Bokod Község Önkormányzata

és

Bokodi Polgármesteri Hivatal

ADATVÉDELMI SZABÁLYZAT

Hatályos: 2020. március 1. napjától

Jóváhagyta:

Csonka László
polgármester

Zsigmond Anikó
jegyző

Tartalomjegyzék

1. Alap adatok

A jelen adatvédelmi szabályzatot a **Bokod Község Önkormányzata** (székhelye: 2855 Bokod, Hősök tere 6.; adószáma 15729916-2-11; képviseli Csonka László polgármester), valamint a **Bokodi Polgármesteri Hivatal** (székhelye: 2855 Bokod, Hősök tere 6.; adószáma 15844868-1-11; képviseli Zsigmond Anikó jegyző) (a továbbiakban Önkormányzat, valamint Hivatal) adták ki, és az Önkormányzat, valamint a Hivatal adatkezelés és adatfeldolgozás műveleteinek szabályozására szolgál.

Az Önkormányzat, valamint a Hivatal adatai

Bokod Község Önkormányzata, valamint a Bokodi Polgármesteri Hivatal	
Intézmény címe	2855 Bokod, Hősök tere 6.
Képviseli:	Csonka László polgármester Zsigmond Anikó jegyző
Telefonszám:	+36 34/ 490-151
E-mail cím:	jegyző@bokod.hu hivatal@bokod.hu
Adószám:	15729916-2-11 (Bokod Község Önkormányzata) 15844868-1-11 (Bokodi Polgármesteri Hivatal)
Weboldal:	http://www.bokod.hu/
Adatvédelmi tisztségviselő:	Glazer DATA&SYSTEMS (Dr. Glázer Noémi e. v.) Képviseli: Dr. Glázer Noémi E-mail: gdsyst@gdsyst.com Telefonszám: + 36 31/781-62-64

A Bokodi Polgármesteri Hivatal jegyzője a polgármesterrel egyetértésben az adatvédelmi szabályzat előírásait az alábbiak szerint határozza meg:
A jelen ***szabályzatot kötelező felülvizsgálni olyan esetekben, amikor*** új kockázatértékelésre okot adó esemény, avagy az adatkezelés módjában és metodikájában egyéb lényeges változás (különösképpen a jogszabály környezet változása) történik. Az új kockázatértékelés elkészítésére olyan okból, avagy eseményből kerül sor, amikor valószínűsíthető, hogy az adatok kezelése az érintettekre kockázatot jelenthet (így különösen új adatkezelési technológia bevezetése, alkalmazása, a korábbitól eltérő módon történő adatgyűjtés vagy adattovábbítás stb.).
A jelen szabályzat az alábbi- további- szabályzatokkal együttesen és összhangban értelmezendő:
- Irattározási szabályzat
- Informatikai Biztonsági Szabályzat
- BYOD szabályzat
- Kamerarendszerre vonatkozó Szabályzat
- Közérdekből Nyilvános Adatokra vonatkozó Szabályzat

2. Bevezető rendelkezések

Az Önkormányzat, valamint a Hivatal jogszabályokban meghatározott feladat- és hatáskörei keretében jár el, rendkívül sokfajta egyedi ügytípusban, ezen tevékenységük körében elengedhetetlenül szükséges személyes adatokat gyűjteniük és kezelniük.

Az Önkormányzat, valamint a Hivatal által kezelt személyes adatok magáncélra való felhasználása tilos.

Az adatkezelésnek mindenkor meg kell felelnie a célhoz kötöttség alapelvének.

Az Önkormányzat, valamint a Hivatal alapvető célja, hogy minden esetben tiszteletben tartsa a természetes személyek alapvető jogait és szabadságait, különösen, ami a személyes adataik védelméhez való jogukat illeti.

A jelen ***Szabályzat célja*** az, hogy biztosítsa az Önkormányzat, valamint a Hivatal tevékenysége során a személyes adatok védelméhez fűződő jogok érvényesülését, továbbá, hogy az Önkormányzat, valamint a Hivatal által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes és különleges adatok kezelése során irányadó adatvédelmi és adatbiztonsági szabályokat, valamint annak biztosítása, hogy az Önkormányzat, valamint a Hivatal adatkezelése megfeleljen a GDPR, továbbá a mindenkori Infotörvény előírásainak.

A jelen adatvédelmi szabályzatban rögzítésre kerül a személyes adatok gyűjtésének, tárolásának és kezelésének módja, valamint rögzítésre kerülnek az Önkormányzat, valamint a Hivatal adatvédelmi elvei.

Az Önkormányzat a tisztségviselői, alkalmazottai, a Hivatal valamennyi köztisztviselője, munkavállalója, illetve a hivatali eljárásban részt vevő egyéb közreműködője (szerződéses jogviszonyban állókra) (a továbbiakban együttesen alkalmazottak) számára átláthatóvá kívánják tenni az adatkezelési eljárásokat, hogy a természetes személyek személyes adataik kezelésével összefüggő védelemhez kapcsolódó elvek és szabályok érvényesüljenek.

A jelen szabályzat az adatvédelmi szabályoknak való megfelelést szolgálja.

A jelen adatvédelmi szabályzat biztosítja, hogy az Önkormányzat, valamint a Hivatal

- megfelel az adatvédelmi jogi követelményeknek, és megfelelő adatvédelmi gyakorlatot és operatív tevékenységet folytat;
- védi és figyelembe veszi az érintettek jogait és jogos érdekeit;
- nyilvánvalóvá teszi az egyes adatkezelési műveleteket (gyűjtés, őrzés, tárolás, törlés, továbbítás);
- szabályozza az adatvédelmi incidens megelőzésére és kezelésére vonatkozó teendőket;
- szabályozza a teendőket adatvédelmi incidens esetére;
- szabályozza a hatásvizsgálatra vonatkozó feladatokat;
- szabályozza az érdekmérlegelésre vonatkozó teendőket;
- szabályozza az adatfeldolgozás során alkalmazandó feladatok.

A szabályzat személyi és tárgyi hatálya

A jelen szabályzat rendelkezései kötelező alkalmazása az alábbi személyi körre tejed ki:

- az Önkormányzat tisztségviselőire, alkalmazottaira,
- a Hivatal valamennyi köztisztviselőjére, munkavállalójára, illetve a hivatali eljárásban részt vevő egyéb közreműködőkre (szerződéses jogviszonyban állókra)

A jelen szabályzat hatálya az alábbi adatok körére terjed ki:

Valamennyi érintettel összefüggésbe hozható személyes adat. Az Önkormányzat, valamint a Hivatal jogszabályokban meghatározott feladat- és hatáskörei keretében jár el, rendkívül sokfajta egyedi ügytípusban.

A jelen **szabályzat hatály nem terjed ki** az olyan személyes adatkezelésre, amely jogi személyekre, illetve amely különösen olyan vállalkozásokra vonatkozik, amelyeket jogi személyként hoztak létre, beleértve a jogi személy nevét és formáját, valamint a jogi személy elérhetőségére vonatkozó adatokat. **A jogi személy kapcsolattartója, továbbá a jogi személy által az Önkormányzat, valamint a Hivatal részére átadott személyes adatokat magában foglaló adatok megadása esetén az átadott adatok személyes adatoknak tekintendők, és ennek megfelelően a jelen Szabályzatban foglaltak szerint kötelező kezelni azokat.**

3. Értelmező rendelkezések

A jelen szabályzat alkalmazásában:

1. „személyes adat": azonosított vagy azonosítható természetes személyre (a jelen Szabályzatban: „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

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

3. „az adatkezelés korlátozása": a tárolt személyes adatok megjelölése jövőbeli kezelésük korlátozása céljából

4. „profilalkotás": személyes adatok automatizált kezelésének bármely olyan formája, amelynek során a személyes adatokat valamely természetes személyhez fűződő bizonyos személyes jellemzők értékelésére, különösen a munkahelyi teljesítményhez, gazdasági helyzethez, egészségi állapothoz, személyes preferenciákhoz, érdeklődéshez, megbízhatósághoz, viselkedéshez, tartózkodási helyhez vagy mozgáshoz kapcsolódó jellemzők elemzésére vagy előrejelzésére használják

5. „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

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

7. „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

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

9. „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

10. „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

11. „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

12. „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

13. adatbiztonság: a személyes adatok jogosulatlan kezelése, így különösen megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni szervezési, technikai megoldások és eljárási szabályok összessége; az adatkezelésnek az az állapota, amelyben a kockázati tényezőket – és ezzel a fenyegetettséget – a szervezési, műszaki megoldások és intézkedések a legkisebb mértékűre csökkentik

14. hardver eszköz: valamennyi olyan eszköz, amelynek feladata az informatikai rendszer folyamatos működésének biztosítása, vagy amely bizton sági adatmentésre, avagy másolatok készítésére szolgál, valamint amely elektronikus vagy egyéb módon a számítógép külső behatás elleni védelmét szolgálja

15. hírközlő eszköz: bármilyen technikai eszköz, technológiai eljárás, amely egy vagy több fogadó személy számára jelzések, adatok és információk továbbítására vagy fogadására alkalmas

16. információs önrendelkezési jog: az Alaptörvény VI. cikkében biztosított személyes adatok védelméhez való jognak az a tartalma, hogy mindenki maga rendelkezik személyes adatainak feltárásáról és felhasználásáról

4 Az adatvédelem jogi háttere

Az adatvédelemre vonatkozó alapvető szabályokat az ***Európai Parlament és Tanács (EU) 2016/679 Rendelete*** (2016. április 27.) szabályozza, mely 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 szól (általános adatvédelmi rendelet, a jelen szabályzatban a továbbiakban: GDPR).

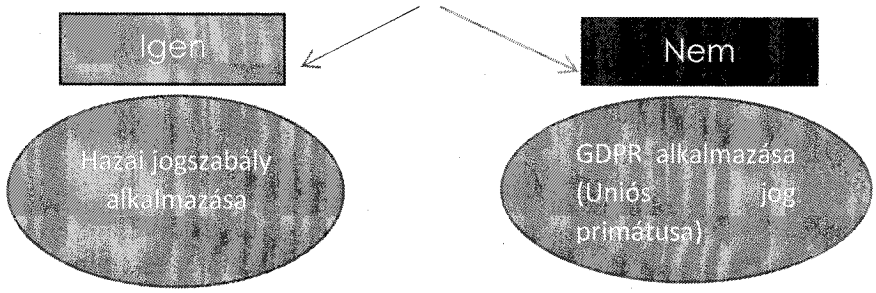
Az Önkormányzat, valamint a Hivatal a GDPR-t az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a jelen szabályzatban a továbbiakban: Infótörvény) mindenkor hatályos rendelkezéseivel összhangban, az abban foglalt szabályok betartásával értékeli és alkalmazza, azzal, hogy ahol az Infótörvény és a GDPR szabályai ellent mondanak egymással (jogszabályi összeütközés/kollízió) ott a GDPR rendelkezései irányadók.

A GDPR és az Infótörvény a személyes adatokra vonatkozó valamennyi adatgyűjtési és adatkezelési műveletre alkalmazandó, tekintet nélkül az adatgyűjtés és az adatkezelés formájára (elektronikus, avagy papír alapú).

Az Önkormányzat, valamint a Hivatal kötelezettséget vállal arra, hogy a további magyarországi szabályokkal és jogszabályokkal összhangban, azoknak megfelelve, az ágazati szabályok figyelembe vételével folytatja az adatkezelési és adatgyűjtési tevékenységét.

Tekintettel arra, hogy a jelen szabályzat elkészítésének idején a jogszabályi környezet folyamatos változása, továbbá sok esetben jogszabályi kollízió figyelhető meg, az Önkormányzat, valamint a Hivatal jogalkalmazói tevékenysége során- a NAIH eddigi gyakorlatát is figyelembe véve- az alábbi módszertant követi:

a) Megvizsgálja, hogy egyéb hazai jogszabály **kötelező erejű kivételt** tesz-e, és a **GDPR** az adott körben **megengedi-e** a hazai jogalkotónak a kivétel alkalmazását?



Az Önkormányzat és a Hivatal az ügyek-és ügytípusok tekintetében minden esetben egyedi mérlegeléssel dönt, azzal, hogy kétség esetén kikéri az adatvédelmi tisztségviselő véleményét.

További alkalmazott jogszabályok

A személyes adatok kezelését a mindenkori hatályos, különösen az alábbiakban felsorolt jogszabályi előírásoknak megfelelően végezi Az Önkormányzat, valamint a Hivatal :

- GDPR (általános adatvédelmi rendelet) – **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)**
- **Adatvédelmi törvény** – Az információs önrendelkezési jogról, és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban Infotv., adatvédelmi törvény)
- 1998. évi VI. törvény **az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről**;
- 1995. évi CXIX. Törvény **(„Katv.")**- a kutatás és a közvetlen üzletszerzés célját szolgáló név- és lakcím adatok kezeléséről
- **Polgári Törvénykönyv** - 2013. évi V. törvény
- 2011. évi CLXXXIX. törvény **Magyarország helyi önkormányzatairól**
- **Magyarország Alaptörvénye** (2011. április 25.)
- 2016. évi CL. törvény az **általános közigazgatási rendtartásról**;
- 2010. évi I. törvény az **anyakönyvi eljárásról**
- 429/2017. (XII.20.) Korm. rendelet az **anyakönyvezési feladatok ellátásának részletes szabályairól**

- 2010. évi XXXVIII. törvény a **hagyatéki eljárásról**
- 2011. évi CXCV. törvény az **államháztartásról**;
- 2000. évi C. törvény a **számvitelről**;
- 368/2011. (XII. 31.) Korm. rendelet **az államháztartásról szóló törvény végrehajtásáról**;
- 2011. évi CXCIX. törvény a **közszolgálati tisztviselőkről**;
- 2012. évi I. törvény a **munka törvénykönyvéről**;
- 1992. évi XXXIII. törvény a **közalkalmazottak jogállásáról**;
- 2017. évi CL. törvény az **adózás rendjéről**;

A jogszabályi megfelelés érdekében az Önkormányzat, valamint a Hivatal vállalja, hogy a személyes adatok gyűjtésére és felhasználására jogszerűen kerül sor, az adatok biztonsága érdekében szükséges lépéseket és intézkedéseket megteszi, továbbá az adatokat jogosulatlanul nem hozza nyilvánosságra.

5. Alapelvek

Az Önkormányzat, valamint a Hivatal tevékenysége során alkalmazott, a személyes adatok kezelésére vonatkozó alapelvek (adatvédelmi irányelvek)

I. Az Önkormányzat, valamint a Hivatal által, illetve az Önkormányzat, valamint a Hivatal szervezetében a **cél megvalósulásához szükséges mértékben és ideig** csak olyan személyes és különleges adat kezelhető, amely **az adatkezelés céljának megvalósulásához elengedhetetlen és a cél elérésére alkalmas. (adatkezelés célja és ideje)**

II. Az adatgyűjtés és kezelés kizárólag pontosan **meghatározott célból és jogcím alapján** történik.

III. Csak annyi adat kerül gyűjtésre és kezelésre, amennyi a célok eléréséhez feltétlenül szükséges, az Önkormányzat, valamint a Hivatal kerüli a felesleges és irreleváns adatok gyűjtését és tárolását. **(adattakarékosság)**

IV. Az Önkormányzat, valamint a Hivatal alkalmazottai a feladataik ellátása körében személyes és különleges adatot csak a vonatkozó jogszabályok előírásainak betartásával kezelhetnek. **(jogszabályi megfelelés biztosítása)**

V. A személyes adatok védelméhez való jog a természetes személyek Alaptörvényben biztosított alapjoga, amely garantálja az adatalanyok információs önrendelkezési jogát. Az információs önrendelkezési jog az érintettek beleegyezésének hiányában kizárólag törvényi felhatalmazás alapján korlátozható. Az információs önrendelkezési jog tiszteletben tartása érdekében az Önkormányzat, valamint a Hivatal., illetőleg alkalmazottai **személyes adatot csak az alábbi esetekben kezelhet**:

- *az érintett előzetes, önkéntes és kifejezett hozzájárulása,*

  Amennyiben az adatkezelés hozzájáruláson alapszik, úgy az érintett a hozzájárulását bármilyen bizonyítható módon megadhatja, így írásban, szóban és ráutaló magatartással. Az Önkormányzat, valamint a Hivatal fenntartja magának a jogot, hogy egyes adatkezelések esetén a hozzájárulás egyes formáit kizárja. Az Önkormányzat, valamint a Hivatal elsődlegesen írásban szerzi be az érintett hozzájárulását.

