

TÖRZSPÉLDÁNY



Budapest Főváros XV. Kerület Önkormányzata
Polgármesterének és Jegyzőjének

5/2023. (V. 31.) számú

UTASÍTÁSA

a személyes adatok kezeléséről és védelméről

TARTALOMJEGYZÉK

I. BEVEZETÉS.....	1
I.1. RELEVÁNS ELŐÍRÁSOK	1
I.2. AZ UTASÍTÁS CÉLJA, TÁRGYA, HATÁLYA	1
I.3. ADATVÉDELMI TISZTVISELŐ.....	1
II. ÁLTALÁNOS RENDELKEZÉSEK.....	3
II.1. FOGALOMMAGYARÁZAT	3
II.2. ADATVÉDELMI ALAPELVEK.....	3
II.3. ADATKEZELÉS JOGALAPJA	4
III. JOGSZABÁLYI MEGFELELÉS MIBENLÉTE.....	5
III.1. A HIVATAL ÁLTALÁNOS FELADATAI A MEGFELELŐ ADATVÉDELEM ÉRDEKÉBEN	5
III.2. ADATKEZELÉSEK SZABÁLYOZÁSA, INTÉZKEDÉSEK MEGHATÁROZÁSA	6
III.3. AZ ADATVÉDELEM SZERVEZETE	7
III.3.1. A jegyző.....	7
III.3.2. Az adatvédelmi tisztviselő.....	7
III.3.3. A szervezeti egység vezetője	8
III.3.4. A Hivatal munkatársai	9
III.4. A HIVATAL KÖTELEZETTSÉGEINEK LISTÁJA.....	10
III.4.1. Nyilvántartásvezetés	10
III.4.2. Átláthatósági intézkedések	10
III.4.2.1. Tájékoztatás.....	10
III.4.2.2. Joggyakorlás elősegítése	10
III.4.3. Adatbiztonság	10
III.4.3.1. Fizikai védelem	11
III.4.3.2. Logikai védelem	11
III.4.3.3. Adatvédelmi hatásvizsgálat elvégzése.....	11
III.4.3.4. Adatvédelmi incidensek kezelése.....	12
III.4.4. Adatvédelmi tudatosság.....	12
III.4.4.1. Adatvédelmi tisztviselő kijelölése.....	12
III.4.4.2. Utasítás megismerése	12
III.4.4.3. Partneri megállapodások felülvizsgálata	12
III.4.4.4. Adatvédelmi tudatosság	12
IV. AZ ÉRINTETTEK ADATKEZELÉSSSEL KAPCSOLATOS JOGAI	13
IV.1. TÁJÉKOZTATÁS KÉRÉSE	13
IV.2. AZ ADATOK HELYESBÍTÉSE, KIEGÉSZÍTÉSE	13
IV.3. AZ ÉRINTETT TILTAKOZÁSI JOGA.....	13
IV.4. AZ ADATOK TÖRLÉSE	14
IV.5. AZ ELFELEDTETÉSHEZ VALÓ JOG	14
IV.6. AZ ADATKEZELŐ EGYÉB INTÉZKEDÉSI KÖTELEZETTSÉGE.....	14
IV.7. AZ ADATKEZELÉS KORLÁTOZÁSA.....	14
IV.8. ADATHORDOZHATÓSÁGHOZ VALÓ JOG	15
V. ZÁRÓ RENDELKEZÉSEK	16

VI. MELLÉKLETEK	17
1. MELLÉKLET	18
ADATKEZELŐI KÖTELEZETTSÉGEK.....	18
2. MELLÉKLET	19
ELJÁRÁSREND ÉRINTETTI MEGKERESÉSEK ESETÉN	19
3. MELLÉKLET	21
ELJÁRÁSREND ADATVÉDELMI INCIDENSEK ESETÉRE	21
3.1. <i>Tájékoztató adatvédelmi incidensekről érintettek részére</i>	25
3.2. <i>Adatvédelmi incidensek nyilvántartása</i>	27

I. Bevezető rendelkezések

I.1. Releváns előírások

Budapest Főváros XV. Kerület Önkormányzata és Polgármesteri Hivatala, mint adatkezelő (a továbbiakban együtt: „Hivatal”, vagy „Adatkezelő”) személyes adatok kezelésével kapcsolatos gyakorlatát és működését az alábbiakra figyelemmel határozza meg:

- 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 szóló, az Európai Parlament és a Tanács által 2016. április 27. napján elfogadott és 2018. május 25. napjától alkalmazandó általános adatvédelmi rendelet (a továbbiakban: „GDPR”),
- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: „Infotv.”),
- a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: „NAIH”), valamint az Európai Adatvédelmi Testület (a továbbiakban: „EPDB”) iránymutatásai, ajánlásai.

I.2. Az utasítás célja, tárgya, hatálya

A jelen utasítás célja, hogy rögzítse az Adatkezelő által alkalmazott adatvédelmi elveket, szabályokat, valamint bizonyos belső előírásokat. Az utasítás kiadásának célja továbbá, hogy megismerésével és betartásával azon személyek, akikre az utasítás hatálya kiterjed, képesek legyenek az érintettek (azon személyek, akiknek személyes adatai a Hivatal és az Önkormányzat kezeli) személyes adatainak kezelését a fenti előírásoknak megfelelően végezni.

Az utasítás hatálya kiterjed a Budapest Főváros XV. kerületi Önkormányzat, a Nemzetiségi Önkormányzatok és a Budapest Főváros XV. kerületi Önkormányzat Polgármesteri Hivatala (a továbbiakban együtt: Hivatal) teljes körű feladat- és hatáskörének ellátására, illetve az Önkormányzat tisztségviselőire (polgármester, alpolgármesterek) és az önkormányzati képviselőkre, valamint Hivatalban foglalkoztatott valamennyi dolgozóra, függetlenül a foglalkoztatás formájától (köztisztviselő, ügykezelő, munkavállaló, egyéb foglalkoztatott).

Az utasítás hatálya kiterjed a Hivatal minden adatkezelésére és adatfeldolgozására, amely természetes személy személyes adataira vonatkozik.

Az informatikai biztonságra vonatkozó szabályokat a Polgármesteri Hivatal Informatikai Biztonsági Szabályzatának kiadásáról szóló 12/2019. (VIII.29.) polgármesteri és jegyzői együttes utasítás állapítja meg; jelen utasítás rendelkezéseit az IBSZ rendelkezéseivel összhangban kell alkalmazni.

I.3. Adatvédelmi tisztviselő

Az Európai Unió hatósági iránymutatások szerint az adatvédelmi tisztviselő az elszámoltathatóság sarokköve, és az adatvédelmi tisztviselő kijelölése elősegítheti a jogszabályoknak való megfelelést. Az elszámoltathatóság eszközeinek (például az adatvédelmi hatásvizsgálatok megkönnyítése, auditok végzése vagy elősegítése)

végrehajtása mellett az adatvédelmi tisztviselők közvetítő szerepet töltenek be az érdekelt felek (például a felügyeleti hatóságok, az érintettek és a Hivatalon belüli részlegek) között.

