:
a) a tervezett adatkezelési műveletek és célok rendszerezett leírása;

b) a műveletek szükségességének és arányosságának vizsgálata;

c) az érintettek jogait és szabadságait érintő kockázatok értékelése;

d) a kockázatok kezelésére, a személyes adatok védelmének biztosítására és a megfelelés igazolására tervezett intézkedések, garanciák és mechanizmusok.

Ha a hatásvizsgálat megállapítja, hogy az adatkezelés az Adatkezelő által a kockázatok mérséklésére tett intézkedések nélkül magas kockázattal járna, az Adatkezelő a GDPR 36. cikke alapján az adatkezelés megkezdése előtt előzetes konzultációt kezdeményez a NAIH-nál.

12. A szabályzat felülvizsgálata és módosítása

Jelen szabályzat felülvizsgálatára legalább évente egyszer, vagy jogszabályi változások, technikai fejlődés, illetve az Adatkezelő adatkezelési gyakorlatának változása esetén kerül sor. A módosításokról az érintett munkatársakat tájékoztatni kell.

13. Záró rendelkezések

A jelen szabályzatban nem szabályozott kérdésekben a GDPR, az Infotv. és egyéb vonatkozó jogszabályok rendelkezései az irányadóak.

Kelt: Budapest Hegyvidék, 2025. 07. 28.