- *szerződés teljesítése a teljesítéshez szükséges mértékben,*

- *az érintett vagy harmadik személy jogos érdekeinek érvényesítése,*
- *az Önkormányzat, valamint a Hivatal jogi kötelezettségének teljesítése,*
- *Közérdekű vagy az Önkormányzatra, valamint a Hivatalra ráruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtásához szükséges*
- *az érintett vagy más természetes személy létfontosságú érdeke.*

VI. Személyes adat kezelésére csak a jelen szabályzat 5. pontjában meghatározott valamely jogalapon, jog gyakorlása vagy kötelezettség teljesítése érdekében van lehetőség. Törvényben elrendelt adatkezelés esetén kizárólag a felhatalmazást adó törvényben meghatározott célból valósulhat meg adatkezelés. Az Önkormányzat, valamint a Hivatal által kezelt – vagy az Önkormányzat, valamint a Hivatal részére más adatkezelő által rendelkezésre bocsátott – személyes adatok magáncélra való felhasználása tilos. Az adatkezelésnek mindenkor meg kell felelnie a **célhoz kötöttség** alapelvének.

VII. Az Önkormányzat, valamint a Hivatal törekszik arra, hogy az általa kezelt adatok **pontosak** és **naprakészek** legyenek.

VIII. Az Önkormányzat, valamint a Hivatal csak **addig kezeli** a személyes adatokat, ameddig az **feltétlenül szükséges**.

IX. Az Önkormányzat, valamint a Hivatal a szükségtelenné vált adatokat véglegesen és helyre nem állítható módon **törli**.

X. Az **adatok feldolgozására** csak az érintett jogainak figyelembe vételével kerül sor.

XI. Az Önkormányzat, valamint a Hivatal minden tőle telhető és elvárható lépést megtesz az **adatok védelme** érdekében.

XII. Az Önkormányzat, valamint a Hivatal **csak akkor továbbítja** az Európai Gazdasági Térségen kívül eső harmadik országnak, szervezetnek, magánszemélynek vagy vállalkozásnak, amennyiben az adott harmadik ország, szervezet, magánszemély vagy vállalkozás igazolhatóan biztosítja az adatok biztonságának kellő mértékét és módját.

6. Kockázatok

A jelen szabályzat különösen az alábbi kockázatokkal szembeni védelmet hivatott elősegíteni:

- az adatok jogosulatlan személy vagy személyek általi megszerzése,
- érintett adatokkal való rendelkezési jogának megsértése,
- adatok biztonsági rendszer megsértésével/ kijátszásával történő megszerzése.

7. Az adatok megismerésére jogosultak köre

A személyes adatokat az Önkormányzat, valamint a Hivatal a vonatkozó adatkezelési célhoz kapcsolódó hozzáférési jogosultságokkal rendelkező alkalmazottai ismerhetik meg a tevékenységük végzéséhez szükséges mértékben.

8. Specifikus felelősségek

Az Önkormányzat, valamint a Hivatal alkalmazottainak kötelessége annak biztosítása, hogy az adatok gyűjtése, kezelése és tárolása jogszerűen történjen. Az egyes részfeladatok és **felelősségi körök** az alábbiak szerint kerülnek meghatározásra:

a) A teles jogszabályi és jogi megfelelés biztosítása a **jegyző és a polgármester közös** feladata.

- az Önkormányzat, valamint a Hivatal sajátosságainak figyelembevételével meghatározza az adatvédelemre, valamint az azzal összefüggő tevékenységre vonatkozó feladat és hatásköröket, és kijelöli az adatkezelés felügyeletét ellátó személyt.

- Kiadja az Önkormányzat, valamint a Hivatal adatvédelemmel kapcsolatos belső szabályait.

Felelős:

- az érintettek Infotv.-ben meghatározott jogainak gyakorlásához szükséges feltételek biztosításáért;
- az Önkormányzat, valamint a Hivatal által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosításáért;
- felelős az adatkezelésre irányuló ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért;
- felügyeli az adatvédelmi tisztviselő tevékenységét;

b) Az Önkormányzat, valamint a Hivatal az adatkezelési működését és a kezelt adatok körére és mennyiségére tekintettel, valamint az adatkezelések okán **adatvédelmi tisztségviselő** kijelölésére kötelezett.

Az Önkormányzat, valamint a Hivatal az adatvédelmi tisztviselő nevét és elérhetőségét közzéteszi honlapján, valamint bejelenti ezen adatokat a NAIH részére.

Az adatvédelmi tisztviselő feladatai:

- segítséget nyújt az érintett jogainak biztosításában
- jogosult jelen szabályzat betartását ellenőrizni
- az Önkormányzat, valamint a Hivatal adatvédelmi rendszerének felügyeletét ellátja
- figyelemmel kíséri az adatvédelemmel és információszabadsággal kapcsolatos jogszabályváltozásokat, ezek alapján indokolt esetben kezdeményezi jelen szabályzat módosítását
- tájékoztatást és szakmai tanácsot ad az Önkormányzat, valamint a Hivatal adatvédelmi jogszabályokban előírt kötelezettségeinek ellátásával kapcsolatban
- harmadik féllel kötött olyan megállapodások vizsgálata, amely adatkezelési- és továbbítási kérdéseket vet fel.
- együttműködés a partnerek adatvédelmi tisztségviselőivel.
- kapcsolattartás az illetékes adatvédelmi hatósággal.
- amennyiben az illetékes adatvédelmi hatóság előírja, a Hatóság által tartott továbbképzéseken és konferenciákon való részvétel az adatvédelmi ismeretek naprakészen tartása érdekében.

- ellátja a GDPR és az Infótörvény rendelkezéseiben meghatározott további feladatokat.

c) A ***webfejlesztő szakértő partner*** felelőssége az alábbiakra terjed ki:

- a weblapokkal összefüggő adatvédelmi feladatok ellátása és ellenőrzése,
- a weblapok rendszeres karbantartása és felügyelete
- új webszerkesztési metodikák alkalmazása és bevezetése
- az adatbiztonság növelésére vonatkozó javaslatok megtétele
- adatvédelmi (informatika- webbel összefüggő) incidens esetén haladéktalanul az érintettek érdekeit védő intézkedések megtétele

d) Az ***informatikus szakértő partner*** felelőssége az alábbiakra terjed ki:

- valamennyi rendszer, informatikai szolgáltatás és eszköz informatikai biztonsági szempontoknak való megfelelésének biztosítása a rendelkezésre álló vagy észszerűen elérhető szoftver és hardver megoldások segítségével
- rendszeres felülvizsgálat és ellenőrzés lefolytatása a szoftverek és hardverek megfelelő működésének biztosítása érdekében
- valamennyi, külső szolgáltató által biztosított és adattárolásra vagy feldolgozásra alkalmas eszköz vállalati alkalmazás megkezdése előtti értékelése, akár szoftver, akár hardver, akár offline, akár online eszközről van szó
- rendszertámadás vagy adatszivárgás esetén az informatikai védelem és helyreállítás biztosítása az azonnali informatikai adatvédelem ellátása érdekben

e) Az ***alkalmazottak*** általános felelősségei:

- valamennyi alkalmazott, aki a jelen szabályzatban meghatározott adatokhoz hozzá fér, **a megszerzett adatokat kizárólag a munkavégzése, feladat ellátása körében és céljából kezelheti, rögzítheti, tarthatja nyilván.**
- a munkavégzés, feladat elvégzése során megszerzett adatokat az alkalmazott, erre vonatkozó **külön írásos engedély nélkül nem oszthatja meg arra illetéktelen személyekkel, nem teheti közzé, adatot önkényesen nem kezelhet.**
- arra **fel nem hatalmazott személlyel vagy személyekkel** az alkalmazott **nem oszthat meg személyes adatokat az Önkormányzat, illetőleg a Hivatal szervezetrendszerén belül.**
- az Önkormányzat, valamint a Hivatal működése során **nem vihető ki személyes adatokat tartalmazó iratok az Önkormányzat, valamint a Hivatal székhelyéről vagy telephelyéről.** Amennyiben ez mégis **szükségessé válna**, úgy e tekintetben az alkalmazottak kötelesek azt **bejelenteni, és egyedi jóváhagyást kérni** a felettesüktől.
- az Önkormányzat, valamint a Hivatal biztosítja, hogy **az alkalmazottak adatvédelmi képzés/oktatás keretében ismerhessék meg pontos teendőiket és feladatukat, valamint felelősségüket az adatvédelem és az adatkezelés tekintetében**.
- az alkalmazottak **kötelesek valamennyi birtokukba jutott adatot biztonságosan kezelni, munkavégzésük során elővigyázatosnak lenni, és a jelen adatvédelmi szabályzatban meghatározott feladatokat végrehajtani**.
- az Önkormányzat, valamint a Hivatal alkalmazottai **a munkájuk során gondoskodnak arról, hogy jogosulatlan személyek ne tekinthessenek be**

személyes adatokba, továbbá arról, hogy a személyes adat **tárolása, elhelyezése úgy kerüljön kialakításra, hogy az jogosulatlan személy részére ne legyen hozzáférhető, megismerhető, megváltoztatható, megsemmisíthető**.

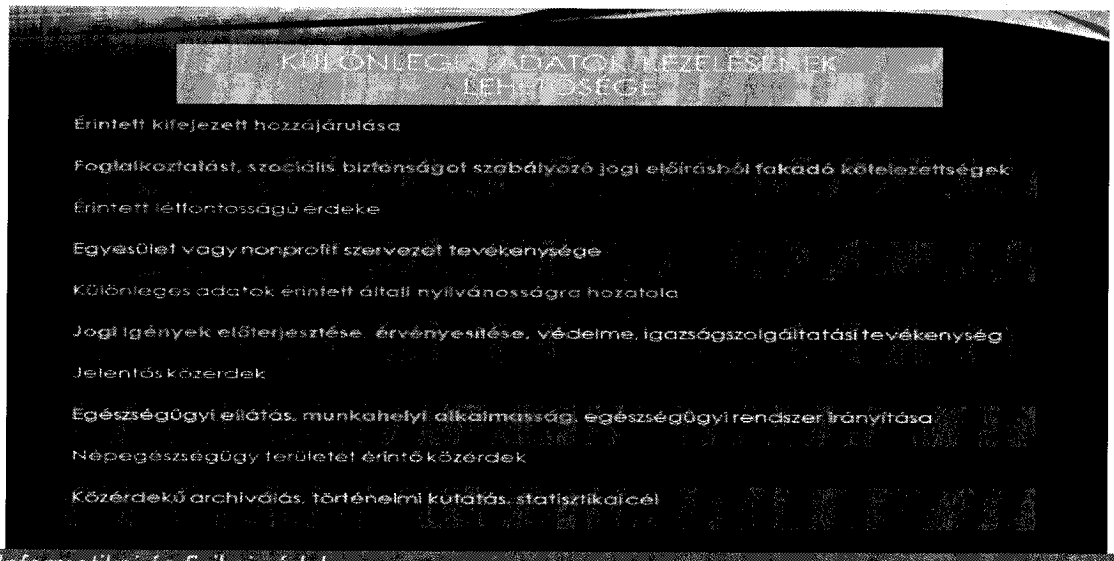
- az alkalmazottak köteles **a szoftveres hozzáférés esetén erős és titkos jelszavakat alkalmazni, a jelszót megosztani, másnak felfedni még a szervezetrendszeren belül is szigorúan tilos**.
- a személyes adatokkal dolgozó alkalmazottak **a munkaterület elhagyása során kötelesek a felhasznált eszközt képernyőzárral védeni, melyhez egyedi belépési azonosító, illetőleg kód kapcsolódik.**
- az alkalmazottak napi operatív tevékenységük során **tilos a saját gépre személyes adatokat menteniük, valamennyi adatot kötelező az Önkormányzat, valamint a Hivatal saját belső rendszerére (szerverre), illetőleg a mentés célját szolgáló jogszabályba kijelölt adatbázisokba (anyakönyvi nyilvántartás, választási adatbázis, központi CRM) menteni.**
- a személyes adatokat tartalmazó **file-okat, üzeneteket kóddal, vagy egyéb módon titkosítani szükséges;**
- személyes adat csak **olyan levelezőrendszeren küldhető tovább, melynek biztonsága és zárt jellege garantált, továbbá olyan címzett számára, aki megfelelő és biztos módon beazonosítható olyan személyként, aki a fogadott személyes adatokat jogszerűen megismerheti;**
- a személyes adatok **Európai Gazdasági Térségen túli továbbítása fő szabály szerint tilos**; amennyiben annak továbbítása mégis szükségessé válik, úgy azt **csak olyan fogadó részére szabad továbbítani, aki igazoltan megfelel a GDPR-ban foglalt valamennyi adatvédelmi követelménynek;**
- az alkalmazott **köteles rendszeresen felülvizsgálni és aktualizálni a rendelkezésekre álló adatokat**, annak érdekében, hogy személyes adat **szükségtelenül ne kerüljön sem tárolásra, sem egyéb kezelésre. A már szükségtelenné váló adatok törlése az alkalmazott felelőssége.**
- amennyiben az alkalmazott **bizonytalan a helyes adatkezelés, vagy az adatvédelmi szempontok tekintetében, úgy köteles tanácsért a vezetőjéhez vagy az adatvédelmi tisztségviselőhöz fordulni**.
- ha az alkalmazott **tudomást szerez arról, hogy az általa kezelt személyes adat hibás, hiányos, vagy időszerűtlen, köteles azt helyesbíteni, vagy helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni.**
- az Önkormányzat, valamint a Hivatal adatkezelést végző alkalmazottja **fegyelmi, kártérítési, szabálysértési és büntetőjogi felelősséggel tartozik a munkavégzése, a feladat elvégzése során tudomására jutott személyes adatok jogszerű kezeléséért**, az Önkormányzat, valamint a Hivatal nyilvántartásaihoz rendelkezésére álló **hozzáférési jogosultságok jogszerű gyakorlásáért**.

Az alkalmazottak munkakör- specifikus adatvédelmi feladatainak és felelősségének részletezése és megállapítása **a munkaköri leírásban kerül ismertetésre.**

9. A különleges adatok kezelésére vonatkozó speciális szabályok

A GDPR 9. cikk szerinti személyes adatok kezelése fő szabály szerint tilos.
Különleges adatok:
- faji, etnikai származás, hovatartozás
- politikai vélemény, vallási, világnézeti meggyőződés
- szakszervezeti tagság
- egészségügyi adatok

- a természetes személy egyedi azonosítását célzó genetikai és biometrikus adatok- természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó adatok



10. Informatikai és fizikai védelem

Az Önkormányzat, valamint a Hivatal az alábbi informatikai védelmi eszközöket és módokat alkalmazza:

a) fizikai védelem:

- zárható iroda
- zárható szekrények
- az érzékeny adatokat tároló szervereket különálló zárt szekrényben kell elhelyezni a szekrények nyitását-zárását dokumentálni kell.

b) IT védelem

- tűzfal,
- vírusirtó,
- kémprogram eltávolító,
- kódok,
- rendszertisztító eszközök,
- biztonsági mentések,
- internet elérés biztonsága (router),
- rendszeres számítástechnikai felülvizsgálat,
- felesleges programok és programnyomok törlése,
- zárt forráskódok.

11. Az adattárolás és az adatkezelés módja

A jelen bekezdés célja annak meghatározása, hogy az adatokat hol és milyen módon szükséges kezelni ahhoz, hogy az adatok biztonsága biztosítható legyen. Az adattárolásra vonatkozó további esetleges kérdésekkel a Rendszergazdához, illetőleg az Adatvédelmi tisztségviselőhöz fordulhatnak az Önkormányzat, valamint a Hivatal alkalmazottai.

Az adatokat az irattározási jogszabályok és belső szabályzatok, elsősorban az **irattári terv** szerint meghatározott ideig kezeli az Önkormányzat, valamint a Hivatal.

Ha az adatot az érintett hozzájárulásával kezeli az Önkormányzat, valamint a Hivatal, de a **hozzájárulását visszavonja az érintett, akkor más jogalap hiányában az adatot véglegesen és visszavonhatatlanul törli** az Önkormányzat, valamint a Hivatal.

a) Papír alapú adatkezelés

Fizikai megsemmisülése elleni védelem

Kiemelt figyelmet kell szentelni az adatállomány fizikai megsemmisülése elleni védelemnek.