A GDPR értelmében bizonyos adatkezelők és adatfeldolgozók kötelesek adatvédelmi tisztviselőt (DPO) kijelölni. Ez a kötelezettség kiterjed

- a) minden közhatalmi szervre vagy egyéb, közfeladatot ellátó szervre (függetlenül attól, hogy milyen adatokat dolgoz fel), valamint
- b) egyéb olyan szervezetekre, amelyek fő tevékenysége az egyének szisztematikus, nagymértékű megfigyelése, vagy
- c) amelyek a személyes adatok különleges kategóriáit nagy számban kezelik.

A fenti vagylagos kategóriák közül az a) pont feltételei fennállnak a Hivatal esetében, mivel közfeladatot ellátó szerv, így a DPO kinevezése kötelező a GDPR alapján.

Adatvédelmi tisztviselő neve: Dr. Miklós Péter

Adatvédelmi tisztviselő elérhetősége: adatvedelmi.tisztviselo@bpxv.hu

II. Általános rendelkezések

II.1. Fogalommagyarázat

Az utasítás alkalmazása során használt fogalmak – figyelemmel a jogalkotásról szóló 2010. évi CXXX. törvény (Jat.) 24. § (2) bekezdésére – az Infotv., illetve a GDPR szövegezése szerint vehetők figyelembe.

II.2. Adatvédelmi alapelvek

A GDPR 5. cikke tartalmazza az alábbiakban leírandó adatkezelési elveket. Jelentőségük abban áll, hogy minden, adatkezeléshez kapcsolódó tevékenység során ezeknek a kiemelt figyelembevételével kell eljárnia Az utasítás hatálya alá tartozó személyeknek. Ha magasabb az adatvédelmi tudatosság, kevesebb kockázat rejlik a Hivatal működésében. Emellett a lenti elveknek való megfelelés biztosítása, illetve ennek bizonyítása az elszámoltathatóság elve alapján a Hivatal kötelezettsége.

- a) Jogszerűség, tisztességes eljárás és átláthatóság: a személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.
- b) Célhoz kötöttség: a személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon. Nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.
- c) Adattakarékosság: a személyes adatoknak az adatkezelés céljai szempontjából megfelelőnek és relevánsnak kell lenniük, és a szükségesre kell korlátozódniuk.
- d) Pontosság: a személyes adatoknak pontosnak és szükség esetén naprakésznek kell lenniük. Minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék.
- e) Korlátozott tárolhatóság: a 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 közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel.
- f) Integritás és bizalmas jelleg: a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.

II.3. Adatkezelés jogalapja

Személyes adat kizárólag az alábbi, a GDPR 6. cikk (1) bekezdésében rögzített esetek valamelyikének teljesülésekor kezelhető jogszerűen:

- 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, vagy
- 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 Hivatal tevékenységéből adódóan az adatkezelések jellemzően közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladatok végrehajtásához (például az egyes hatósági eljárások során az ügyfelek személyes adatainak kezelése), valamint az Adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez (például munkatársak személyes adatainak rögzítése a foglalkoztatás bejelentéséhez az adóhatóság felé) szükségesek. Emellett magánszemélyekkel kötött szerződések esetében az adatkezelés szerződéskötéshez, vagy szerződés teljesítéséhez szükséges.

III. Jogszabályi megfelelés mibenléte

A személyes adatok kezelésével és védelmével kapcsolatos jogszabályi előírásokhoz való megfelelés egy lépcsőzetes folyamat, melynek során jogi és informatikai ismereteket felhasználva, a Hivatal vezetésével folyamatosan együttműködve kell elvégezni a szükséges feladatokat.

Az utasítás I.1. pontjában rögzített előírásoknak való megfeleléshez szükséges intézkedések, kötelezettségek összesítése:

III.1. A Hivatal általános feladatai a megfelelő adatvédelem érdekében

- a) Az adatvédelmi tudatosság: Biztosítani kell a szakmai felkészültséget a jogszabályoknak való megfeleléshez. Elengedhetetlen a munkatársak szakmai felkészítése és az utasításban foglaltak megismerése.
- b) Át kell tekinteni valamennyi adatkezelés célját, szempontrendszerét, a személyes adatkezelés koncepcióját. Az utasítással összhangban kell biztosítani jogszerű adatkezelést.
- c) Az érintett személyeknek nyújtott tájékoztatás tömör, könnyen hozzáférhető és érthető legyen, ezért azt világos és közérthető nyelven kell megfogalmazni és megjeleníteni.
- d) Az átlátható adatkezelés követelménye, hogy az érintett személy tájékoztatást kapjon az adatkezelés tényéről és céljairól. A tájékoztatást az adatkezelés megkezdése előtt kell megadni és a tájékoztatáshoz való jog az adatkezelés során annak megszűnéséig megilleti az érintettet.
- e) Az adatkezelő indokolatlan késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható.

III.2. Adatkezelések szabályozása, intézkedések meghatározása

A Hivatal ügyfelei és partnerei (természetes személyek, vagy jogi személyek képviselői) személyes adatai kezelésének leírása külön tájékoztatókban, vagy a felek közötti jogviszonyt szabályozó dokumentumokban (például szerződés, jogi közlemény, egyéb nyilatkozat) rögzítendő.

Az utasítás hatálya alá tartozó érintettek személyes adatai kezelésének leírása külön adatkezelési tájékoztatóban, vagy a felek közötti jogviszonyt szabályozó dokumentumban (például szerződés, jogi közlemény, egyéb nyilatkozat) rögzítendő.

Az utasítás hatálya alá nem tartozó külső személyek (például vállalkozók, partnerek) által végzett adatkezeléseket a felek közötti adatfeldolgozói szerződésekben, illetve közös vagy egyedi adatkezelői megállapodásokban szükséges szabályozni, amelyek szükség szerint belefoglalhatók a felek között már meglévő szerződésekbe.

A Hivatal köteles belső szabályozást alkotni, amennyiben a személyes adatok kezelése és védelme szempontjából indokolt egy adott tárgykörben (például kamerarendszer működtetése).

Figyelemmel az Infotv. 5. § (5) bekezdésére, a Hivatal – ha a kötelező adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát törvény, helyi önkormányzat rendelete vagy az Európai Unió kötelező jogi aktusa nem határozza meg – az adott adatkezelés megkezdésétől legalább háromévente felülvizsgálja, hogy az általa, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adat kezelése az adatkezelés céljának megvalósulásához szükséges-e.

Az adatkezelésekkel kapcsolatos szabályozás, vagy intézkedések szükségességével kapcsolatban a Hivatal köteles rendszeresen egyeztetni az adatvédelmi tisztviselővel.

III.3. Az Adatvédelem szervezete

III.3.1. A jegyző

A személyes adatok védelméért, az adatkezelés jogszerűségéért a jegyző a felel, aki

- a) kiadja az adatvédelmi és adatbiztonsági tárgyú szabályzatokat,
- b) felügyeli a szabályzatok, illetve az adatvédelemre vonatkozó jogszabályok érvényesülését,
- c) adatvédelmi tisztviselőt nevez ki az adatkezelése jogszerűségének biztosítása érdekében,
- d) engedélyezi a munkakör ellátásához szükséges informatikai alkalmazásokhoz való hozzáférési jogosultságot és annak terjedelmét.