Fizikai megsemmisülés elleni védelemi szabályok a papír alapú nyilvántartások esetében:

- Tűzvédelem

  A jegyző a tűzvédelem érdekében gondoskodik a tűzvédelmi szabályzatban előírtak fokozott betartásáról és ellenőrzéséről, különös tekintettel

  - a tűzveszélyforrást jelentő fűtőberendezésekre, valamint arra, hogy azok közelében gyúlékony anyag, eszköz ne legyen,
  - az elektromos tűzveszélyforrást jelentő berendezésekre, továbbá arra, hogy a szükséges áramtalanítási feladatokat ellássák, a nem üzemképes berendezések használatát megtiltsák, a géphasználat tilalmát a gépen jelöljék stb.
  - egyéb, pl.: nyílt láng használatával, illetve robbanásveszéllyel járó anyagok használatának tilalmára.

- Vízkár elleni védelem

  A vízkár elleni védekezés érdekében a papír alapú nyilvántartásokat a tárolóhelyen úgy kell elhelyezni, hogy azok, egy esetleges vízkár esetén a legkevésbé sérüljenek.

- Egyéb fizikai kár elleni védelem

  Gondoskodni kell arról, hogy a nyilvántartáshoz csak az arra kijelölt személy, személyek férjen(ek) hozzá.

Jogosulatlan hozzáférés elleni védelem

- Az adatok védelme a tároló helyek zárásával

  A papír alapon kezelt adatokat olyan biztonságos helyen szükséges tárolni, ahol arra jogosulatlan személy azokat nem ismerheti meg. Az adatokhoz való illetéktelen hozzáférés megakadályozását a tároló eszköz, illetve helyiség zárásával kell megoldani, melybe kötelező az iratokat az alkalmazott irattárolási rendnek megfelelően a használatot követően azonnal visszahelyezni, illetőleg újonnan bele tenni.

  A tárolók kulcsával csak azok a köztisztviselők rendelkezhetnek, akiket a jegyző erre feljogosított.

  Amennyiben a tárolóeszköz kulcsa elveszik, azt haladéktalanul jelenteni kell a jegyzőnek, aki gondoskodik a zár lecseréléséről.

- Az adatok védelme az adatkezelés során

  Az adatkezelés során, az adatkezelő helyiségbe csak olyan személy léphet be, aki adatkezelésre jogosult.

  Ügyfél érkezése esetén az adatkezelést meg kell szakítani, a dokumentumokat el kell zárni.

  Az adatokat csak az arra jogosultak ismerhetik meg, azokhoz más nem férhet hozzá.

  A folyamatos aktív kezelésben lévő iratokhoz csak az illetékesek férhetnek hozzá.

Az Önkormányzat, valamint a Hivatal adatkezelést végző alkalmazottai a munkavégzés befejeztével a papíralapú adathordozót elzárja;

Az Önkormányzat, valamint a Hivatal működése során nem vihető ki személyes adatokat tartalmazó iratok az Önkormányzat, valamint a Hivatal székhelyéről vagy telephelyéről. Amennyiben ez mégis szükségessé válna, úgy e tekintetben az alkalmazott kötelesek azt bejelenteni, és egyedi jóváhagyást kérni a felettesüktől.

- Az adatok védelme érdekében vezetett adatkezelési nyilvántartás

Az adatok védelme érdekében az adatkezelésről az e szabályzat külön pontjában meghatározott nyilvántartásokat kell vezetni. A jegyző ellenőrzi a nyilvántartás naprakészségét, valamint az adatkezelők körét, és adatkezelésük jogszerűségét.

A nyilvántartások tárolási, kezelési helyének kijelölésekor ügyelni kell arra, hogy a helyiségbe történő illetéktelen és erőszakos behatolás elleni védelem biztosítva legyen.

Azokat az elektronikus úton érkezett vagy kezelt adatokat, melyek valamely okból nyomtatásra kerülnek elzárt irattárolóban, illetőleg elkülönítetten szükséges kezelni. Az Önkormányzat, valamint a Hivatal alkalmazottai kötelesek gondoskodni arról, hogy a kinyomtatott iratokhoz arra jogosulatlan személyek ne férjenek hozzá. A kinyomtatott adatokat tartalmazó iratokat azonnal szükséges megsemmisíteni akkor, amikor a kinyomtatás oka megszűnik.

Amennyiben a papíralapon kezelt személyes adatok digitalizálásra kerülnek, a digitálisan tárolt dokumentumokra irányadó biztonsági szabályokat alkalmazza az Önkormányzat, valamint a Hivatal

Amennyiben a papíralapon tárolt személyes adat kezelésének célja már nem áll fenn (adatkezelés határideje letelt), úgy az Önkormányzat, valamint a Hivatal intézkedik a papír megsemmisítéséről.

b) Elektronikus adatkezelés

Az adatkezelés során használt számítógépek az Önkormányzat, valamint a Hivatal tulajdonát képezik.

Az elektronikusan tárolt adatokat védeni szükséges a jogosulatlan eléréstől, véletlen törléstől, és kémprogramokkal/vírusokkal/illetéktelen rendszerfeltörésekkel és rendszertámadásokkal szemben.

Valamennyi adattárolásra szolgáló szervert és számítógépet szükséges tűzfallal, kémprogram védelemmel és vírusirtóval védeni.

Az adatokat tilos a vállalat tulajdonában nem álló számítógépre, illetőleg egyéb adattároló eszközre menteni.

A különleges adatokat is tartalmazó fájlokat csak annyi ideig szabad online rendszerben (akár levelező rendszeren) tárolni, ameddig a feltétlenül szükséges, egyéb esetekben a megőrzési időtartamra szükséges biztonsági mentés keretében elmenteni.

A különleges adatokat tartalmazó fájlokat vagy álnevesítve, vagy kódolva szabad csak tárolni, a jogosulatlan hozzáférés megelőzése érdekében.

A számítógépen található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal - legalább felhasználói névvel és jelszóval – lehet csak hozzáférni.

Erős jelszavak használata szükséges, melyek cseréjére rendszeresen, de legalább fél évente sor kerül. A jelszavaknak titkosnak, hozzáférhetetlennek kell lenniük, az alkalmazottak nem oszthatják meg azt sem egymás között, sem más személyekkel.

Az adatokkal történő minden számítógépes rekord nyomon követhetően naplózásra kerül;

Az Önkormányzat, valamint a Hivatal informatikai eszközein naplózza a tevékenységeket. A tevékenységek naplózása azt jelenti, hogy az Önkormányzat, valamint a Hivatal minden esetben figyeli és figyelemmel kíséri, hogy pontosan ki és milyen céllal fért hozzá az adatokhoz.

Az Önkormányzat, valamint a Hivatal az alábbiakat naplózza:

a) az adatkezelési művelettel érintett személyes adatok körének meghatározását,

b) az adatkezelési művelet célját és indokát,

c) az adatkezelési művelet elvégzésének pontos időpontját,

d) az adatkezelési műveletet végrehajtó személy megjelölését,

e) a személyes adatok továbbítása esetén az adattovábbítás címzettjét.

Az elektronikus naplóban rögzített adatok kizárólag az adatkezelés jogszerűségének ellenőrzése, az adatbiztonsági követelmények érvényesítése, továbbá büntetőeljárás lefolytatása céljából ismerhetők meg és használhatók fel.

Az adatkezelés célja: A **személyes adatokkal elektronikus úton végzett adatkezelési műveletek jogszerűségének ellenőrizhetősége céljából** gyűjti és kezeli az Önkormányzat, valamint a Hivatal.

A naplózási tevékenység jogalapja: jogszabályi rendelkezés írja elő (2011. évi CXII. törvény, azaz az Infotörvény)

A naplótevékenység során rögzített adatokat a Önkormányzat, valamint a Hivatal az adattörlést követően 10 (tíz) évig őrzi.

Szerveren tárolt adatokhoz csak megfelelő jogosultsággal és csakis az arra kijelölt személyek férhetnek hozzá.

Amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájl visszaállíthatatlanul törlésre kerül, az adat újra vissza nem nyerhető.

Személyes adatok külső adathordozóra mentése nem megengedett, kivéve, ha az az elvégzendő feladat alapján indokolt. Ilyen esetekben az adatmentés kizárólag az Önkormányzat, valamint a Hivatal tulajdonában és kezelésében álló adathordozóra történhet, egyedi engedély alapján.

Olyan adathordozó, amely nem áll az Önkormányzat, valamint a Hivatal tulajdonban és/vagy kezelésében, az Önkormányzat, valamint a Hivatal számítógépeihez nem csatlakoztathatok.

Amennyiben az adat hordozható adattárolón (CD, DVD, pendrive, egyéb külső adattároló) kerül rögzítésre, ezek az adattároló eszközöket a használatot követően biztonságos helyen, jogosulatlan személyek számára hozzáférhetetlenül szükséges tárolni.

Személyes adatokat tartalmazó adatbázisok aktív adataiból napi mentést végez.

Felhő alapú szolgáltatás igénybevételével adat csak a kijelölt és meghatározott szolgáltatóval kötött szerződés alapján és szerint tárolható. Az Önkormányzat, valamint a Hivatal az adattárolás megkezdése előtt meggyőződik arról, hogy a felhő alapú szolgáltatást biztosító partner megfelel az adatvédelem jogszabályi és technikai követelményeknek.

A tárolt adatokat rendszeresen szükséges felülvizsgálni.

Az adattárolásra alkalmazott szoftvereket rendszeresen frissíteni szükséges. A frissítés megkezdése előtt a szoftverfrissítési metódust az adatvesztés elkerülése érdekében tesztelni szükséges.

c) Postai küldeményekre vonatkozó speciális szabályok

A postai küldemények átvételére az Önkormányzat, valamint a Hivatal által kijelölt alkalmazott jogosult. Átvételre jogosult lehet más, az Önkormányzat, valamint a Hivatal által meghatározott személy is. A kiadmányozási jog és annak gyakorlása tekintetében a Hivatal és az Önkormányzat egyéb szabályzatai irányadók.

12. Az adatok felhasználása

Az adatkezelések célja elsősorban közhatalmi feladatok, jogi kötelezettségek teljesítése.
Az Önkormányzat, valamint Hivatal az alábbiak szerint használja fel az adatokat:

- Jogszabályban meghatározott feladatainak ellátása a közigazgatási ügyek
- tekintetében
- Jogszabályban meghatározott nyilvántartási kötelezettségek teljesítése végett
- Közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtása
- Az érintett azonosítása, az érintettel való kapcsolattartás
- Elemzések, statisztikák készítése, a szolgáltatások fejlesztése - ezen célból az adatkezelő csak anonimizált adatokat, személyazonosításra alkalmatlan összesítéseket használ fel
- Tájékoztatás adatvédelmi incidens esetére
- Adatkezelői esetlegesen adatfeldolgozói nyilvántartás vezetése
- Kapcsolatfelvétel esetén, e-mailben vagy telefonon való tájékoztatás, értesítés
- Munkaviszonnyal kapcsolatos adatkezelés
- Köztisztviselői jogviszonnyal kapcsolatos adatkezelés
- Szerződéshez kapcsolódó adatkezelések

Az Önkormányzat, valamint a Hivatal a kezelt adatok tekintetében részletes adatvédelmi nyilvántartást (adattérképet) készít, továbbá az adatfeldolgozás és az adattovábbítás tekintetében adatfeldolgozói és adattovábbítási nyilvántartást vezet.

13. A kezelt adatok pontossága

Az Önkormányzatnak, valamint a Hivatalnak jogszabályi kötelezettsége az általa kezelt személyes adatok naprakész és pontos nyilvántartása.

Az Önkormányzat, valamint a Hivatal kiemelt figyelmet fordít az esetlegesen (és szükségesen) nyilvántartott különleges adatok naprakészségére és pontosságára.

A fentiek okán az Önkormányzat, valamint a Hivatal valamennyi alkalmazottjának kiemelt feladata, hogy a tőle telhető legjobb módon az adatokat naprakészen és pontosan tartsa nyilván.

Az adatokat a lehető legkevesebb adattároló helyen szükséges tartani, az Önkormányzat, valamint a Hivatal alkalmazottai feleslegesen és engedély nélkül semmilyen egyéb nyilvántartást, vagy személyes adatokat tartalmazó egyéb forrást nem készíthetnek.

Az Önkormányzat, valamint a Hivatal alkalmazottai kötelesek azon lenni, hogy a személyes adatok naprakészek legyenek, és kötelesek az adatokat az érintettel- és egyéb kapcsolatok során folyamatosan egyeztetni.

Az Önkormányzat, valamint a Hivatal az érintettek számára folyamatosan biztosítja az adatpontosítás lehetőségét.

Amennyiben a kezelt adatok körében pontatlan adatok kerülnek elő, azt haladéktalanul pontosítani szükséges, így különösen, ha az érintett az általa megadott telefonszámon vagy elektronikus levelezési címen már nem érhető el. Az elektronikus levelezés mindaddig elérhetőnek tekinthető, ameddig az érintett a cím megváltozását nem jelenti be, vagy onnan a kézbesítés sikertelenségére vonatkozó rendszerüzenet vissza nem érkezik. Az érintett jelzésének hiányában is pontatlannak bizonyult adatot valamennyi rendszerből és adattárolóról a pontatlanság megállapítását követően haladéktalanul törölni szükséges.

14. Hatásvizsgálat

Amennyiben a Önkormányzat, valamint a Hivatal új adatkezelési folyamat bevezetését tervezi, és amennyiben ezen új adatkezelési folyamat valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve – *figyelemmel annak jellegére, hatókörére, körülményére és céljaira* - akkor az adatkezelés megkezdését megelőzően az Önkormányzat, valamint a Hivatal hatásvizsgálatot folytat le arra vonatkozóan, hogy az adatkezelési folyamat a személyes adatok védelmét hogyan érinti.

Az adatvédelmi hatásvizsgálat lényege az adatkezelés előzetes kontrollja.

Amelynek során az adatkezelő a tervezett adatkezelési műveletet vagy műveleteket áttekinti, annak jellegére, körülményeire, hatókörére (érintettekre gyakorolt hatására), céljaira, tekintettel.

Megvizsgálja és felméri annak kockázatait, a kockázatok kezelésének módját, és a kockázatok mérséklésére teendő intézkedéseket tesz.

Egymáshoz hasonló adatkezelési műveletek, amelyek hasonló kockázatokat jelentenek egyetlen egy hatásvizsgálat keretében is elvégezhetők.

Az Önkormányzat, valamint a Hivatal az adatvédelmi hatásvizsgálat lefolytatására a francia adatvédelmi hatóság (CNIL) által kiadott, és magyar nyelven is elérhető PIA szoftver hazai Nemzeti Adatvédelmi és Információszabadság Hatóság weblapján keresztül elérhető változatát alkalmazza.

A hatásvizsgálatot főszabály szerint a Hivatalt érintő ügyekben a jegyző, az Önkormányzatot érintő ügyekben pedig a polgármester végzi. azzal, hogy az Önkormányzat, valamint a Hivatal köteles kikérni az adatvédelmi tisztviselő szakmai tanácsát. Az adatvédelmi tisztségviselő felkérhető a hatásvizsgálat tervezetének előkészítésére, amennyiben ahhoz számára minden lényeges tényadatot a rendelkezésére bocsátottak.

15. Érdekmérlegelés

Lehetőség van hozzájárulás nélküli adatkezelésre, ha ezt valamilyen jogos érdek lehetővé teszi, feltéve, hogy az Adatkezelő eleget tesz tájékoztatási kötelezettségének.

Az adatkezelés jogalapjának vizsgálata során a GDPR 6. cikk (1) bekezdése a) - f) pontjai az irányadók.

Amennyiben a jogalapot a GDPR 6. cikk (1) bekezdés f) pontja jelenti, az adatkezelési folyamat akkor lesz jogszerű, amennyiben az adatkezelés az adatkezelő vagy az érintett esetleg mindkettő jogos érdekeinek érvényesítéséhez szükséges, és felülmúlja az érintett személyes adatainak védelméhez fűződő érdekeit, alapvető jogait és szabadságait.

Az adatkezelés jogszerűségének vizsgálatához az Önkormányzat, valamint a Hivatal elvégez egy érdekmérlegelési tesztet, mely során az adatkezelés céljának szükségességét és az érintettek jogainak és szabadságainak arányos mértékű korlátozását vizsgálja és megfelelően alátámasztja.

16. Hozzájáruláson alapuló adatkezelés

Amennyiben az Önkormányzat, valamint a Hivatal hozzájáruláson alapuló adatkezelést kíván végezni, az érintett hozzájárulását személyes adatai kezeléséhez a *Hozzájáruló Nyilatkozatban* foglalt tartalommal és tájékoztatással kell kérni.