III.3.2. Az adatvédelmi tisztviselő

- a) vezeti az adatkezelési tevékenységekre vonatkozóan a GDPR 30. cikk szerinti nyilvántartást,
- b) előkészíti és folyamatosan felülvizsgálja az általános adatvédelmi szabályzatot és további adatvédelmi tárgyú szabályzatokat, gondoskodik azok jogszabályváltozásokkal összefüggő szükséges módosításáról, kiegészítéséről,
- c) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, véleményezi az adatvédelemmel kapcsolatos előterjesztéseket, valamint döntéseket,
- d) elemzi és ellenőrzi az adatkezelési tevékenységek megfelelőségét és részt vesz az adatvédelmi ellenőrzésekben és vizsgálatokban,
- e) megszervezi a munkatársak adatvédelmi tárgyú oktatását,
- f) az adatvédelmi jogszabályi változások és a gyakorlati tapasztalatok alapján javaslatokat készít az adatkezelő szabályzatainak módosítására és szükség esetén kezdeményezi új szabályzatok kibocsátását,
- g) közreműködik az adatkezelési tájékoztatók elkészítésében,
- h) konkrét ügyekben felmerülő igények alapján adatvédelmi kérdésekben segítséget nyújt a Hivatal munkatársai részére,
- i) kivizsgálja a személyes adatok kezelésével (feldolgozásával, továbbításával) kapcsolatban hozzá érkezett bejelentéseket és panaszokat,
- j) a tudomására jutott Hivatalon belüli visszásság esetén felhívja az érintett munkatársat a jogosulatlan adatkezelés megszüntetésére, illetve kezdeményezi az arra jogosultak intézkedését,
- k) ügyintézőként közreműködik a kötelezően közzéteendő adatok nyilvánosságra hozatalának és a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló külön szabályzat rendelkezései szerint az írásban benyújtott közérdekű adatigénylések teljesítésében,
- l) vezeti a közérdekű adatigénylések elutasítására vonatkozóan az Infotv. 30. § (3) bekezdése szerinti nyilvántartást,

- m) az előző évi elutasított közérdekű adatigénylésekről minden év január 31. napjáig tájékoztatást küld a felügyeleti hatóság részére,
- n) vezeti az adatvédelmi incidensekre vonatkozó nyilvántartást és annak tartalmáról az érintett részére jogszabály alapján vagy az érintett kérelmére tájékoztatást ad,
- o) közreműködik az adatvédelmi incidensekkel kapcsolatos feladatok végrehajtásában (az adatvédelmi incidens kivizsgálását és elhárítását végző szakértői csapat felállítása, az incidens kivizsgálása, a felügyeleti hatóság felé bejelentés, kárelhárítás, új intézkedések bevezetése stb.),
- p) együttműködik és – szükség esetén – konzultál a felügyeleti hatósággal,
- q) megválaszolja a felügyeleti hatóság, a bíróságok és a hatóságok adatvédelmi tárgyú megkereséseit, valamint az érintettek kéréseit és beadványait a jogszabályban, illetve a határozatokban meghatározott időn belül, illetve azok alapján intézkedéseket foganatosít.
- r) közreműködik az adatvédelmi hatásvizsgálatok megtervezésében és végrehajtásában,
- s) vezeti az érintettek kérelmének elutasítására vonatkozó nyilvántartást.

III.3.3. A szervezeti egység vezetője

A szervezeti egység vezetője személyesen felel az irányítása alá tartozó szervezeti egységnél az adatkezelés jogszerűségéért, ennek körében

- a) kezdeményezi a jegyzőnél a szervezeti egységnél vezetett egyes adatállományok vonatkozásában a munkatársak hozzáférési jogosultságának beállítását, módosítását, törlését;
- b) biztosítja a szervezeti egység működése körében keletkezett információk törvényességét, alaposságát, pontosságát, teljességét, sérthetetlenségét,
- c) biztosítja a kezelt adatok megóvását a jogosulatlan hozzáférés, módosítás vagy nyilvánosságra hozatal ellen, megakadályozza a kezelt adatok jogosulatlan törlését, illetve minden fajta fizikai megsemmisülését, jogosulatlan megsemmisítését;
- d) felügyeli a szervezeti egység ügyviteléhez és feladatköréhez kapcsolódó nyilvántartások vezetését; felel a szervezeti egységnél vezetett, az egység felelősségi körébe tartozó adattovábbításokra és az adatfeldolgozókra vonatkozó nyilvántartások naprakésztségéért,
- e) a természetes személyek jogaira és szabadságaira nézve valószínűsíthetően magas kockázattal járó adatkezelés megkezdése előtt az adatvédelmi tisztviselő véleményét kéri adatvédelmi hatásvizsgálat lefolytatásának a szükségességéről, szükség esetén az adatvédelmi tisztviselő bevonásával lebonyolítja az adatvédelmi hatásvizsgálatot,
- f) haladéktalanul tájékoztatja a jegyzőt az esetleges jogellenes adatkezelés feltárásáról, illetve megteszi a jogellenesség megszüntetése iránti intézkedéseket és intézkedik a jogellenes adatkezelés folytán esetleg bekövetkező kárenyhítés és kárelhárítás érdekében,
- g) felel az érintetti jogok teljesítéséért, biztosítja az érintett személyes adataira vonatkozó adatigénylésének, az adatai helyesbítésére, törlésére, zárolására, adathordozhatóságra irányuló kérelmének jogszerű teljesítését,
- h) biztosítja a szóban benyújtott közérdekű adatigénylések jogszerű teljesítését, illetve az írásban benyújtott közérdekű adatigénylésekre adott válaszoknak a kötelezően közzeendő

adatok nyilvánosságra hozatalának és a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló külön szabályzat rendelkezései szerinti előkészítését,

i) adatot szolgáltat az adatvédelmi tisztviselő részére a felügyeleti hatóság felé a közérdekű adatigénylések elutasítására vonatkozó bejelentési kötelezettség teljesítéséhez,

j) haladéktalanul tájékoztatja a jegyzőt és az adatvédelmi tisztviselőt az esetleges tudomására jutott adatvédelmi incidensről, illetve megteszi annak megszüntetése iránti, illetve a kárenyhítés és kárelhárítás érdekében szükséges intézkedéseket,

k) szükség esetén részt vesz az adatvédelmi incidens kivizsgálásában és elhárításában, illetve az adatvédelmi incidens kivizsgálását és elhárítását végző szakértői csapat munkájában.