Az elszámoltathatóság elvéből is következően, ha az adatkezelés hozzájáruláson alapul, az adatkezelőnek kell igazolnia, hogy az érintett a személyes adatainak kezeléséhez hozzájárult.

Az érintett jogosult arra, hogy hozzájárulását bármikor visszavonja. Ugyanakkor a hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét. A hozzájárulás megadása előtt az érintettet erről tájékoztatni kell. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.

A hozzájárulás visszavonását *Hozzájárulást visszavonó nyilatkozatban* foglalt tartalommal és tájékoztatással kell kérni.

A hozzájárulás visszavonhatósága is mutatja, hogy olyan esetekben, amikor más jogalap is rendelkezésre áll, akkor azt kell használni.

17. Az érintettek jogai

Valamennyi érintett, akinek az Önkormányzat, valamint a Hivatal a személyes adatait kezeli jogosult:

- tájékoztatást kérni arról, hogy milyen okból és mely adatait kezeli az Önkormányzat, valamint a Hivatal ;
- tájékoztatást kérni azon címzettekről vagy címzettek kategóriáiról, akikkel, illetve amelyekkel a személyes adatokat közölni fogják, ideértve különösen a harmadik országbeli címzetteket, nemzetközi szervezeteket;
- adott esetben a személyes adatok tárolásának időtartamáról, vagy ha ez nem lehetséges, az időtartam meghatározásának szempontjairól tájékoztatást kérni;
- kérheti az adatok helyesbítését, törlését vagy kezelésének korlátozását, tiltakozhat a személyes adatok kezelése ellen;
- ha az adatokat az Önkormányzat, valamint a Hivatal nem az érintettől gyűjtötte, a forrásukra vonatkozó valamennyi fellelhető információról jogosult tájékoztatás kérni;
- a Hatósághoz fordulás lehetőségéről tájékoztatást kérni;
- tájékoztatást kérni arról, hogy hogyan érheti el az Önkormányzat, valamint a Hivatal által kezelt adatokat;
- tájékoztatást kérni arról, hogy az Önkormányzat, valamint a Hivatal naprakészen tartja- e az adatait, és milyen intézkedéseket hozott a naprakészen tartás érdekében;
- tájékoztatást kérni arról, hogy az Önkormányzat, valamint a Hivatal hogyan teljesíti az adatvédelmi kötelezettségeit.

Amennyiben valamely érintett a fenti tájékoztatások egyikét kéri, azt az „érintett hozzáférési jogának" hívjuk.

Az érintett hozzáférési joga e-mailen érkezhet, az Önkormányzat, valamint a Hivatal hivatal@bokod.hu elektronikus levelezési címeire, továbbá az Önkormányzat, valamint a Hivatal alkalmazottai útján, valamint a Önkormányzat, valamint a Hivatal postai levelezési címére érkezett

megkereséssel, végül személyes vagy telefonos megkeresés útján. Az Önkormányzat, valamint a Hivatal az ilyen igények bejelentésére űrlapot alkalmazhat, melyet az érintetteknek azonban nem kötelező alkalmazni, az egyéb úton történő bejelentés is érvényes bejelentésnek minősül.

Az Önkormányzat, valamint a Hivatal az érintett hozzáférési kérelmének fél éven belüli *megismételt teljesítéséért* adminisztrációs díjat kérhet. Az Önkormányzat, valamint a Hivatal az érintett kérelmét 30 (harminc) napon belül köteles teljesíteni.

Az érintettnek joga van továbbá:

- hozzájáruláson alapuló adatkezelés esetén a hozzájárulását visszavonni;
- tiltakozni a személyes adatai kezelése ellen;
- kérni az adatai más szerv/személy részére történő hiánytalan továbbítását (adathordozhatóság).

Az Önkormányzat, valamint a Hivatal minden esetben pontosan azonosítja az adatkérő személyét a kért információ kiadását megelőzően.

Az Önkormányzat, valamint a Hivatal vezetője- az adatvédelmi tisztségviselővel való egyeztetést követően- jogosult dönteni az érintett kérelméről. Ha alkalmazotthoz érkezik a megkeresés, azt haladéktalanul köteles az Önkormányzat, valamint a Hivatal vezetője részére továbbítani.

18. *Az adatok egyéb okból történő hozzáférhetővé tétele*

Meghatározott feltételek mellett a GDPR Rendelet megengedhetővé teszi azt, hogy jogérvényesítési okokból az érintett hozzájárulása nélkül is más számára megismerhetővé tegye az egyes személyes adatokat.

Az Önkormányzat, valamint a Hivatal jogosult a személyes adatokat másokkal megosztani azzal. hogy a megosztás kizárólag az igényérvényesítéshez szükséges terjedelemben és okból, illetőleg kizárólag jogszerű megkeresés alapján, szükség esetén ügyvéd, adatvédelmi tisztségviselő tanácsának kikérése mellett történik.

19. *Az adatok adatfeldolgozó és önálló adatkezelő részére történő átadása*

Az Önkormányzat, valamint a Hivatal szervezetén kívül az Önkormányzat, valamint a Hivatal saját ügymenetének biztosítása végett az alábbi okból és személyekkel (a jelen szabályzatban a továbbiakban: Szolgáltató Partner) osztja meg az érintettre vonatkozó személyes adatokat:

Adatfeldolgozó:

- elektronikus számla kiállítását segítő felhő alapú alkalmazás)
- *számlázóprogram*
- *webszerkesztő*
- *tárhelyszolgáltató*
- *informatikus*
- *mobiltelefon, mobil internet és vezetékes telefon szolgáltató*
- *Internet szolgáltató*

Önálló adatkezelő:

- *banki szolgáltató*

- **Magyar Posta Zrt.** *(postázási szolgáltatások)*
Adatvédelmi tájékoztató: https://www.posta.hu/adatkezelesi_tajekoztato

Az Önkormányzat, valamint a Hivatal minden esetben, valamennyi Ügyfélkiszolgáló együttműködő partner tekintetében az adatok továbbításának megkezdése előtt meggyőződik arról, hogy az adott partner az Európai Uniós és magyarországi adatvédelmi szabályoknak megfelelően jár el. Az Önkormányzat, valamint a Hivatal valamennyi partnerrel írásbeli szerződést köt, melyben rögzítésre kerül:

- az adatkezelés módja;
- az adatkezelés időtartama;
- a közös adatkezelők közötti felelősség- és feladatmegosztást;
- a közös adatkezelők érintettekkel szembeni szerepét és a velük való kapcsolatukat;

Az Önkormányzat, valamint a Hivatal minden esetben biztosítja, hogy a közös adatkezelők közötti megállapodás kivonatolt személyes adatok kezelésére vonatkozó lényegi megállapításait az érintettek tudomására hozza.

Az Önkormányzat, valamint a Hivatal szervezetén kívül adatfeldolgozási céllal megosztott adatok tekintetében az adatfeldolgozási tevékenységre az alábbi tartalommal feltétlenül rendelkező szerződéseket köt:

- A Szerződő felek pontosan meghatározzák azt az adatfeldolgozási tevékenységet, amelye a szerződés létrejött (tárgy).
- A Szerződő felek meghatározzák az adatfeldolgozás célját.
- A Szerződő Felek meghatározzák azokat a személyes adatokat (jelleg, típus szerint), melyekre az adatfeldolgozási tevékenység irányul.
- A Szerződő Felek meghatározzák általánosan, de az érintetti kör tekintetében azonosíthatóan az érintettek körét (akiknek az adatai feldolgozásra kerülnek).
- A Szerződő Felek meghatározzák azt az időtartamot, ameddig az adatfeldolgozási tevékenységet folytatja az adatfeldolgozó (ha folyamatos a szerződés, akkor határozatlan időre kötik).
- A Szerződő Felek kikötik, hogy az adatfeldolgozó az Önkormányzat, valamint a Hivataltól elkülönült szervezetként kizárólag az Önkormányzat, valamint a Hivatal által adott írásbeli utasításai alapján dolgozza fel, az adatfeldolgozó önálló adatkezelési tevékenységet az adatfeldolgozási szerződéssel érintett adatokkal kapcsolatban nem végez.
- A Szerződő Felek kikötik, hogy az adatfeldolgozónak haladéktalanul tájékoztatnia kell arról az Önkormányzatot, valamint a Hivatalt, ha az adatfeldolgozási utasítás adatvédelmi rendelkezésekbe ütközik.
- A Szerződő Felek kikötik az adatfeldolgozó titoktartási kötelezettségét, illetőleg rögzítik azt, ha az adatfeldolgozó titoktartási szakmai szabályok hatálya alá tartozik.
- A Szerződő Felek kikötik, hogy az adatfeldolgozó az adatbiztonsági követelményeknek megfelel, a szükséges titkosítási, álnevesítési intézkedéseket az adatok biztonsága érdekében végrehajtja.
- A Szerződő Felek kikötik, hogy az adatfeldolgozó csak az Önkormányzat, valamint a Hivatal Külön írásbeli hozzájárulásával vehet igénybe további adatfeldolgozót, illetőleg rögzítik, hogy az adatfeldolgozónál pontosan milyen további adatfeldolgozók igénybevétele történik, kikötve a további adatfeldolgozással szembeni tiltakozás jogát, azzal, hogy az adatfeldolgozó partner biztosítja, hogy az általa igénybe vett további adatfeldolgozóra az Önkormányzat, valamint a Hivatal -vel kötött szerződésben foglaltaknak megfelelő kötelezettségeket telepít.
- A Szerződő Felek kikötik, hogy az adatfeldolgozási szerződés teljesítése során kölcsönösen együttműködnek az érintetti jogok biztosítása és érvényre juttatása érdekében.

- A Szerződő Felek rögzítik, hogy az adatfeldolgozási szerződés megszűnését, avagy megszüntetését követően az adatfeldolgozó az Önkormányzat, valamint a Hivatal által az adatfeldolgozó részére továbbított adatokat, illetőleg az adatfeldolgozás során keletkezett valamennyi további adatot a Önkormányzat, valamint a Hivatal döntésének megfelelően törtöl, avagy visszajuttatja azt az Önkormányzat, valamint a Hivatal -nek.
- A Szerződő Felek megállapodnak abban, hogy az adatfeldolgozó minden olyan adatot kiad és visszaszolgáltat az Önkormányzat, valamint a Hivatal -nek, amely ahhoz szükséges, hogy az Önkormányzat, valamint a Hivatal az adatvédelmi kötelezettségeit teljesíteni tudja, különös tekintettel az érintettek tájékoztatására vonatkozó feladatokra.
- A Szerződő Felek megállapodnak abban, hogy az Önkormányzat, valamint a Hivatal , vagy az erre a feladatra szerződött partnere az adatfeldolgozónál auditot tarthat annak érdekében, hogy az adatfeldolgozási tevékenységre vonatkozó adatvédelmi követelmények adatfeldolgozó általi teljesítését ellenőrizze, és az érintetti jogok érvényre juttatását biztosíthassa.
- A Szerződő Felek kikötik, hogy adatvédelmi incidens esetén az adatfeldolgozó haladéktalanul köteles értesíteni az Önkormányzatot, valamint a Hivatalt, valamint a kárfelmérésben és a kárenyhítésben, illetőleg az adatvédelmi elemzés és vizsgálat során kölcsönösen együttműködnek, továbbá minden szükséges információt közösen megadnak egymásnak ahhoz, hogy az érintetti jogok sérelmét enyhítsék vagy megelőzzék.

20. Tájékoztatási kötelezettség teljesítése

Az Önkormányzat, valamint a Hivatal biztosítja, hogy az érintettek tisztában legyenek azzal, hogy a személyes adataik feldolgozásra kerülnek, és felvilágosítást kapjanak arról, hogy:

- hogyan használják/dolgozzák fel az adataikat;
- hogyan érvényesíthetik a jogaikat.

A fenti okból az Önkormányzat, valamint a Hivatal adatvédelmi tájékoztatót készít, és könnyen hozzáférhetővé teszi a magánszemélyek számára, még az adatkezelés megkezdését megelőzően. Az adatvédelmi tájékoztató minden adatkezelési művelet vagy műveletsorozat tekintetében külön- külön meghatározza az érintettek jogait, továbbá rögzíti az adatkezelés célját, módját, idejét.

Az adatkezelési tájékoztatót az Önkormányzat, valamint a Hivatal az érintett kérésére bármikor megküldi, azzal, hogy az adatvédelmi tájékoztató az Önkormányzat, valamint a Hivatal weblapján is megtalálható.

21. A személyes adatok törlése

Az Önkormányzat, valamint a Hivatal törli a személyes adatokat, ha

- a személyes adatra nincsen szükség abból a célból, amelyből gyűjtötte vagy más módon kezelte;
- az érintett a hozzájárulását visszavonja, és az adatkezelésnek más jogalapja nincsen;
- a személyes adatok kezelése valamely okból jogellenesen történt;
- a személyes adatokat jogi kötelezettség teljesítése érdekében törölni kell;
- a személyes adat gyermekre vonatkozik.

A törlés szükségességének felismerése az alkalmazott feladata, aki azt- amennyiben a törlés szükségessége tekintetében bizonytalan- köteles a vezetőjének, illetőleg az adatvédelmi tisztségviselőnek jelezni.

Az Önkormányzat, valamint a Hivatal nem töröl olyan adatot, mely a jogi kötelezettsége teljesítéséhez, illetőleg a jogai érvényesítéséhez szükséges.

A személyes adatok törlése végleges, és helyreállíthatatlan módon, igazolhatóan valósul meg, melyet vagy digitális bejegyzés, vagy egyéb feljegyzés igazol.

22. Intézkedések adatvédelmi incidens esetén

Az Önkormányzat, valamint a Hivatal alkalmazottai bármely adatvédelmi incidens esetén azonnal köteles értesíteni az Önkormányzatot, valamint a Hivatalt, illetőleg adatvédelmi tisztségviselőjét, akiknek haladéktalanul vizsgálatot kell indítaniuk az incidens kockázatának felmérésére.

Amennyiben az adatvédelmi incidens magas kockázatot jelent az érintett jogaira nézve, úgy az Önkormányzat, valamint a Hivatal legkésőbb 72 (hetvenkét) órán belül köteles azt bejelenteni a Nemzeti Adatvédelmi és Információszabadság Hatóság incidens- bejelentési nyilvántartási rendszerébe.

A bejelentésben:

- ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket
- ismertetni kell az adatkezelő által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket;

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

Az Önkormányzat, valamint a Hivatal nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az Önkormányzat, valamint a Hivatal indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell:

- az adatvédelmi tisztségviselő neve és elérhetősége;
- az adatvédelmi incidensből eredő, valószínűsíthető következményeket
- az Önkormányzat, valamint a Hivatal által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az Önkormányzat, valamint a Hivatal mellőzi az érintett tájékoztatását, ha a következő feltételek bármelyike teljesül:

- az Önkormányzat, valamint a Hivatal 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 Önkormányzat, valamint a Hivatal 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;

- 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.

23. Adatfeldolgozói tevékenységre vonatkozó szabályok

Az adatfeldolgozás jogalapja az Önkormányzat, valamint a Hivatal és az adatkezelő között fennálló szerződéses kötelezettség.

Az Önkormányzat, valamint a Hivatal a személyes adatokat kizárólag az Adatkezelővel kötött írásbeli szerződés alapján kezeli és dolgozza fel.

A személyes adatok az Önkormányzat, valamint a Hivatal részére a tevékenysége ellátása során jutnak a tudomására.

Az Önkormányzat, valamint a Hivatal tevékenysége során az Adatkezelő állapítja meg a személyes adatok kezelésének céljait és módszereit, valamint kizárólag az Adatkezelő írásbeli utasítása alapján jár el, kivéve, ha az adatkezelést az Adatfeldolgozóra alkalmazandó uniós vagy tagállami jog írja elő. Ebben az esetben az Önkormányzat, valamint a Hivatal az Adatkezelőt az adatkezelést megelőzően értesíti, kivéve, ha az Adatkezelő értesítését az adott jogszabály fontos közérdekből tiltja.

Elsősorban a szerződésben foglaltak tekintendők írásbeli adatkezelői utasításnak. A szerződésben nem szabályozott esetben az utasítás írásbeliségére a Szerződés kapcsolattartásra vonatkozó szabályai az irányadók.

A kezelt személyes adatok az Önkormányzat, valamint a Hivatal tevékenységéből, szerződéses kötelezettségéből származó.