III.3.4. A Hivatal munkatársai

Valamennyi munkatárs köteles

a) a GDPR, az Infotv. és az ágazati jogszabályok, valamint jelen utasítás adatvédelmi előírásait megismerni és maradéktalanul betartani,

b) előzetesen egyeztetni az adatvédelmi tisztviselővel a személyes adatok kezelését vagy a közérdekű adatok nyilvánosságát érintő ügyekben,

c) a munkaköri leírásban foglalt szerint részt venni az adattovábbítási és az adatfeldolgozó nyilvántartások vezetésében,

d) haladéktalanul tájékoztatni közvetlen vezetőjét a tudomására jutott jogellenes adatkezelésről vagy bekövetkezett adatvédelmi incidensről és a közvetlen vezető, továbbá az adatvédelmi tisztviselő iránymutatása szerint közreműködni az adatvédelmi incidensek kivizsgálásában és azok, illetve következményeik elhárításában, az esetleges károk enyhítésében,

e) szükség esetén részt venni az adatvédelmi incidens kivizsgálását és elhárítását végző szakértői csapat munkájában,

f) észrevétel esetén az adatkezeléssel kapcsolatosan feltárt visszásságot haladéktalanul megszüntetni,

g) teljesíteni az érintett személyes adataira vonatkozó kérelmeket, illetve a közérdekű adatok megismerésére irányuló szóbeli kérelmeket a kötelezően közzéteendő adatok nyilvánosságra hozatalának és a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló külön szabályzat rendelkezései szerint,

h) adatot szolgáltatni az írásban benyújtott közérdekű adatigényléshez és az éves adatvédelmi jelentéshez az adatvédelemi ügyintéző által megjelölt határidő figyelembevételével a kötelezően közzéteendő adatok nyilvánosságra hozatalának és a közérdekű adatok megismerésére irányuló igények teljesítésének rendjéről szóló külön szabályzat rendelkezései szerint,

i) haladéktalanul tájékoztatni közvetlen vezetőjét a feladatkörében felmerült bármely adatvédelmi problémáról, esetleges visszásság észleléséről.

III.4. A Hivatal kötelezettségeinek listája

A Hivatalnak, mint adatkezelőnek a személyes adatok kezelésével és védelmével kapcsolatos megfeleléséhez szükséges kötelezettségekkel járó, 1. mellékletben rögzített intézkedései az alábbiak:

III.4.1. Nyilvántartásvezetés

A Hivatal köteles a GDPR 30. cikke szerinti adatkezelési nyilvántartást vezetni felelősségi körébe tartozó adatkezelési tevékenységekről. A Hivatal adatvédelmi tisztviselője a nyilvántartást elektronikus formában vezeti.

III.4.2. Átláthatósági intézkedések

III.4.2.1. Tájékoztatás

A Hivatal – az adatvédelmi tisztviselő javaslata alapján és közreműködésével – köteles valamennyi – az utasítás hatálya alá tartozó és a Hivatallal kapcsolatba kerülő, az utasítás hatálya alá nem tartozó érintett részére az adatkezelés egyedi körülményeinek függvényében – a GDPR 13. vagy 14. cikkében meghatározottak szerint tájékoztatást nyújtani.

III.4.2.2. Joggyakorlás elősegítése

A Hivatal a GDPR 15-22. cikke szerint meghatározott érintetti kérelmek teljesítésére köteles belső eljárásrendet kialakítani. Az eljárásrend a jelen utasítás 2. mellékletében található.

III.4.3. Adatbiztonság

A személyes 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 rendelkezhetőek.

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.

A GDPR 25. cikke megfogalmazza a beépített és alapértelmezett adatvédelem, más néven Privacy by Design követelményét, mely a következőképp szól:

„Az adatkezelő 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 mind az adatkezelés módjának meghatározásakor, mind pedig az

adatkezelés során olyan megfelelő technikai és szervezési intézkedéseket – például álnevesítést – hajt végre, amelyek célja egyrészt az adatvédelmi elvek, például az adattakarékosság hatékony megvalósítása, másrészt a GDPR-ban foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák beépítése az adatkezelés folyamatába. [...] Ezek az intézkedések különösen azt kell, hogy biztosítsák, hogy a személyes adatok alapértelmezés szerint a természetes személy beavatkozása nélkül ne válhassanak hozzáférhetővé meghatározatlan számú személy számára.”

Ezt egészíti ki a GDPR 32. cikke, mely elvárja az adatkezelőktől, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantáljanak, melyhez különféle intézkedéseket, mint az említett cél elérésére alkalmas módszereket (például álnevesítés, titkosítás, rendszeres tesztelés, felmérés, értékelés, stb.) sorol fel.

III.4.3.1. Fizikai védelem

A személyes adatok fizikai védelme az alábbi biztonsági intézkedéseket foglalja magában:

- környezeti hatásoktól való védelem biztosítása,
- a belépési jogosultságok ellenőrzése,
- az eszközök és a dokumentumok biztonságának biztosítása.

III.4.3.2. Logikai védelem

A személyes adatok logikai védelme az alábbi biztonsági intézkedéseket foglalja magába:

- anonimizálás, álnevesítés,
- titkosítás,
- jogosultság menedzsment és összeférhetlenségi mátrix,
- biztonsági mentések és visszaállítási protokollok,
- kártékony kódok elleni védelem,
- hálózatbiztonsági intézkedések,
- munkaállomások biztonságának és rendelkezésre állásának biztosítása.

III.4.3.3. Adatvédelmi hatásvizsgálat elvégzése

A Hivatal köteles az adatvédelmi tisztviselő szakmai iránymutatása alapján adatvédelmi hatásvizsgálatot végezni, amennyiben adatkezelés valamely – különösen új technológiákat alkalmazó – típusa –, figyelemmel annak jellegére, hatókörére, körülményére és céljaira – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Olyan egymáshoz hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló magas kockázatokat jelentenek, egyetlen hatásvizsgálat keretei között is értékelhetőek. A Hivatal az adatvédelmi hatásvizsgálat elvégzésének szükségessége kapcsán a NAIH adatkezelési műveletekre vonatkozó jegyzékét köteles figyelembe venni.

III.4.3.4. Adatvédelmi incidensek kezelése

A Hivatal köteles adatvédelmi incidensekkel kapcsolatos eljárásrendet alkalmazni. Az eljárásrendet a jelen utasítás 3. melléklete tartalmazza.

III.4.4. Adatvédelmi tudatosság

III.4.4.1. Adatvédelmi tisztviselő kijelölése

A Hivatal a kijelölt adatvédelmi tisztviselőt megbízási jogviszony keretében alkalmazza.

A Budapest Főváros XV. Kerület Önkormányzata és Polgármesteri Hivatala, Budapest Főváros XV. kerületi nemzetiségi önkormányzatai: Bolgár Önkormányzat, Cigány Nemzetiségi Önkormányzat, Görög Nemzetiségi Önkormányzat, Horvát Önkormányzat, Német Nemzetiségi Önkormányzat, Örmény Nemzetiségi Önkormányzat, Román Nemzetiségi Önkormányzat, Szerb Nemzetiségi Önkormányzat, Szlovák Nemzetiségi Önkormányzat számára a GDPR rendelkezéseire figyelemmel külön-külön kell adatvédelmi tisztviselőt kinevezni. Az adatvédelmi tisztviselő személye Budapest Főváros XV. Kerület Önkormányzata és Polgármesteri Hivatala, illetve Budapest Főváros XV. kerületi nemzetiségi önkormányzatai tekintetében megegyezik – az adatvédelmi tisztviselő neve: Dr. Miklós Péter.

III.4.4.2. Utasítás megismerése

Az utasítás tartalmáról való tájékoztatást a Hivatal az utasítás hatálya alá tartozó személyeknek szóló megismerési nyilatkozat alkalmazásával igazolja.

III.4.4.3. Partneri megállapodások felülvizsgálata

A Hivatal köteles felülvizsgálni a vele szerződéses kapcsolatban álló partnerek, vállalkozók, megbízottak szerződését adatvédelmi szempontból. Az új megállapodások esetén megfelelő adatvédelmi kikötéseket kell rögzíteni a szerződésekben.

III.4.4.4. Adatvédelmi tudatosság

A Hivatal gondoskodik arról, hogy az adatvédelmi tisztviselő által meghatározott rendszerességgel, vagy eseti jelleggel adatvédelmi tárgyú oktatásokra kerüljön sor a+ utasítás hatálya alá tartozó személyek részére.

IV. Az érintettek adatkezeléssel kapcsolatos jogai

Az Érintett a személyes adatainak kezelésével kapcsolatos jogait az Adatkezelőhöz eljuttatott kérelme útján gyakorolhatja, így különösen tájékoztatást, illetve egyéb, az adatait érintő műveletek végrehajtását (pl. az adatok törlését, helyesbítését, korlátozását) kérheti az Adatkezelőtől.

IV.1. Tájékoztatás kérése

Az Érintett kérelmére az Adatkezelő köteles tájékoztatást adni az Érintettnek az Adatkezelő által kezelt adatairól, az adatkezelés céljáról, jogalapjáról, terjedelméről, időtartamáról, adatfeldolgozás esetén az adatfeldolgozó nevééről, címéről és az adatkezeléssel összefüggő tevékenységéről, az esetlegesen bekövetkezett adatvédelmi incidens körülményeiről, hatásairól és az elhárítására megtett intézkedésekről, továbbá – az Érintett személyes adatainak továbbítása esetén – az adattovábbítás jogalapjáról és címzettjéről. Az Érintett személyes adatainak kezelésével kapcsolatos kérelmét szóban és írásban terjesztheti elő. A szóban benyújtott kérelemről a Hivatal arra jogosult dolgozója jegyzőkönyvet vesz fel a későbbi azonosításra alkalmas módon történő rögzítés érdekében.

Az Adatkezelő köteles biztosítani, hogy az Érintett – erre irányuló kérelme esetén – a személyes adatait tartalmazó nyilvántartásokba betekinthesse. Az Érintett betekintési jogának gyakorlása során az Adatkezelő köteles gondoskodni a nyilvántartásban szereplő további Érintettek személyes adatainak védelméről, felismerhetetlenné tételéről.

IV.2. Az adatok helyesbítése, kiegészítése

Az Érintett jogosult arra, hogy az Adatkezelőtől a pontatlan vagy hiányos személyes adatainak helyesbítését vagy kiegészítését kérje. Az Érintett helyesbítési kérelme esetén a helyesbítést az adatkezelést végző dolgozó haladéktalanul köteles elvégezni. Az Érintett kiegészítési kérelme esetén az Érintett köteles a kiegészítéshez szükséges információkat, adatokat az Adatkezelő részére átadni, valamint szükség esetén az adatok kezeléséhez szükséges hozzájárulást megadni.

IV.3. Az Érintett tiltakozási joga

Az Érintett jogosult arra, hogy személyes adatainak kezelése ellen tiltakozzon az Adatkezelő közérdekű adatkezelése, vagy az Adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges adatkezelése esetében [a GDPR 6. cikk (1) bekezdés e) pontján alapuló adatkezelés]. Ebben az esetben az Adatkezelő a személyes adatok további kezelésére csak abban az esetben jogosult, ha bizonyítja, hogy az adatkezelést olyan kényszerítő erejű jogos okok indokolják, amelyek elsőbbséget élveznek az Érintett érdekeivel, jogaival és szabadságaival szemben, vagy amelyek jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kapcsolódnak.

A Hivatal köteles az Érintettet a tiltakozási jogáról adatkezelési tájékoztatója útján, továbbá az Érintettnek a GDPR 6. cikk (1) bekezdés e) pontján alapuló adatkezelésről történő tájékoztatásával egyidejűleg tájékoztatni.

IV.4. Az adatok törlése

A Hivatal köteles az Érintettre vonatkozó személyes adatokat a kérelem teljesíthetőségének megállapítását követően haladéktalanul, de legfeljebb három munkanapon belül törölni, ha az alábbi indokok valamelyike fennáll:

- a) a személyes adatok kezelése jogellenes,
- b) az Érintett a hozzájárulását visszavonja, és nincs helye a további adatkezelésnek az Adatkezelő vagy harmadik fél jogos érdekeinek érvényesítése érdekében,
- c) a személyes adatok kezelésére már nincs szükség,
- d) az Érintett tiltakozik az adatkezelés ellen, és az Adatkezelő nem jogosult a további adatkezelésre, vagy
- e) a személyes adatok törlését jogszabály vagy bírósági/hatósági határozat előírja.

IV.5. Az elfeledtetéshez való jog

Ha az Adatkezelő nyilvánosságra hozta a személyes adatot, és azt törölni köteles, abban az esetben az Adatkezelő köteles minden ésszerű intézkedést megtenni annak érdekében, hogy az Érintett törlésre irányuló kérelméről tájékoztasson minden olyan adatkezelőt, aki az Érintett esetlegesen nyilvánosságra került adatait megismerte, illetve megismerhette.

IV.6. Az Adatkezelő egyéb intézkedési kötelezettsége

Az Adatkezelő az Érintett adatainak továbbítása esetén az adatok helyesbítéséről, törléséről, az adatkezelés korlátozásáról az Érintetten kívül mindazokat is köteles értesíteni, akiknek korábban az adatot adatkezelés céljából továbbította, kivéve, ha ez lehetetlen, vagy aránytalanul nagy erőfeszítést igényel. Az Érintett kérelmére az Adatkezelő köteles az Érintettet tájékoztatni azon címzettekről, akik részére az adatok továbbítása megtörtént.

IV.7. Az adatkezelés korlátozása

Az Érintett jogosult kérelmezni, hogy az Adatkezelő korlátozza az Érintett személyes adatainak kezelését, azaz a tárolt személyes adatokat jelölje meg a jövőbeli kezelésük korlátozása céljából. Az Adatkezelő – az Érintett kérésére – akkor korlátozza az adatkezelést, ha az alábbi esetek valamelyike teljesül:

- a) a személyes adatok pontossága vitatott,
- b) jogellenes az adatkezelés, de az Érintett a törlést ellenzi,
- c) az Érintett tiltakozik az adatkezelés ellen,
- d) az Adatkezelőnek nincs szüksége a továbbiakban a megadott személyes adatokra, de az Érintett jogai védelméhez azokat igényli.

Az adatkezelés korlátozásának a) pontja esetén a személyes adatok pontosságának ellenőrzéséig, a d) pont esetén pedig annak megállapításáig van helye, hogy az Adatkezelő jogos indokai elsőbbséget élveznek-e az Érintett jogos indokaival szemben.