Az Önkormányzat, valamint a Hivatal, mint adatfeldolgozó kötelezettségei és jogai

Értesíti az Adatkezelőt, amennyiben megítélése szerint valamely utasítás az Adatvédelmi jogszabályokba ütközik, és ezen a véleményét megindokolja.

Az Önkormányzat, valamint a Hivatal a szerződésben meghatározott feladatok ellátása érdekében megfelelő ismerettel és gyakorlattal rendelkező személyeket köteles igénybe venni.

Köteles továbbá gondoskodni az általa igénybe vett személyek felkészítéséről, hogy megfelelő képzésben részesüljenek a betartandó adatvédelmi jogszabályi rendelkezések, a szerződésben, valamint a jelen szabályzatban foglalt kötelezettségek, valamint az adatfelvétel célja és módja tekintetében.

Az Önkormányzat, valamint a Hivatal biztosítja, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak. Adatkezelő erre irányuló kérése esetén az Önkormányzat, valamint a Hivatal köteles haladéktalanul az Adatkezelő rendelkezésére bocsátani a titoktartási kötelezettség vállalását alátámasztó dokumentumokat.

Adatbiztonság:

Az Önkormányzat, valamint a Hivatal gondoskodik az adatok biztonságáról, megteszi azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek az adatbiztonság követelményének érvényesülését biztosítják.

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

Az Önkormányzat, valamint a Hivatal gondoskodik arról, hogy a tárolt adatokhoz belső rendszeren keresztül vagy közvetlen hozzáférés útján kizárólag az arra feljogosított személyek, és kizárólag az adatkezelés céljával összefüggésben férjenek hozzá.

Az Önkormányzat, valamint a Hivatal gondoskodik a felhasznált eszközök szükséges, rendszeres karbantartásáról, fejlesztéséről.

Az adatokat tároló eszközt megfelelő fizikai védelemmel ellátott zárt helyiségben helyezi el, gondoskodik annak fizikai védelméről is.

Informatikai nyilvántartások védelme

Az Önkormányzat, valamint a Hivatal az informatikai védelemmel kapcsolatos feladatai körében gondoskodik különösen:

- a jogosulatlan hozzáférés elleni védelmet biztosító intézkedésekről, ezen belül a szoftver és hardver eszközök védelméről, illetve a fizikai védelemről ***(hozzáférés védelem, hálózati védelem)***;
- az adatállományok vírusok elleni védelméről ***(vírusvédelem)***;
- az adatállományok helyreállításának lehetőségét biztosító intézkedésekről, ezen belül a rendszeres biztonsági mentésről és a másolatok elkülönített, biztonságos kezeléséről ***(tükrözés, biztonsági mentés)***;
- az adatállományok, illetve az azokat hordozó eszközök fizikai védelméről, ezen belül a tűzkár, vízkár, villámcsapás, egyéb elemi kár elleni védelemről, illetve az ilyen események következtében bekövetkező károsodások helyreállíthatóságáról ***(archiválás, tűzvédelem)***.

Papíralapú nyilvántartások védelme

Az Önkormányzat, valamint a Hivatal a papíralapú nyilvántartások védelme érdekében megteszi a szükséges intézkedéseket különösen a fizikai biztonság, illetve tűzvédelem tekintetében. Az alkalmazottak és egyéb, Önkormányzat, valamint a Hivatal érdekében eljáró személyek az általuk használt, vagy birtokukban lévő, személyes adatokat is tartalmazó adathordozókat, függetlenül az adatok rögzítésének módjától, kötelesek biztonságosan őrizni, és védeni a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.

További adatfeldolgozó igénybevétele

Az Önkormányzat, valamint a Hivatal a további adatfeldolgozó igénybe vételét megelőzően tájékoztatja az adatkezelőt a további adatfeldolgozó személyéről, valamint a további adatfeldolgozó által végzendő tervezett feladatokról.

Ha az adatkezelő ezen tájékoztatás alapján a további adatfeldolgozó igénybe vételével szemben kifogást emel, a további adatfeldolgozó igénybevételére az adatfeldolgozó kizárólag a kifogásban megjelölt feltételek teljesítése esetén jogosult.

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

Együttműködés az Adatkezelővel

Az Önkormányzat, valamint a Hivatal minden megfelelő eszközzel segíti az Adatkezelőt az érintettek jogai érvényesítésének elősegítése, ezzel kapcsolatos kötelezettségei teljesítése érdekében.

Az Adatkezelő kötelezettségei és jogai

1. Adatkezelő jogosult ellenőrizni az Önkormányzatnál, valamint a Hivatalnál a szerződés szerinti tevékenység végrehajtását.
2. Adatkezelőnek a szerződésben meghatározott feladatokkal kapcsolatos utasításai jogszerűségéért az Adatkezelőt terheli felelősség, ugyanakkor az Önkormányzat, valamint a Hivatal köteles haladéktalanul jelezni az Adatkezelőnek, amennyiben Adatkezelő utasítása vagy annak végrehajtása jogszabályba ütközne.

Adatvédelmi incidens jelentése

Az Önkormányzat, valamint a Hivatal az adatvédelmi incidenst az arról való tudomásszerzést követően indokolatlan késedelem nélkül, de legkésőbb 24 órán belül köteles bejelenteni az Adatkezelőnek az alábbiak szerint:

- ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket
- ismertetni kell az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket;

24. Záró rendelkezések

A szabályzat 2020. március 1. napján lép hatályba.

Bokod, 2020. február 26.

Bokod Község Polgármestere Komárom-Esztergom megye

Csonka László
polgármester

Zsigmond Anikó
jegyző

Bokod Község Jegyzője

1. számú melléklet

Adatvédelmi incidens nyilvántartás

(minta)

Közfeladatot ellátó szerv neve:	**Bejegyzés sorszáma:**
Vezető:	**(Ha van) hatósági bejelentés száma:**
Felelős:	**Adatvédelmi incidens időpontja:**
Bejegyző személy neve:	**A nyilvántartásba jegyzés időpontja:**
Bejegyző személy beosztása:	**(Ha van) kiegészítés időpontja:**
(Ha van) DPO neve, elérhetősége:	
Egyéb megjegyzések:	
Az adatvédelmi incidensre vonatkozó alapadatok:	

Időpont/ időtartam:	**Érintettek száma:**	**Az incidens jellege:**	**Az incidens ismertetés:**	**Tudomásszerzés módja:**	**Érintett adatok köre és száma:**
Egyéb megjegyzések:					
Megtett intézkedések:					

Intézmény itájékoztatás (vezetők, DPO, stb.)	Érintetek tájékoztatás a/tájékoztatás elmaradás indoka	Hatóság tájékoztatása	Megtett sürgősségi intézkedések	Helyreállítási feladatok	Valószínű síthető következmények
Mikor?					
Kit?					
Milyen módon?					
Adatvédelmi incidens súlyosságának értékelése:					

Az Önkormányzat, valamint a Hivatal az adatvédelmi incidensek értékelése során az Európai Hálózatbiztonsági Ügynökség (ENISA) adatvédelmi incidens- értékelési módszertanát alkalmazza.

Az Önkormányzat, valamint a Hivatal az adatvédelmi incidens értékelése során az adatvédelmi incidens- nyilvántartásba az incidenst felvezeti.

Adatkezelési környezet(AK)

Adatkezelési Környezet (AK): az incidenssel érintett adatokat vizsgálja, az adatkezelés összes körülményre tekintettel.

AZ ADATOK TÍPUSÁNAK CSOPORTOSÍTÁSA

- Egyszerű adat
- Viselkedésre/attitűdre vonatkozó adat
- Pénzügyi adat
- Érzékeny adat

AZ ADATTÍPUSOKHOZ TARTOZÓ MÉRŐSZÁMOK TÁBLÁZATA

A táblázat módszertana szerint úgynevezett „viszonyítási pontos rendszer" működik, azaz meghatároz egy eseményt/adatkört, ad rá egy pontszámot, és megvizsgálja, hogy mi súlyosbítja vagy enyhíti a helyzetet az alap pontszámhoz képest.

EGYSZERŰ ADATOK

Életrajzi adat, elérhetőség (név, e-mail stb.), teljes név, családi élet, végzettség, munkahelyi tapasztalat stb.

Adatkezelési környezet	Pontszám
Az adatvédelmi incidens alapvető súlyossági fokozata (viszonyítási pont): Ha valamely adatot megszerezték, és súlyosbító tényező nem merül fel.	1
Ha az adatt típusa szerint, vagy az adatot megszerző egyéb okból az adat segítségével az érintett részbeni profilozását, vagy szociális/ pénzügyi helyzetére vonatkozó megállapításokat és következtetéseket vonhat le.	2
Ha az adatt típusa/ mennyisége szerint, vagy az adatot megszerző egyéb okból az adat segítségével az érintett egészségi állapotára, szexuális irányultságára, politikai preferenciáira vagy vallási- hitbeli meggyőződésére vonatkozó megállapításokat tehet.	3
Ha az adatok érzékeny csoportba tartozó személyekre (pl.hátrányos helyzetűek, kiskorúak stb.) vonatkozik, mivel az adatok kritikusak lehetnek az érzelmi/ mentális/lelki/fizikai fejlődésük tekintetében.	4

VISELKEDÉSRE/ ATTITŰDRE VONATKOZÓ ADAT

Pl. helymeghatározás, közlekedés, személyes érdeklődés, szokások stb.

Az adatvédelmi incidens alapvető súlyossági fokozata (viszonyítási pont) Ha valamely adatot megszerezték, és sem enyhítő, sem súlyosbító körülmény nem merül fel.	2
Ha az incidenssel érintett adat nem enged lényeges betekintést az érintett attitűdjeibe, vagy az adatok az incidenstől függetlenül egyébként nyilvánosan is elérhetőek (pl. a webes keresések alapján történő attitűdre vonatkozó következtetések)	1
Ha az adatt típusa/ mennyisége szerint, vagy az adatot megszerző egyéb okból képes az érintettről részben profilt alkotni, az érintett mindennapi életébe, szokásaiba betekintési lehetőséget ad.	3
Ha az érintett érzékeny adatai segítségével profilozható az érintett.	1

PÉNZÜGYI ADATOK

Bármely, az érintettre vonatkozó pénzügyi adat, így az adózásra, a pénzügyi tranzakciókra, banki státuszra, befektetésekre, hitelkártyákra, számlákra stb. vonatkozó adatok

Az adatvédelmi incidens alapvető súlyossági fokozata (viszonyítási pont) Ha valamely pénzügyi adatot megszerezték, és sem enyhítő, sem súlyosbító körülmény nem merül fel.	3
Ha az incidenssel érintett adat nem enged lényeges betekintést az érintett pénzügyi adataiba (pl. az, hogy az érintett egy adott bank ügyfele, minden további részinformáció nélkül)	1
Ha az incidenssel érintett pénzügyi adat ugyan megszerzésre kerül, de még mindig nem alkalmas az érintett pénzügyeibe történő betekintésre (például bankszámlaszámok név vagy további részletek nélkül)	3
Ha az érintett adatai mennyiségileg vagy minőségileg már lehetőséget biztosítanak a csalásra, vagy részletes szociális/pénzügyi profil felállítására.	4

ÉRZÉKENY ADATOK

A GDPR egyrészt „különleges adatként", másrészt pedig „egyéb okból érzékeny adatként" definiálja.

Az adatvédelmi incidens alapvető súlyossági fokozata (viszonyítási pont) Ha valamely adatot megszerezték, és enyhítő körülmény nem merül fel.	4
Ha a megszerzett adat nem enged semmilyen lényeges betekintést az érintett viselkedésébe, vagy az adatot nyilvánosan is megosztották az adatvédelmi incidenstől függetlenül is.	1
Ha a megszerzett adatok általános következtetés(ek) levonásához vezethet.	2
Ha a megszerzett adatok érzékeny/különleges adatokra vonatkozó következtetés(ek) levonásához vezethet.	3

Kockázatot növelő tényezők

A kockázatot növeli:

- az **egy érintettre vonatkozó lekért összes adat mért**éke (mennyiségi és minőségi mérték is, hiszen „megfelelő" kevés adattal is lehet nagy kárt okozni, és nagyon sok „nem releváns" adattal is lehet kisebb a kár mértéke)
- az **adatkezelő (adatfeldolgozó) vállalkozás fő profilja** (például egészségügyi vállalkozásnál nagyobb valószínűséggel van érzékeny adat, mint egy kézműves termékeket gyártó vállalatnál)
- az **érintettek érzékeny köre** (például egy rászorultaknak segítő alapítvány, vagy egy gyermektáborokat szervező cég adatai)

Kockázatot csökkentő tényezők

- **adat érvénytelensége vagy pontatlansága** (bár kockázatot csökkentő tényező, de ellentétben áll a „pontos és naprakész adatok" GDPR-ban foglalt alapelvével)
- az **adat nyilvános elérhetősége** (ha a nyilvános elérés nem az adatvédelmi incidens eredménye)
- az **adat természete** (lényeges vagy széles körű információ nem szűrhető le belőle az érintettről, ilyen például egy olyan igazolás megszerzése, mely minden további következtetés nélkül az érintett megfelelő egészségi állapotát mondja ki

Azonosíthatóság megléte (AM)

Azonosíthatóság Mértékének (AM) meghatározása: e körben azt vizsgálja, hogy az incidenssel érintett adatok segítségével mennyire könnyen azonosítható az érintett; e körben általánosan elmondható, hogy a kockázat annál kisebb, minél kevésbé és minél nehezebben azonosítható az érintett.

Név

Az országban sokan viselik ugyan azt a nevet	0,25 (Alacsony)
Az országban csak néhányan viselik azt a nevet	0,5 (Közepes)
Kisebb város, ahol kevesen/senki nem viseli ugyanazt a nevet	0,75 (Magas)
Az egész országra nézve, azonban a születési dátumot és az e-mail címet is megszerezték	1 (Nagyon magas)

SZEMÉLYAZONOSÍTÓ ÉS EGYÉB OKMÁNYOK SZÁMAI (EGY EZEK KÖZÜL)

Az érintettről semmilyen egyéb adatnem érintett az incidenssel, illetőleg további adatot nem tud beszerezni	0,25 (Alacsony)

Egy okmányszám mellett további, de nem érzékeny vagy kockázatos adat is érintett az incidenssel	0,5 (Közepes)
Egy okmányszámhoz rendelve további azonosító adat is érintett, és ez további adatok (cím, e- mail) eléréséhez vezethet	0,75 (Magas)
Amikor több további azonosításra szolgáló személyes adat is érintett (pl. személyi igazolvány másolata)	1 (Nagyon magas)

Telefonszám/lakcím közül valamelyik

Ha az országos viszonylatban– ha a név/ telefonszám nincsen benne nyilvános adatbázisban(pl. telefonkönyvben)	**0,25 (Alacsony)**
Ha helyi (kisvárosi) viszonylatban- ha a név/ telefonszám nincsen benne nyilvános adatbázisban (pl. telefonkönyvben)	0,5 (Közepes)
Egy adottlakókerületben viszonylatában, - ha a név/ telefonszám nincsen benne nyilvános adatbázisban (pl. telefonkönyvben)	0,75 (Magas)
Országos viszonylatban, és a név és a szám a címmel együtt nyilvános regiszterben is fellelhető.	1 (Nagyon magas)

Sérülés körülményei (SK)

Sérülés Körülményeinek (SK) vizsgálata: azt vizsgálja, hogy az incidens során az adatok sérülése következtében mennyire sérült az adatok biztonsága; e körben azt is vizsgálja, hogy az adatok sérülése milyen körülmények között történt (tehát például szándékolt támadás)

Adat titkosságának elvesztése

Nem biztos, hogy bárki jogosulatlanul megismeri ténylegesen az adatokat (pl. Egy zárolt és jól védett fájlokat tároló laptop, vagy irat elvesztése)	0
Meghatározható számú személy ismerheti meg jogosulatlanul az adatokat (pl. tévedésből több címzettnek megküldött, személyes adatokat tartalmazó elektronikus levél)	0,25
Meghatározhatatlan személy számára hozzáférhetővé vált személyes adat (pl. nyilvános megosztás az interneten)	0,5

Adat épségének/egységének elvesztése

Jogosulatlan, illegális behatás nélkül sérül az adat, de az helyre állítható (pl. rossz frissítés miatt elveszik, de a biztonsági mentéssel helyre állítható)	0
Helytelen vagy jogtalan kezelés során sérül az adat, de az helyreállítható	0,25
Helytelen vagy jogtalan kezelés során sérül az adat, és a helyreállítás nem lehetséges	0,5

Az adat elérhetőségének elvesztése

Az elvesztett adat minden gond nélkül helyreállítható	0
Az adat időlegesen elérhetetlen (nincsen biztonsági mentés, de az adat ismételten beszerezhető)	0,25
Teljes elérhetetlenség (az adat elveszett, biztonsági mentés nincsen, és nem szerezhető be újból)	0,5

Szándékos támadás

A mérőszám mindig 0,5.

AZ ÉRTÉKELÉS MÓDJA

Az értékelés az alábbi képlet szerint történik:

Veszély súlyossága: Adatkezelési környezet (AK) x Azonosíthatóság mértéke (AM) + Sérülés körülményei (SK)

Azaz: **VS= AK x AM + SK**

Az értékelés eredményeként megállapítható az alacsony, közepes, magas vagy nagyon magas súlyossági fok.

Súlyossági fokok (VS) értékhez rendelve

kisebb, mint 2	**Alacsony kockázatú incidens**	**Vagy nem okoz gondot az érintettnek, vagy csak nagyon kis mértékben**
2 vagy annál több, de 3- nál kevesebb	Közepes kockázatú incidens	Az érintettek némi kellemetlenséggel ugyan, de túljutnak az incidens okozta nehézségeken.
3 vagy annál több, de 4- nél kevesebb	Magas kockázatú incidens	Az érintettek komoly következményekkel számolhatnak, amit csak nagy nehézségekkel oldhatnak meg, hozzák helyre.
4 vagy annál több	Nagyon magas kockázatú incidens	Azérintettek hatalmas, beláthatatlankövetkezményekkel számolhatnak, amiket lehet, hogy nem tudnak megoldani, helyrehozni.

2. SZÁMÚ MELLÉKLET

Adatvédelmi hatásvizsgálat

Az Önkormányzat, valamint a Hivatal az adatvédelmi hatásvizsgálat lefolytatásához alapvetően a francia adatvédelmi hatóság (CNIL) erre a célra kibocsátott ingyenes szoftvert használja. Amennyiben a szoftver használata akadályokba ütközne, úgy az alábbi folyamatok és minták szerint jár el:

Folyamata

1. a tervezett adatkezelési műveletek leírása és az adatkezelés céljainak ismertetése
2. az adatkezelés szükségességi és arányossági vizsgálata
3. az érintett jogait és szabadságait érintő kockázatok vizsgálata
4. intézkedések a kockázatok kezelésére
5. nyomon követés, felülvizsgálat

Tematikája:

- módszeres leírás készül az adatfeldolgozásról
- figyelembe veszik az adatkezelés jellegét, hatókörét, körülményeit és céljait
- a személyes adatokat, a címzetteket, valamint a személyes adatok tárolásának időtartamát rögzítik;
- funkcionális leírás készül az adatkezelési műveletről;
- a személyes adatokhoz használt eszközöket (hardverek, szoftverek, hálózatok, személyek, papírok vagy papíralapú továbbítási csatornák) azonosították;
- figyelembe veszik a jóváhagyott magatartási kódexek előírásainak teljesítését
- értékelik a szükségességet és az arányosságot
- a jogi szabályozók betartására irányuló intézkedéseket meghatározták figyelembe véve az alábbiakat:

  Az adatkezelés arányosságát és szükségességét előmozdító intézkedések a következők alapján:

  - meghatározott, kifejezett és jogos cél(ok)
  - az adatkezelés jogszerűsége
  - megfelelőek, relevánsak, és a szükséges adatokra korlátozódnak
  - korlátozott tárolási időtartam
  - az érintettek jogait támogató intézkedések:
  - az érintetteknek nyújtott tájékoztatás
  - betekintési jog és az adathordozhatósághoz való jog
  - a helyesbítéshez és a törléshez való jog
  - kifogásolási jog és az adatkezelés korlátozásához való jog

- az feldolgozókkal fennálló kapcsolatok
- a nemzetközi adattovábbításhoz kapcsolódó garanciák
- előzetes konzultáció
- az érintett jogait és szabadságait érintő kockázatokat kezelik
- a kockázatok forrását, jellegét, egyediségét és súlyosságát felmérték vagy konkrétabban mindegyik kockázat (jogosulatlan hozzáférés, nemkívánatos módosítás és az adatok eltűnése) esetében az érintettek szemszögéből:

1. figyelembe vették a kockázatforrásokat;
2. az érintettek jogaira és szabadságaira esetlegesen gyakorolt hatásokat
3. beazonosították olyan eseményekre vonatkozóan, mint a jogosulatlan hozzáférés, a nemkívánatos módosítás és az adatok eltűnése;
4. az esetleg jogosulatlan hozzáféréshez, nemkívánatos módosításhoz vagy adatok eltűnéséhez vezető veszélyeket beazonosították;
5. felmérték a valószínűséget és a súlyosságot
6. az említett kockázatok orvoslására irányuló intézkedéseket meghatározták, az érdekelteket bevonták:
7. kikérték az adatvédelmi tisztviselő tanácsát, adott esetben kikérték az érintettek véleményét

Amennyiben az adatkezelő valamely okból (személyes okok, vagy a technika jelenlegi állása) **nem tudja a kockázatokat csökkenteni, mindenképpen szükséges konzultációt kezdeni a felügyeleti hatósággal.**

ALAPADATOK

Projekt elnevezése	**Közfeladatot ellátó szerv neve**	**Felelős neve és elérhetősége**	**Projekt kezdete**	**Befejezés tervezett ideje**
A projekt rövid leírása				
A projekt alapvető célja				

Az adatgyűjtés célja **(nem azonos a projektcéllal, itt azt kell meghatározni, hogy az adat a projekten belül hogyan és milyen céllal kerül felhasználásra)**
Mik a kockázatos pontjai a személyes adatok gyűjtésének? **(Pl. hálózat informatikai védelme stb.)**
Van-e erre az adatgyűjtési tevékenységre korábbi szabályzat vagy minta? **(Pl. az Önkormányzat korábban már üzemeltetett hasonló rendszert)**
Kik azok a munkavállalók/ vezetők, akik a projekt végrehajtásába be lettek vonva?
Kik azok a szolgáltatók, akikkel a projekt során együttműködik a Közfeladatot ellátó szerv?
Be vannak vonva a szolgáltatókon túl egyéb, a Közfeladatot ellátó szerven kívüli harmadik személyek? Kik?
Milyen (adatvédelmen túli) speciális jogszabályok vagy kamarai és egyéb szabályozók vonatkoznak a projekttel érintett adatkezelésre?

ADATOK AZONOSÍTÁSA

Milyen személyes adatokat gyűjt?

- **név**
- **cím**
- **e- mail**
- **telefonszám**
- **személyi igazolvány szám**
- **adóazonosító jel stb.**

Milyen különleges adatokat gyűjt a projekt/tevékenység során?

- **faji vagy etnikai származásra,**
- **politikai véleményre,**
- **vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok,**
- **a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok,**
- **az egészségügyi adatok (fizikai és pszichikai)**
- **természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok**
- **bűnügyi személyes adatok**

Adatok részletezése:

Milyen egyéb tematizált adatokat gyűjt a projekt/tevékenység során:

- **korábbi munkaviszonyra, munkavállalói profilra vonatkozó adatok**
- **párkapcsolatra vonatkozó adatok**
- **külső megjelenésre vonatkozó adatok**
- **életkor**
- **szociális körülményekre vonatkozó adatok**
- **családi életre vonatkozó adatok**
- **életstílusra vonatkozó adatok**
- **személyes pénzügyekre vonatkozó adatok**
- **kamarai tagsággal összefüggő adatok**

A lista alapján vizsgálja felül, hogy valamennyi adat feltétlenül szükséges és indokolt-e a projektfeladatok végrehajtásához!

JOGI MEGFELELÉS

Mi a jogalapja az adatkezelésnek?

- **hozzájárulás**
- **szerződés teljesítése**
- **jogos érdek**
- **jogi kötelezettség teljesítése**
- **létfontosságú érdek**
- **közhatalmi jogosítványok**

Érint-e valamilyen emberi jogot (akár pozitívan, akár negatívan) az adatkezelés?

- ***diszkrimináció, hátrányos megkülönböztetés tilalma***
- ***egyenjogúság, törvény előtti egyenlőség***
- ***hátrányos helyzetű csoportok pozitív megkülönböztetése***
- ***élethez és emberi méltósághoz való jog***
- ***szabadság, személyi biztonság***
- ***magán- és családi életét, otthon, kapcsolattartás és jó hírnév tiszteletben tartása***
- ***személyes adatok védelme***
- ***közérdekű adatok megismerése***
- ***jogtalan támadás elháritásának joga***
- ***gondolat, lelkiismeret, vallás szabadsága***
- ***(békés) gyülekezés joga (párt, szakszervezet, gyűlések, kamarák, legális tüntetések, stb.)***
- ***véleménynyilvánítás szabadsága***
- ***tudományos kutatás, művészeti alkotás szabadsága***
- ***művelődés joga (oktatások, képzések, egyéb...)***
- ***munka és foglalkozás szabad megválasztása***
- ***tulajdon és öröklés***

- gyermekek jogai a megfelelő testi, szellemi és erkölcsi fejlődéséhez szükséges védelemhez és gondoskodáshoz ***- szociális biztonság*** ***- testi és lelki egészség*** ***- egészséges környezet*** ***- emberhez méltó lakhatás*** ***- választás és választhatóság (országgyűlés, önkormányzat)*** ***- panasztétel joga (közhatalmi szervhez bejelentés)*** ***- szabad mozgás és tartózkodás*** ***- nemzetiségi jogok*** ***- család, otthon, magánélet védelme***
Milyen társadalmi szükségletet elégít ki a projekt? Alkalmas a szükséglet kielégítésére?
Hogyan/ milyen módon (forrás) gyűjti/szerzi be a projekthez szükséges személyes adatokat?
Szükséges-e az érintettektől az újfajta adatkezeléshez hozzájárulást beszerezni, vagy a meglévő hozzájárulások megfelelőek?

Az Adatvédelmi Szabályzat lefedi ezt a tevékenységet is?
Használ a projekt során olyan adatot, amit korábban más céllal gyűjtött?
Valamennyi korábbi adatra szükség van a projekt során?
A már rendelkezésre álló adatok alkalmasak (minőség, tárolás ideje, pontosság) a cél elérésére?
Megfelelően tájékoztatta az érintettet az adatai más célú felhasználásáról?

Szükség esetén tudja pontosítani, módosítani, törölni, zárolni, anonimizálni az adatokat minden adatbázisból?

Szükség esetén a Közfeladatot ellátó szerv közvetlenül hozzáférhetővé tudja tenni az adatokat az érintett kérésére?

Ha a vállalkozáson kívüli harmadik személytől szerzi be az adatokat, hogyan biztosítja azok pontosságát és megfelelőségét?

Az adatkezelés teljes ciklusát (kezdete, és pontos vége) meg tudja határozni?

Tudja biztosítani az érintettek számára, hogy az adataihoz hozzá férhessen, illetőleg az adatkezelésről tájékoztatást kapjon?

A Közfeladatot ellátó szerv a projekt során biztosítani tudja, hogy az érintett éljen a tiltakozási jogával?

Pontosan a Közfeladatot ellátó szerv melyik munkavállalója/vezetője van kijelölve arra, hogy az ügyfélmegkereséseket megválaszolja és intézze?

Meg van pontosan határozva az, hogy mely vezető/munkavállaló/partner milyen céllal és milyen terjedelemben férhet hozzá az adatokhoz?

Valamennyi, az adatokhoz hozzáférő személy és munkavállaló tudja az adatkezelésre és adatfeldolgozásra vonatkozó szabályokat?

Az informatikai biztonság megfelelő szintű és színvonalú?

Az adattovábbítás biztonsága megfelelő?

Továbbítja az adatokat harmadik országba?
Hogyan továbbítja az adatokat harmadik országba?
Mi garantálja az adatok biztonságát a harmadik országba való továbbítás során?
Megvizsgálta az adatvédelmi kockázatokat az adatgyűjtés megkezdése előtt?
Kikkel konzultált/egyeztetett az adatkezelés jogszerűsége és biztonsága érdekében?

Milyen adatvédelmi kockázatokat tárt fel?
Milyen konkrét intézkedéseket tett az adatkezelés jogszerűsége és biztonsága érdekében?

1. számú melléklet	
A ..... napján ..... helyszínen tartott személyes egyeztetés/ megbeszélés jegyzőkönyve	
Megbeszélés vezetője:	Megjelentek neve:
Megbeszélés vezetőjének beosztása:	Megjelentek beosztása:
JEGYZŐKÖNYV	

KOCKÁZATOK ELEMZÉSE

Analitikai módszertanok

RAG MÁTRIX

KOCKÁZAT BEKÖVETKEZÉS VALÓSZÍNŰSÉGE

Valószínűségi pontszám	***Nem valószínű*** *(1)*	**Előfordulhat** (2)	**Valószínűleg elő fog fordulni** (3)	***Nagy valószínűséggel előfordul*** *(4)*	***Szinte teljesen biztos, hogy előfordul*** *(5)*
A kockázathoz rendelt valószínűségi érték, azaz annak az esélye, hogy a kockázat problémát okoz az adatvédelemben	Nagyon nem valószínű, hogy bármi probléma felmerülne	Nem várható/várjuk, hogy előfordul, de teljesen nem zárható ki	Esetenként előfordulhat	Előre ugyan nem várható, de valószínűleg elő fog fordulni	Szinte biztosan előfordul, az sem kizárt, hogy többször

KOCKÁZAT HATÁSA

Kockázat hatása	***Nagyon kicsi hatás*** *(1)*	***Kicsi hatás*** *(2)*	***Közepes hatás*** *(3)*	***Nagy hatás*** *(4)*	***Nagyon nagy hatás*** *(5)*
A kockázat bekövetkezésének van-e negatív hatása?	Nem valószínű, hogy negatív hatása lenne	Csak kevés negatív hatása lenne	Lenne hatása	Nagy valószínűséggel jelentős hatása lenne	Igen nagy hatása lenne

ÉRTÉKELÉS

A két táblázatban adott értékek összege	***Kockázat mértéke***
1-2	*Nagyon kicsi kockázat*

3-4	*Kicsi kockázat*
5-6	*Közepes kockázat*
7-8	*Nagy kockázat*
9-10	*Nagyon magas kockázat*

ALKALMAZOTT MÓDSZERTAN- HÁROM TÉNYEZŐS ÉRTÉKELÉS

A vegyes értékelésnél a valószínűségi (RAG) mátrix elemeit keverjük a tényadatok értékeléséhez, mint például a biztonsági szint. A mátrixhoz hasonló ábra itt is felvázolható, ez esetben három tényezőt vizsgálunk alaposabban, a kockázati lehetőséget (adatvédelmi rendszer megsértése), a kockázat hatása, és a védelmi szint.

KOCKÁZAT BEKÖVETKEZÉSI VALÓSZÍNŰSÉGE

Kockázat valószínűsége	***Súlyos*** *(4)*	***Közepes*** *(2)*	***Csekély*** *(1)*
Esélyek	Nagyon valószínű, hogy a kockázat bekövetkezik	Bekövetkezhet a kockázat	Nem valószínű, hogy a kockázat bekövetkezik

A KOCKÁZAT HATÁSA

A kockázat bekövetkezésének hatása	***Súlyos*** *(4)*	***Közepes*** *(2)*	***Csekély*** *(1)*
Adatvédelmi rendszer megsértésének valószínűsége			
Adatvédelmi rendszermegsértésének következménye			
Adatkezelőre (beleértve a vezetést és a munkavállalókat			
Érintettre			
Együttműködő partnerekre			

ADATVÉDELMI KÉSZÜLTSÉG SZINTJE

	Gyenge ***(4)***	***Átlagos*** ***(2)***	***Nagyon jó*** ***(1)***
Adatvédelmi rendszer felkészültsége (előzetes intézkedések védelmiszintje)			

A készültség szintjénél a pontszámozás fordított, hiszen a gyenge készültségi szint magasabb szorzóértéket (kockázatot) jelent.

ÉRTÉKELÉS

Ebben az esetben a három kapott pontszámot szorozzuk össze. A legmagasabb (és legrosszabb) érték a 4x4x4, azaz a 64. Mivel 3 mérési számunk van, a besorolási értékeket (azaz a tényleges kockázati szintet) a 64-es szám hárommal való elosztásával kaphatjuk meg.