Az adatkezelés korlátozása esetén, az ilyen személyes adatok kezelésére - a tárolás kivételével - csak az Érintett hozzájárulásával, vagy jogi igények előterjesztése, érvényesítése, védelme, illetőleg más természetes vagy jogi személy jogainak védelme érdekében, továbbá fontos közérdekből kerülhet sor. A Hivatal köteles az Érintettet az adatkezelés korlátozásának feloldásáról a korlátozás feloldását megelőzően tájékoztatni.

IV.8. Adathordozhatósághoz való jog

Az Érintett – amennyiben személyes adatainak kezelése hozzájárulásán alapul vagy az adatkezelés automatizált módon történik – jogosult arra, hogy a rá vonatkozó, általa az Adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa.

V. Záró rendelkezések

V.1. Amennyiben az Adatkezelő valamely adatkezelésre jogosult dolgozója adatkezeléssel kapcsolatos eljárása során az utasítás és a vonatkozó jogszabályok alapján sem találja tisztázottnak a követendő eljárást, az adatvédelmi tisztviselőhöz fordulhat. Az adatvédelmi tisztviselő szakmai álláspontja alapján a Hivatal vezetője dönt a követendő eljárásról, melyről a Hivatal vezetője a Hivatal dolgozóit tájékoztatja.

V.2. Az adatvédelmi tisztviselő köteles az utasítás szükség szerinti, de legalább évenkénti felülvizsgálatát elvégezni, és a felülvizsgálat eredményeként tett megállapításairól, módosítási javaslatairól a Hivatal vezetőjét tájékoztatni.

V.3. Hatályát veszti a Budapest Főváros XV. Kerületi Önkormányzat és Polgármesteri Hivatal belső adatvédelmi és adatbiztonsági szabályzatáról szóló 14/2020. (VI. 29.) számú együttes utasítás.

V.4. Ez az utasítás 2023. június 1. napján lép hatályba.

V.5. Az utasítással érintett kollégáknak és a nemzetiségi önkormányzatoknak a szabályzat rendelkezéseit meg kell ismerniük és a megismerés tényét megismerési nyilatkozaton igazolniuk kell.

Budapest, 2023. május 31.



Cserdiné Németh Angéla
polgármester



dr. Kevevári Edit
jegyző

VI. Melléklet

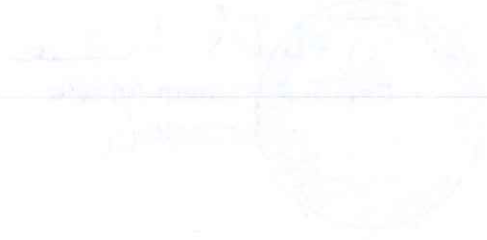
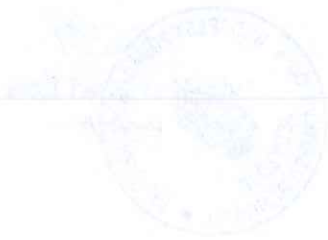
1. A mellékletben megadott adatok alapján a vállalkozás a 2017. évi adóbevallásában a következő adókat kell megfizetnie:

2. A vállalkozás a 2017. évi adóbevallásában a következő adókat kell megfizetnie:

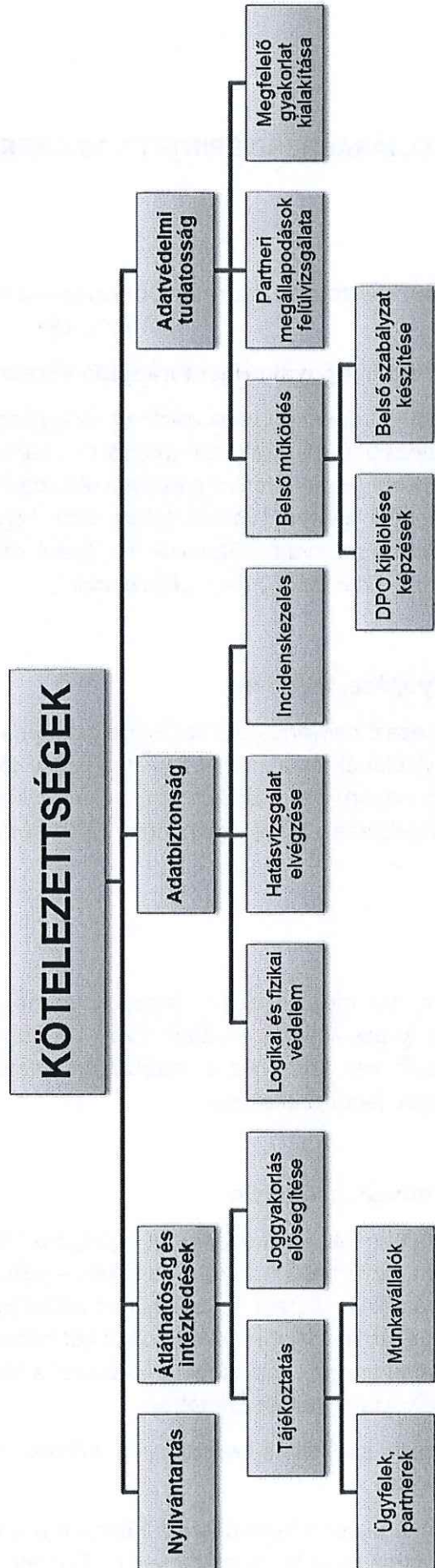
3. A vállalkozás a 2017. évi adóbevallásában a következő adókat kell megfizetnie:

4. A vállalkozás a 2017. évi adóbevallásában a következő adókat kell megfizetnie:

5. A vállalkozás a 2017. évi adóbevallásában a következő adókat kell megfizetnie:



ADATKEZELŐI KÖTELEZETTSÉGEK



ELJÁRÁSREND ÉRINTETTI MEGKERESÉSEK ESETÉN

A Budapest Főváros XV. Kerület Önkormányzata és Polgármesteri Hivatala eljárásrendje

- Érintetti joggyakorlásra irányuló kérelmekkel kapcsolatban -

A jelen eljárásrend előírásai abban az esetben alkalmazandók, amennyiben a Hivatallal, mint adatkezelővel kapcsolatban álló természetes személy, (a továbbiakban: „Érintett”) tájékoztatást kér személyes adatai kezelésének részleteiről, személyes adataihoz hozzáférést kér (például másolatot igényel) valamint kéri azok helyesbítését, törlését, zárolását, vagy kezelésének korlátozását, vagy tiltakozik az ilyen személyes adatok kezelése ellen (a továbbiakban együtt: „Kérelem”, vagy „Kérelmek”).

I. A kérelem benyújtása, fogadása

Kérelem az Adatkezelő nyilvános elérhetőségein nyújtható be. A Kérelemről – ha azt nem az adatvédelmi tisztviselőnek címezték – az Adatkezelő képviselője köteles haladéktalanul, de legkésőbb három napon belül tájékoztatni az adatvédelmi tisztviselőt. Az Adatkezelő az adatvédelmi tisztviselő szakmai véleményének kikérését követően köteles a Kérelem kezelése során eljárni.