A három táblázatban adott értékek szorzata	**Kockázat mértéke**
1-20	*Kicsi kockázat*
21-41	*Közepes kockázat*
42-64	*Magas kockázat*

VEGYES RENDSZER- ALAP RAG HÁROM TÉNYEZŐVEL

A RAG szerinti 1,2,3,4,5 cizellált számokkal pontosított kockázati besorolás alkalmazását olyan technikával, mely a kockázatok mindhárom adatvédelmi aspektusát (azaz a kockázat bekövetkezésének valószínűsége, a kockázat hatása és a rendszer felkészültségi szintje) figyelembe veszi.

A vegyes rendszer szerinti táblázatok az alábbiak szerint néz ki:

KOCKÁZAT BEKÖVETKEZÉS VALÓSZÍNŰSÉGE

Valószínűségi pontszám	***Nem valószínű*** ***(1)***	**Előfordulhat** **(2)**	**Valószínűleg elő fog fordulni** **(3)**	***Nagy valószínűséggel előfordul*** ***(4)***	***Szinte teljesen biztos, hogy előfordul*** ***(5)***

A kockázathoz rendelt valószínűségi érték, azaz annak az esélye, hogy a kockázat problémát okoz az adatvédelemben	Nagyon nem valószínű, hogy bármi probléma felmerülne	Nem várható/várjuk, hogy előfordul, de teljesen nem zárható ki	Esetenként előfordulhat	Előre ugyan nem várható, de valószínűleg elő fog fordulni	Szinte biztosan előfordul, az sem kizárt, hogy többször

KOCKÁZAT HATÁSA

Kockázat hatása	***Nagyon kicsi hatás (1)***	***Kicsi hatás (2)***	***Közepes hatás (3)***	***Nagy hatás (4)***	***Nagyon nagy hatás (5)***
A kockázat bekövetkezésének van-e negatív hatása?	Nem valószínű, hogy negatív hatása lenne	Csak kevés negatív hatása lenne	Lenne hatása	Nagy valószínűséggel jelentős hatása lenne	Igen nagy hatása lenne
Adatkezelőre (beleértve a vezetést és a munkavállalókat)					
Érintettre					
Együttműködő partnerekre					

ADATVÉDELMI RENDSZER SZINTJE

Adatvédelmi rendszer szintje	***Gyenge (5)***	***Alacsony szintű (4)***	***Átlagos (3)***	***Jó (2)***	***Nagyon jó (1)***
Adatvédelmi rendszer felkészültsége (előzetes intézkedések védelmi szintje)	Nem valószínű, hogy negatív hatása lenne	Csak kevés negatív hatása lenne	Lenne hatása	Nagy valószínűséggel jelentős hatása lenne	Igen nagy hatása lenne

ÉRTÉKELÉS

Ebben az esetben is a három kapott pontszámot szorozzuk össze. A legmagasabb (és legrosszabb) érték a 5x5x5, azaz a 125. Mivel 5 mérési számunk van, a besorolási értékeket (azaz a tényleges kockázati szintet) a 125-ös szám öttel való elosztásával kaphatjuk meg, azaz 25 pontértékenként változik a besorolás.

A három táblázatban adott értékek szorzata	Kockázat mértéke
1-25	*Nagyon kicsi kockázat*
26-51	*Kicsi kockázat*
52-76	*Közepes kockázat*
76-101	*Nagy kockázat*
102-125	*Nagyon magas kockázat*

A VEGYES RENDSZER SZERINTI ÖSSZKOCKÁZATI ÉRTÉK

Az öt fajta kockázatértékelés (**Informatikai kockázatértékelés**, **Adatkezelési kockázatértékelés**, **Munkavállalókkal kapcsolatos kockázatértékelés**, **Papír alapú iratokra vonatkozó kockázatértékelés**, **Jogi megfelelési kockázatértékelés** mindegyikéhez hozzárendelve az 1-5 skála szerinti értékeket megkaphatjuk a Teljes kockázatértékelést, azaz azt, hogy a **Közfeladatot ellátó szerv** jelenleg mennyire kezeli megfelelően az adatkezelési műveleteket:

KOCKÁZAT BEKÖVETKEZÉSÉNEK VALÓSZÍNŰSÉGE

Valószínűségi pontszám	**Nem valószínű** (1)	**Előfordulhat** (2)	**Valószínűleg elő fog fordulni** (3)	**Nagy valószínűséggel előfordul** (4)	***Szinte teljesen biztos, hogy előfordul*** (5)
A kockázathoz rendelt valószínűségi érték, azaz annak az esélye, hogy a kockázat problémát okoz az adatvédelemben	Nagyon nem valószínű, hogy bármi probléma felmerülne	Nem várható/várjuk, hogy előfordul, de teljesen nem zárható ki	Esetenként előfordulhat	Előre ugyan nem várható, de valószínűleg elő fog fordulni	Szinte biztosan előfordul, az sem kizárt, hogy többször
Informatikai kockázatkértékelés					
Adatkezelési kockázatkezelés					
Munkavállalókkal kapcsolatos kockázatértékelés					
Papír alapú iratok					

kockázatértékel és					
Jogi megfelelés kockázatértékel és					
Teljes átlag (azaz a teljes hatás szintje). *<u>Számítás:</u> átlagolni az 5 kapott összpontszámot, azazaz öt értéket összeadjuk, majd elosztjuk öttel, végül kerekítjük.*					

KOCKÁZAT BEKÖVETKEZÉSÉNEK HATÁSA

Tekintettel arra, hogy az összpontszámot kihozásánál három hatást is vizsgálunk (munkavállaló, érintett, partner), szükséges egy átlagértéket produkálnunk. Ezt a fenti módszertan alkalmazásával tudjuk megoldani, azaz például az Informatikai kockázatértékelés esetén: munkavállaló kockázata kap pontot 1-5-ig, az érintett kap pontot 1-5-ig, a partner kap pontot 1-5-ig, összeadjuk a kapott pontszámokat, és mivel 3 tényezőt vizsgálunk, 3-mal elosztjuk.

Kockázat hatása	***Nagyon kicsi hatás*** *(1)*	***Kicsi hatás*** *(2)*	***Közepes hatás*** *(3)*	**Nagy hatás** *(4)*	**Nagyon nagy hatás** **(5)**	**Átlagolt kockázat**
A kockázat bekövetkezésének van-e negatív hatása?	Nem valószínű, hogy negatív hatása lenne	Csak kevés negatív hatása lenne	Lenne hatása	Nagy valószínűséggel jelentős hatása lenne	Igen nagy hatása lenne	Átlag

Informatikai kockázatkértékelés		Adatkezelőre (beleértve a vezetést és a munkavállalókat)		
		Érintettre		
		Együttműködő partnerre		
Adatkezelési kockázatértékelés		Adatkezelőre (beleértve a vezetést és a munkavállalókat)		
		Érintettre		
		Együttműködő partnerre		
Munkavállalókkal kapcsolatos kockázatértékelés		Adatkezelőre (beleértve a vezetést és a munkavállalókat)		
		Érintettre		
		Együttműködő partnerre		
Papír alapú iratokra vonatkozó kockázatértékelés		Adatkezelőre (beleértve a vezetést és a munkavállalókat)		
		Érintettre		
		Együttműködő partnerre		
Jogi megfelelési kockázatértékelés		Adatkezelőre (beleértve a vezetést és a munkavállalókat)		
		Érintettre		
		Együttműködő partnerre		
Teljes átlag (azaz a teljes hatás szintje). ***Számítás: átlagolni az 5 kapott összpontszámot, azazaz öt értéket összeadjuk, majd elosztjuk öttel, végül kerekítjük.***				

Az adatvédelmi rendszer szintje

***Adatvédelmi rendszer szintje* (felkészültsége)**	***Gyenge*** *(5)*	***Alacsony*** *(4)*	***Közepes*** *(3)*	***Jó*** *(2)*	***Nagyon jó*** *(1)*	***Alacsony***
Informatikai kockázatkértékelés			Adatkezelőre (beleértve a vezetést és a munkavállalókat)			
			Érintettre			
			Együttműködő partnerre			
Adatkezelési kockázatértékelés			Adatkezelőre (beleértve a vezetést és a munkavállalókat)			
			Érintettre			
			Együttműködő partnerre			
Munkavállalókkal kapcsolatos kockázatértékelés			Adatkezelőre (beleértve a vezetést és a munkavállalókat)			
			Érintettre			
			Együttműködő partnerre			
Papír alapú iratokra vonatkozó kockázatértékelés			Adatkezelőre (beleértve a vezetést és a munkavállalókat)			
			Érintettre			
			Együttműködő partnerre			
Jogi megfelelési kockázatértékelés			Adatkezelőre (beleértve a vezetést és a munkavállalókat)			
			Érintettre			
			Együttműködő partnerre			

ÉRTÉKELÉS (ÖSSZVÁLLALATI MUTATÓÉRTÉK)

Ebben az esetben is a három véglegesített és teljes, a táblázatok végén kapott három összpontszámot szorozzuk össze. A legmagasabb (és legrosszabb) érték a 5x5x5, azaz a 125. Mivel 5 mérési számunk van, a besorolási értékeket (azaz a tényleges kockázati szintet) a 125-ös szám öttel való elosztásával kaphatjuk meg, azaz 25 pontértékenként változik a besorolás.

A három táblázatban adott értékek szorzata	**Kockázat mértéke**
1-25	*Nagyon kicsi kockázat*
26-51	*Kicsi kockázat*
52-76	*Közepes kockázat*

76-101	*Nagy kockázat*
102-125	*Nagyon magas kockázat*

Kockázatelemzés mintái

ÁLTALÁNOS ADATOK

Közfeladatot ellátó szerv neve	Közfeladatot ellátó szerv vezetőjének neve	Felelős neve és elérhetősége	Kockázatértékelés ideje	Felülvizsgálat tervezett ideje

(HA VOLT) A KORÁBBI KOCKÁZATÉRTÉKELÉS EREDMÉNYEI ÉS A MEGTETT INTÉZKEDÉSEK

Korábbi kockázatértékelés eredményei és fő megállapításai:
Korábbi kockázatértékelés alapján megtett intézkedések:

KOCKÁZATÉRTÉKELÉSEK

Közfeladatot ellátó szerv tevékenységeinek rövid leírása
A munkavállalók száma (a vezetést is beleértve)
Kockázatértékelésért felelős munkavállalók és vezetők
A kezelt adatok típusa: *a) <u>Általános</u>* **Munkavállalói** **Partner** **Ügyfél** **Közfeladatot ellátó szervi saját** **Hatósági**

b) Adatminőség

Személyes adat

Különleges adat

Egyéb okból különleges figyelmet igénylő adat

Mik a kockázatos pontjai a személyes adatok gyűjtésének?

1. ***eszköz szintű (hardware)***

Kockázatok: Az eszközök használata nem szabályos, a munkavállalók nem lettek tájékoztatva megfelelően, a biztonsági mentések nincsenek vagy hiányosak, az eszközök könnyen hozzáférhetők stb.

2. ***program szintű (software)***

Kockázatok: A programok nincsenek egyedi jelszóval vagy kóddal védve, többen ugyan azt a jelszót használják, a program forrása nem megbízható, nincsen vírusírtó, nincsen weblap védelem stb.

Informatikai kockázatelemzés:

*3. **adatátvitellel összefüggő***

Kockázatok: az adatátvitel menete nem biztonságos, a partnerek nem lettek megfelelően ellenőrizve adatmegküldése előtt, nem tudjuk, pontosan ki is látja meg és hogyan használja fel az adatot, a hozzájáruló nyilatkozatok nem lettek megszerezve, az érintettek nincsenek megfelelően tájékoztatva, az adatvédelmi incidensekre vagy a megkeresések teljesítésére nincsen intézkedési terv stb.

Adatkezelési kockázatelemzés:

*4. **emberi tényező (felhasználó, munkavállaló)***

Kockázatok: a munkavállaló túl sok adathoz fér hozzá, a munkavállaló megosztja a megszerzett adatokat, a munkavállaló kiviszi a Közfeladatot ellátó szervtől az adatokat, a munkavállaló nem tudja az adatkezelés menetét és szabályozását, a munkavállaló munkaszerződése vagy tájékoztatása nem megfelelő stb.

Munkavállalókkal kapcsolatos kockázatértékelés:

*5. **papír alapú iratok***

Kockázatok: nincsen szabály az adatkezelésre, sok a felesleges nyomtatás, az iratok nincsenek biztonságos helyen kezelve, az iratok nincsenek rendszerezve stb.

*6. **papír alapú iratok továbbítása (pl. posta, futárszolgálat)***

Kockázatok: a beérkező papír alapú iratok megismerése nincsen rendesen szabályozva, illetőleg a szabályok betartva, a papaír alapú iratokat ki lehet vinni a cégtől, a továbbítás menete nincsen leszabályozva, a partner, akinek továbbítjuk nincsen rendben adatvédelmileg stb.
Papír alapú iratokra vonatkozó kockázatértékelés:

Jogi megfelelésre vonatkozó kockázatértékelés
Kik azok a szolgáltatók, akikkel együttműködik a Közfeladatot ellátó szervvel?
(Opcionális lehetőség- A partnerekkel kapcsolatos kockázatértékelés)
Be vannak vonva a Közfeladatot ellátó szerv tevékenységébe a szolgáltatókon túl egyéb, a Közfeladatot ellátó szerven kívüli harmadik személyek? Pontosan kik?
Milyen (adatvédelmen túli) speciális jogszabályok vagy kamarai és egyéb szabályozók vonatkoznak a Közfeladatot ellátó szerv adatkezelésére?

CSELEKVÉSI TERVEK

Intézkedések és tervezett intézkedések:
1. ***A kockázat csökkentése*** **Probléma:** **Ok:** **Módszer:** **Felelős:** **Határidő:** 2. ***A kockázat szabályozása, katasztrófatervek*** **Probléma:** **Ok:** **Módszer:** **Felelős:** **Határidő:**
3. ***A kockázat elkerülése*** **Probléma:** **Ok:**

Módszer:

Felelős:

Határidő:

4. A kockázat átruházása

Probléma:

Ok:

Módszer:

Felelős:

Határidő:

5. A kockázat tudomásul vétele

Probléma:

Ok:

Módszer:

Felelős:

Határidő:

PONTOS FELADATOK ÉS JÖVŐBELI INTÉZKEDÉSEK

Feladatok és célkitűzések:

Fejlesztési terv leírása:

Határidő:

Felelős:

ÖSSZEFOGLALÓ

Korábbi kockázati szint:

Jelenlegi kockázati szintek:

Cselekvési tervek:

A Közfeladatot ellátó szerv általános adatvédelmi kockázatai:
(Behivatkozható itt a kockázatelemzés)

A projekt/működés során azonosítható kockázatok:
(projektre/működési területre elkészített egyedi kockázatértékelés)

Tervezett intézkedések a kockázatérékelés alapján:

Tervek (konkrét):

Felelős:

Közreműködők:

Határidő:

Utóellenőrzés időpontja:

Utóellenőrzés felelőse:

Utóellenőrzés menete:

Résztvevők az utóellenőrzésben:

Az utóellenőrzés megbeszéléseinek jegyzőkönyvei:

A hatásvizsgálatot az alapelvek figyelembe vételével, azok tükrében és szellemiségében szükséges elvégezni.