II. Ellenőrzés

Kivételes esetben, ha megalapozott kétségek vannak a Kérelmet benyújtó természetes személy kilétével kapcsolatban, további, személyazonosság megerősítéséhez szükséges információ nyújtását kell kérni. Ez a személyes adatokhoz való jogosulatlan hozzáférés megakadályozása céljából szükséges.

III. Tájékoztatás módja, határideje

A Kérelmek nyomán hozott intézkedésekről legfeljebb a Kérelem beérkezésétől számított egy hónapon belül – ha az Érintett másként nem kéri – elektronikus formában (e-mail címünkről küldött) tájékoztatást kell nyújtani. Ez a határidő szükség esetén – a Kérelem összetettsége, illetve a Kérelmek számára tekintettel – további két hónappal meghosszabbítható. A határidő meghosszabbításáról annak okainak megjelölésével a Kérelem kézhezvételétől számított egy hónapon belül tájékoztatni kell az Érintettet.

Az Érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolja személyazonosságát.

Amennyiben nem kerül sor intézkedésre a Kérelem nyomán, legfeljebb annak beérkezésétől számított egy hónapon belül tájékoztatni kell az Érintettet ennek okairól, valamint arról, hogy

panaszt nyújthat be a Nemzeti Adatvédelmi és Információszabadság Hatóságnál, és élhet bírósági jogorvoslati jogával.

IV. Kamerafelvétellel kapcsolatos kérelmek

Ha az Érintett kamerás megfigyelés útján kezelt személyes adatairól kér másolatot, akkor megközelítőleg egyórás időkereten belül kell megadnia, mikor haladt át a megfigyelt területen.

Az Érintettnek nem kell igazolnia a hozzáférési joga gyakorlásához fűződő jogát vagy jogos érdekét, illetve nem kell indokolnia, hogy mi okból kíván élni ezzel a jogával.

Harmadik felek jogainak védelme nem használható kifogásként az Érintettek hozzáférés iránti jogos igényének megtagadására, ezért az Adatkezelőnek technikai intézkedéseket (például: képszerkesztés, ezen belül elfedés vagy eltorzítás) kell hoznia ilyen esetekre, hogy teljesíteni tudja a hozzáférési kérelmet.

V. Címzettek értesítése

Helyesbítésről, törlésről, adatkezelés-korlátozásról minden esetben értesíteni kell azokat az esetleges címzetteket, akikkel, illetve amelyekkel az Érintett személyes adatai közöldre kerültek, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel. Az Érintett kérésére tájékoztatást kell nyújtani ezekről a címzettekről.

VI. Tájékoztatás és intézkedés költségei

A Kérelmekre adott tájékoztatást, illetve az azok alapján megtett intézkedéseket díjmentesen kell biztosítani.

Ha az Érintett kérelme egyértelműen megalapozatlan vagy – különösen ismétlődő jellege miatt – túlzó, – figyelemmel a kért információ, vagy tájékoztatás nyújtásával, vagy a kért intézkedés meghozatalával járó adminisztratív költségekre – ésszerű díjat kell felszámítani, vagy meg kell tagadni a Kérelem alapján történő intézkedést.

ELJÁRÁSREND ADATVÉDELMI INCIDENSEK ESETÉRE

Eljárásrend adatvédelmi incidensek esetére

1. Bevezetés, az adatvédelmi incidens fogalma

A természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló rendelet (a továbbiakban: az általános adatvédelmi rendelet, GDPR) bevezeti azt a követelményt, miszerint minden adatvédelmi incidenst (a továbbiakban: adatvédelmi incidens) be kell jelenteni a nemzeti felügyeleti hatóságnak (Nemzeti Adatvédelmi és Információszabadság Hatóság), és egyes esetekben tájékoztatni kell azokat az egyéneket, akiknek a személyes adatait az incidens érinti.

E kötelezettség mibenlétét a **Budapest Főváros XV. Kerület Önkormányzata és Polgármesteri Hivatala, mint adatkezelő** jelen eljárásrend elfogadásával kívánja rögzíteni és megszerezni.

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.

2. Az adatvédelmi incidensek fajtái

Az adatvédelmi incidensek az alábbi három információbiztonsági elv alapján kategorizálhatók;

- „titoksértés”: személyes adatok jogosulatlan vagy véletlen közlése vagy az ilyen adatokhoz való jogosulatlan vagy véletlen hozzáférés;
- „sértetlenségi adatsértés”: személyes adatok jogosulatlan vagy véletlen módosítása;
- „hozzáférhetőségi adatsértés”: a személyes adatokhoz való hozzáférés véletlen vagy jogosulatlan elvesztése vagy a személyes adatok véletlen vagy jogosulatlan megsemmisítése.

Az incidens a körülményektől függően egyidejűleg vagy bármilyen kombinációban érintheti a személyes adatok titkosságát, sértetlenségét és hozzáférhetőségét.

Míg a titoksértés vagy a sértetlenségi adatsértés viszonylag egyértelműen megállapítható, addig a hozzáférhetőségi adatsértés már kevésbé nyilvánvaló. Az incidens mindig hozzáférhetőségi adatsértésnek minősül, ha a személyes adatok véglegesen elvesznek vagy megsemmisülnek.

3. Reagálás az adatvédelmi incidensekre

Az adatkezelő valamennyi szervezeti egysége számára kötelező, hogy kinevezzen egy olyan felelős személyt, akinek feladata az adatvédelmi incidensek nyilvántartásba vétele, illetve indokolt esetben az incidens jelentése az adatkezelő adatvédelmi tisztviselőjének az incidensből eredő kockázatok csökkentése céljából.

A felelős személy részére az adott szervezeti egység valamennyi munkatársa köteles jelenteni, amennyiben adatvédelmi incidenst, vagy annak gyanújáról tudomást szerez.

3.1. Nyilvántartás

Kötelező az adatvédelmi incidensek rögzítésére olyan nyilvántartást vezetni, amely feltünteti az ahhoz kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az GDPR 35. cikke szerinti követelményeknek való megfelelést.

A személyes adatokat tartalmazó adatvédelmi incidens nyilvántartást annyi ideig kötelező megőrizni, amennyi tárolási idő meg van határozva az incidenssel érintett személyes adatokra.

Az incidensekre válaszként hozott döntések mögötti érvelést is nyilvántartásba kell venni. A döntés indoklását különösen akkor kell nyilvántartani, ha az incidenst nem jelentik be. Az indoklásnak tartalmaznia kell azokat az okokat, amiért az adatkezelő úgy véli, hogy az incidens valószínűsíthetően nem jár kockázattal az egyének jogaira és szabadságaira nézve. Ha pedig az adatkezelő szerint teljesül a GDPR 34. cikk (3) bekezdésében foglalt valamely feltétel,¹ akkor az adatkezelőnek erre vonatkozóan megfelelő bizonyítékot kell szolgáltatnia.

3.2. Bejelentés felügyeleti hatóságnak

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.

¹

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

Meg kell bizonyosodni arról, hogy az összes megfelelő technológiai védelmi és szervezési intézkedés végrehajtásra került-e, egyrészt az adatvédelmi incidens haladéktalan megállapítása, másrészt a felügyeleti hatóságnak történő bejelentés és az érintett sürgős értesítése érdekében. Azt, hogy az értesítésre indokolatlan késedelem nélkül került-e sor, különösen az adatvédelmi incidens jellegére és súlyosságára, valamint annak az érintette gyakorolt következményeire, illetve hátrányos hatásaira figyelemmel kell megállapítani. A felügyeleti hatóságnak történt bejelentést a GDPR-ban meghatározott feladataival és hatásköreivel összhangban történő beavatkozását eredményezheti.

Az adatvédelmi incidens akkor jut az adatkezelő tudomására, amikor az adatkezelő észszerű bizonyossággal meggyőződött arról, hogy olyan biztonsági incidens történt, amelynek következtében a személyes adatok veszélybe kerültek.

- A biztonságot érintő összes eseményről tájékoztatni kell a felelős személyt vagy személyeket, akinek vagy akiknek a feladata az incidensek kezelése, az adatvédelmi incidens bekövetkeztének megállapítása és a kockázat felmérése.
- Ezután fel kell mérni az incidens következtében az egyéneket érintő kockázatot (a kockázatmentesség, a kockázat és a jelentős kockázat valószínűsége), egyúttal tájékoztatni kell a szervezet érintett részlegeit.
- Szükség esetén az incidensről bejelentést kell tenni a felügyeleti hatóságnak, és esetleg tájékoztatni kell az érintett egyéneket.
- Az adatkezelőnek egyúttal gondoskodnia kell az incidens elhárításáról, majd a helyreállításról.
- Az incidens alakulásáról nyilvántartást kell vezetni.

Amennyiben az adatkezelő mérlegelése alapján az adatvédelmi incidens a hatóságnak való bejelentési kötelezettség alá esik, – azaz valószínűleg kockázattal jár a természetes személyek jogaira és szabadságaira nézve – az alábbi felületeken keresztül kell megtennie a bejelentést:

<https://dbn-online.naih.hu/public/login>

Az Adatvédelmi Incidensbejelentő Rendszer Felhasználói Kézikönyve az alábbi linken érhető el:

<https://dbn-online.naih.hu/assets/files/UserManual.pdf>

3.3. Érintett tájékoztatása

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.

Az érintettek tájékoztatásáról az észszerűség keretei között a lehető leghamarabb gondoskodni kell, szorosan együttműködve a felügyeleti hatósággal, és betartva az általa vagy más érintett hatóságok például bűnüldöző hatóságok által adott útmutatást.

4. Az eljárásrendhez kapcsolódó dokumentumok

Az adatkezelő kijelenti, hogy az Eljárásrend 3. pontjában szereplő adatvédelmi incidensek esetére előkészített dokumentációval (1. és 2. sz. melléletek) rendelkezik.

5. Záró rendelkezések

Az Eljárásrend 2023. június 1-jén lép hatályba.

3.1. Tájékoztató adatvédelmi incidensekről érintettek részére

Feladó:

Budapest Főváros XV. Kerület Önkormányzata és Polgármesteri Hivatala

1153 Budapest, Bocskai utca 1-3.

Címzett:

[Érintett természetes személy neve]

[Érintett lakcíme]

Tájékoztató formája:

Postai levél	igen/nem
E-mail	igen/nem
Más:	[...]

1. Adatkezelő adatai

Név: **Budapest Főváros XV. Kerület Önkormányzata és Polgármesteri Hivatala**

Székhely: 1153 Budapest, Bocskai utca 1-3.

Képviselőre jogosult neve, beosztása: Dr. Kevevári Edit, jegyző

Törzskönyvi azonosító: 515003

Adószám: 15735784242

2. A tájékoztatás alapjául szolgáló jogszabály

Alulírott Dr. Miklós Péter, az Adatkezelő nevében eljárva, mint adatvédelmi tisztviselő – figyelemmel az Európai Parlament és Tanács (EU) 2016/679. számú Rendeletének (a továbbiakban: GDPR) 34. cikkére – ezúton tájékoztatom Önt a jelen levélben leírt adatvédelmi incidensről.

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 (továbbiakban: incidens).

3. Az adatvédelmi incidens részletei

3.1. Az incidens jellege

Milyen körülmények között és mikor került sor az incidensre?

Kiket, vagy természetes személyek milyen csoportját érinti az incidens?

Hozzávetőlegesen hány személyt érint az incidens?

Milyen személyes adatokat érint az incidens?

Különleges adatokat is érinti az incidens?

Körülbelül milyen mennyiségű személyes adatot érint az incidens?

3.2. Kapcsolattartók elérhetőségei

Az alábbi személyektől kérhet további tájékoztatást az incidenssel kapcsolatban:

Adatvédelmi Tisztviselő

Név:

Telefonszám:

E-mail cím:

Egyéb kapcsolattartó

Név:

Telefonszám:

E-mail cím:

3.3. Az incidensből eredő lehetséges következmények

Álláspontunk szerint az incidens valószínűsíthetően az alábbi következményekkel fog járni;

[...]

3.4. Intézkedések

Az incidens orvoslására az alábbi intézkedéseket tettük, illetve tervezzük tenni:

[...]

Amennyiben az incidensből hátrányos következmények származnának, ezek enyhítése céljából az alábbi intézkedéseket tervezzük megtenni:

[...]

Kelt.:,évhónapnap

.....
Budapest Főváros XV. Kerület
Önkormányzata és Polgármesteri
Hivatala
képviselő:
Dr. Kevevári Edit, jegyző
Adatkezelő

3.2. Adatvédelmi incidensek nyilvántartása

1. Az Európai Parlament és Tanács (EU) 2016/679. számú Rendelet (a továbbiakban: GDPR) 33. cikk (5) bekezdése szerint az adatkezelő számára kötelező az adatvédelmi incidensek nyilvántartása oly módon, hogy feltünteti az ahhoz kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az e cikk követelményeinek való megfelelést.
2. Jelen nyilvántartást a **Budapest Főváros XV. Kerület Önkormányzata és Polgármesteri Hivatala** (a továbbiakban: Adatkezelő) a 29. cikk szerinti Adatvédelmi Munkacsoport 2017. október 3. napján elfogadott és 2018. február 6. napján felülvizsgált, adatvédelmi incidensekről szóló WP250.rev.01 számú Iránymutatás figyelembevételével állítja össze.

Incidens és tudomás szerzés időpontja	Incidenstípusa	Elvesztett adatok formája, száma	Incidenssel érintett személyes adatok	Kiknek a személyes adatait érinti az incidens?	Kockázat elemzés, az incidens hatásai	Értesítés	Incidens orvoslására tett/tervezett intézkedések	Intézkedések határideje és a bennük közreműködő személyek	Incidens azonosítója

Adatkezelő adatai

Név: **Budapest Főváros XV. Kerület Önkormányzata és Polgármesteri Hivatala**

Székhely: 1153 Budapest, Bocskai utca 1-3.

Képviselőre jogosult neve, beosztása: Dr. Kevevári Edit, jegyző

Törzskönyvi azonosító: 515003

Adószám: 15735784242

Utolsó frissítés dátuma: [*]