Alapelvek:

1) Elszámoltathatóság
2) Célhoz kötöttség/jogalap
3) Adatgazdaságosság
4) Érintetti jogok
5) Adathordozhatóság
6) Átláthatóság
7) Adatbiztonság
8) Időtartam
9) Adattovábbítás 3. országba

1) ÁLTALÁNOS BEMUTATÁS

A hatásvizsgálat szükségessége és alapja
A hatásvizsgálat elvégzésének oka:
A projekt rövid ismertetése:
A projekt célja, az érintettek, a vállalkozások és harmadik személyek projekt által biztosított előnye és haszna:

Projekthez kapcsolódó egyéb dokumentációk listája és tárolási helye:

2) ADATTÉRKÉP

Mutassa be, hogy a projekt során milyen adatok, milyen módon, és milyen személyekhez/szervekhez jutnak el (adattérkép és adatfolyam):

3) CSELEKVÉSEK ADATVÉDELMI KOCKÁZATOK FELMÉRÉSE ÉRDEKÉBEN

A projekt kapcsán a megfelelő előkészítés érdekében az alábbi külső és belső előkészítő konzultációk zajlottak:

A projekt kapcsán az alábbi külső és belső adatvédelmi tájékoztató és feladatismertető tevékenységek zajlottak:

4) KOCKÁZATOK AZONOSÍTÁSA ÉS KEZELÉSE

A jogi megfelelőség kockázatai az alábbiak:

A kockázatok enyhítésére/elhárítására az alábbi lépéseket tettük:

A kockázatok enyhítésére/elhárítására az alábbi lépéseket tervezzük (időpont, határidő megjelölésével):

Intézkedésekért felelős személy:

Az informatikai kockázatok az alábbiak:

A kockázatok enyhítésére/elhárítására az alábbi lépéseket tettük:

A kockázatok enyhítésére/elhárítására az alábbi lépéseket tervezzük (időpont, határidő megjelölésével):

Intézkedésekért felelős személy:

A személyügyi kockázatok az alábbiak:

A kockázatok enyhítésére/elhárítására az alábbi lépéseket tettük:

A kockázatok enyhítésére/elhárítására az alábbi lépéseket tervezzük (időpont, határidő megjelölésével):

Intézkedésekért felelős személy:

Az együttműködő partnerekkel kapcsolatos kockázatok az alábbiak:

A kockázatok enyhítésére/elhárítására az alábbi lépéseket tettük:

A kockázatok enyhítésére/elhárítására az alábbi lépéseket tervezzük (időpont, határidő megjelölésével):

Intézkedésekért felelős személy:

A HATÁSVIZSGÁLAT EREDMÉNYEINEK ALKALMAZÁSA

A projekt hatásvizsgálatnak megfelelő utóellenőrzéséért felelős személy:

Az utóellenőrzés ideje és menete:

Konkrét intézkedések a hatásvizsgálat alapján:

3. SZÁMÚ MELLÉKLET

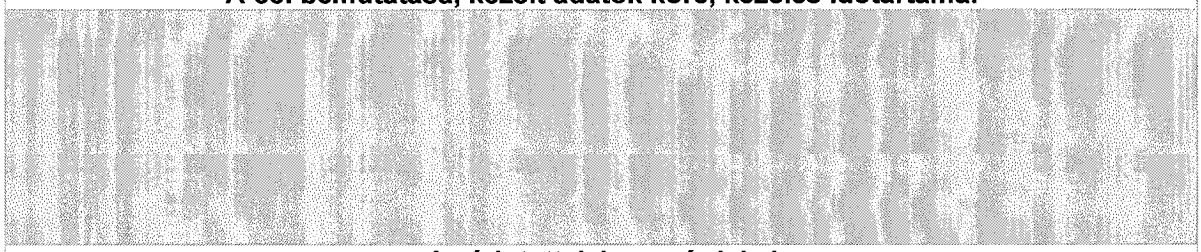
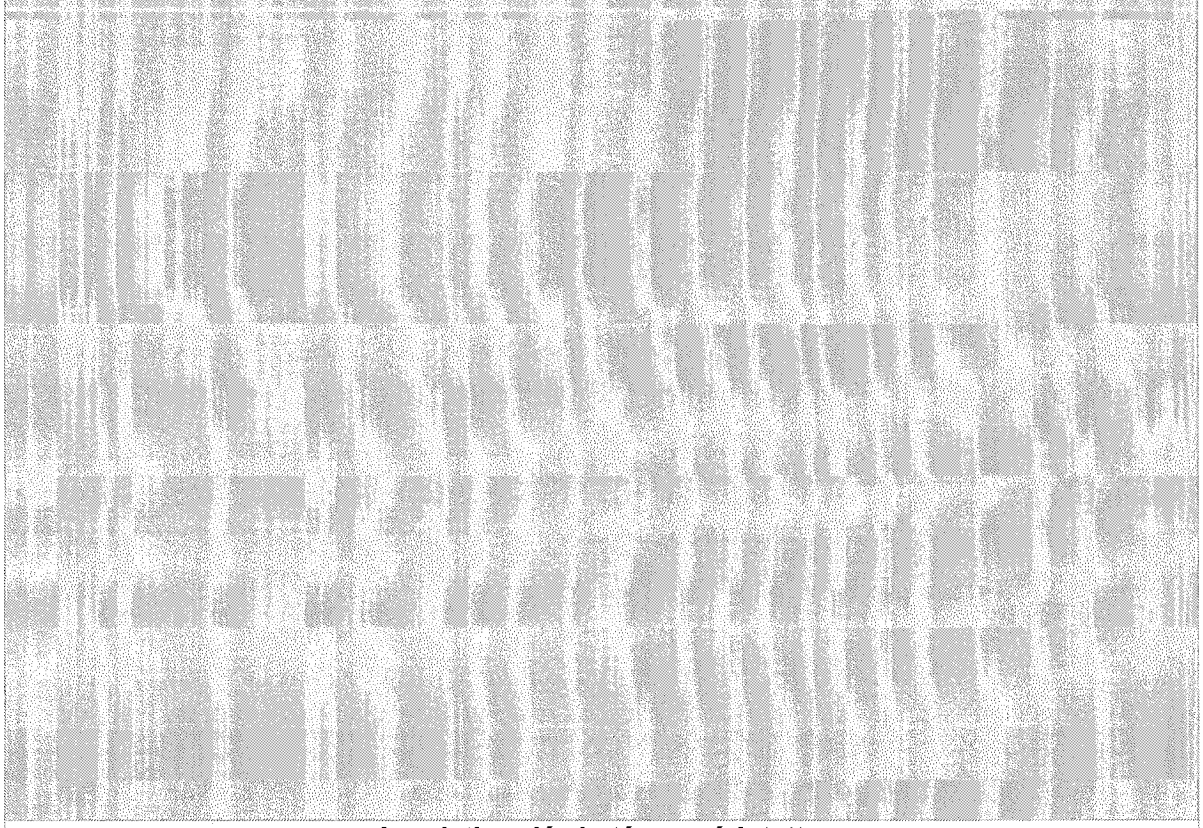
Érdekmérlegelési teszt
(minta)

Érdekmérlegelési teszt

A ..... céljából

Az érdekmérlegelési teszt elvégzésére okot adó körülmények leírása[1]
Kinek a jogos érdeke (a Közfeladatot ellátó szerv vagy harmadik személy?)
Feltétlenül szükséges-e az adat kezelése, vagy az adatkezelési cél más módon/módokon is biztosítható?
A jogos érdek meghatározása
Alkalmazandó jogalap:

[1] Lehetséges: Alapvető jogok, szélesebb közérdek, méltányolható és jogszerű egyéni érdek vagy kulturális, társadalmi elismertség

A cél bemutatása, kezelt adatok köre, kezelés időtartama.

Az érintettek jogos érdekei
Az adatkezelés az alábbi érintetti jogokat érinti: **Információs önrendelkezési jog:**

Az adatkezelés hatása az érintettre

A kezelt adatok jellege (típusa) és terjedelme:

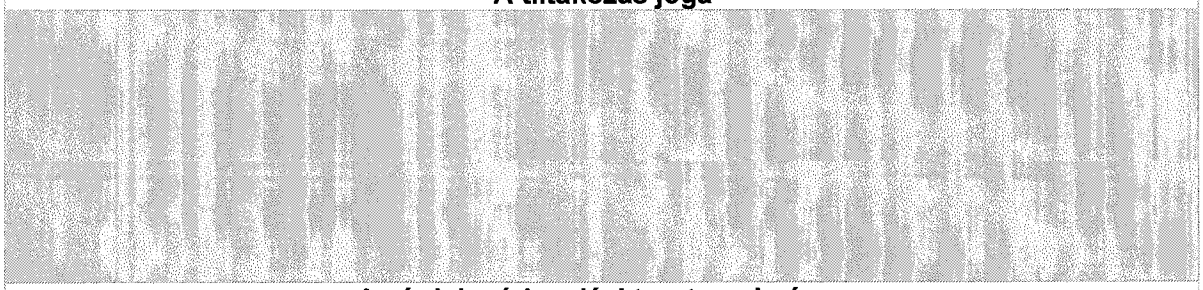
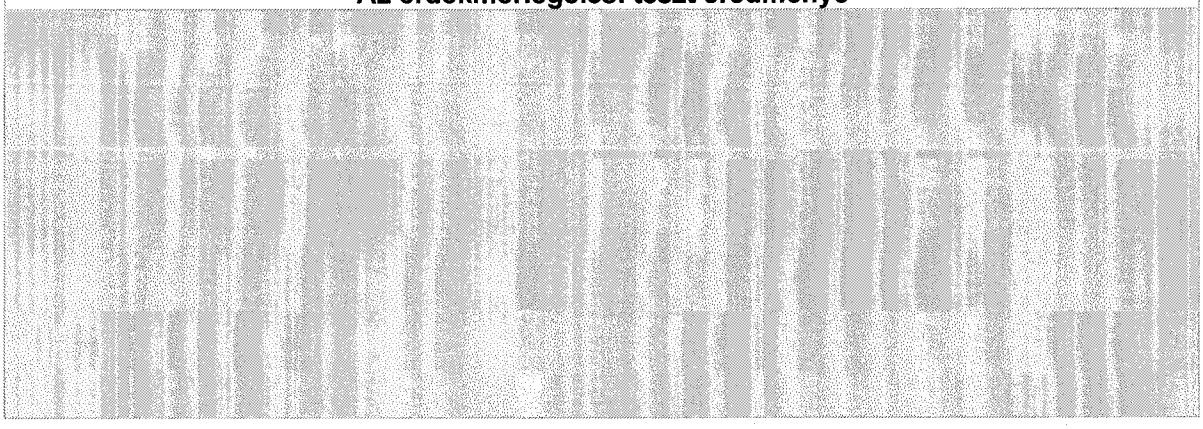
Az adatkezelés hatása:

Adatkezelés módjai:

Az érintett ésszerű elvárásai:

Érdekek összevetése (szükségesség- arányosság)

Garanciák

A tiltakozás joga

Az érdekmérlegelési teszt eredménye


Segédlet az érdekmérlegelési teszt elvégzéséhez

Alapjogok

1. Élethez való jog és emberi méltóság
2. Önazonosság, önrendelkezés, magánszféra
3. Egyenlőség
4. Jogképesség
5. Diszkrimináció tilalma
6. Alapvető szabadságjogok

   I. Szólás- és sajtószabadság

   II. Vallás- és lelkiismereti szabadság

   III. A gyülekezési és egyesülési jog (egyesülési és szervezkedési szabadság)

7. Eljárási alapjogok

   I. A tisztességes eljáráshoz való jog („fair trial")

   II. A jogorvoslathoz való jog, és a bírósághoz fordulás joga

   III. A jogviták ésszerű határidőn belül való elbírálása („reasonable time")

   IV. Védelemhez való jog és a fegyverek egyenlőségének elve

8. Szabadsághoz és személyi biztonsághoz való jog
9. Tulajdonhoz való jog
10. Személyes adatok védelme és információszabadság
11. Az egészséghez és az egészséges környezethez való jog
12. Szociális jogok

    I. A munka és a foglalkozás szabad megválasztása

    II. Szociális biztonság

III. Művelődéshez való jog

13. Gyermekvédelem

Adatkezelések hivatkozási alapja és lehetséges garanciái

Garanciák és csoportosításuk

Általános biztosítékok:

1. *Adatkezelés végrehajtásához kapcsolódó biztosítékok*
   - Adatkezelés terjedelme (adatkör korlátozott és szűk)
   - Adatkezelés időtartama (lehető legrövidebb)
   - Álnevesítés (amennyiben technikailag megoldható)
2. *Informatikai természetű biztosítékok*
   - adatkezelés szigorú, Informatikai Biztonsági Szabályzatban rögzített módon
   - adattovábbítás kriptográfiával (amennyiben megoldható)
   - korlátozott elérés az informatikai rendszereken tárolt személyes adatokhoz (időben és személyileg)
3. *Érintetti rendelkezés biztosítása*
   - Érintettek előzetes véleményének bekérése
   - Érdekteszt szempontjainak és tartalmának előzetes ismertetése
   - Személyes profilban közvetlen, rendelkezési jogot adó felhasználói online vagy egyéb hálózati hozzáférés

Speciális (garanciális) biztosítékok:

- adatvédelmi ellenőrzés lefolytatása harmadik személynek történő adatmegküldés előtt
- adatvédelmi szakmai tanácsadás igénybevétele
- elfogadott tanúsítási mechanizmus
- magatartási kódexekhez csatlakozás és alkalmazása
- érdekmérlegelési teszt fél évente történő felülvizsgálata
- tiltakozás és tájékoztatás joga gyakorlásának egyszerűbbé tétele az érintett számára (érdekteszt közzététele, közvetlen tiltakozási lehetőség online)

4. SZÁMÚ MELLÉKLET

HOZZÁJÁRULÓ nyilatkozat
személyes adatok kezeléséhez

Alulírott, ... az Európai Parlament és a Tanács (EU) 2016/679 rendeletének 6. cikk (1) a) pontja alapján a **Bokod Község Önkormányzata/ Bokodi Polgármesteri Hivatal** részére hozzájárulásomat adom/adjuk a lentebb meghatározott és felsorolt személyes adatok kezeléséhez ..... céljából.

Az adatkezelés jogalapja: 14 év alatti gyermek esetében a szülő (törvényes képviselő) hozzájárulása, 14-16 év közötti gyermek esetében a szülő és a gyermek közösen jogosult nyilatkozni, 16 év fölött a gyermek önállóan jogosult a hozzájárulás megadására.

Kezelt személyes adatok: .....

Kijelentem/ Kijelentjük, hogy ezen hozzájárulásomat, önkéntesen, minden külső befolyás nélkül a megfelelő tájékoztatás ismeretében tettem meg.

Jelen hozzájárulás bármikor korlátozás, feltétel és indoklás nélkül visszavonható.

A hozzájáruló nyilatkozat visszavonását a **Bokod Község Önkormányzata/ Bokodi Polgármesteri Hivatal** felé kell jelezni a következő módokon és elérhetőségekre:

Elektronikus levél útján a következő e-mail címre: hivatal@bokod.hu
Papaír alapú levél útján és személyesen a **Bokod Község Önkormányzata/ Bokodi Polgármesteri Hivatal** székhelyére: **2855 Bokod, Hősök tere 6.**
Telefonos megkeresés útján a következő telefonszámon: **34/490-151**

Kérésére/Kérésükre a személyes adatok kezeléshez való hozzájárulás visszavonása megtételekor, a **Bokod Község Önkormányzata/ Bokodi Polgármesteri Hivatal** az Ön/Önök rendelkezésére bocsát egy hozzájárulás visszavonását tartalmazó üres nyilatkozatot, amelynek kitöltésével és visszaküldésével/visszaadásával, bizonyítható módon megtörténik az Ön/Önök hozzájárulásának visszavonása.

A hozzájárulás visszavonása nem érinti a hozzájáruláson alapuló, a visszavonás előtti adatkezelés jogszerűségét.

A személyes adatokat a **Bokod Község Önkormányzata/ Bokodi Polgármesteri Hivatal** az érintett/érintettek kérésére történő törlésig kezeli.

Ezen hozzájáruló nyilatkozat nem vonatkozik a kezelt személyes adatok harmadik személy részére történő továbbításra.

Ezen nyilatkozattal az érintett/érintettek hozzájárul/hozzájárulnak a kezelt személyes adatok harmadik személy részére történő átadására.

Harmadik személy:

Jelen hozzájárulás megadása tekintetében nyilatkozom/nyilatkozunk, hogy a gyermek felett a szülői felügyeleti jogot közösen gyakoroljuk/egyedül gyakorlom.

Különélő vagy elvált szülők esetében csak az a szülő adhat érvényes adatkezelési nyilatkozatot, aki a szülői felügyeleti jogok gyakorlására jogosult - az intézménynek azonban nem feladata, hogy ezt a kérdést mélységében vizsgálja, el kell fogadnia az erről szóló szülői tájékoztatást azzal, hogy vita esetén az ellentmondást az erre jogosult hatóságnak (gyámhatóság, bíróság) kell megoldania.

A jelen aláírásommal igazolom, hogy a **Bokod Község Önkormányzata/ Bokodi Polgármesteri Hivatal** Adatvédelmi Tájékoztatóját az alábbi módon megismertem és megértettem:

- weblapon történő elérés útján megismertem
- nyomtatott formában elolvastam
- nyomtatva átvettem[2]

Kelt:

....

Nyilatkozó Nyilatkozó

[2] Kérem, hogy a megfelelő részt szíveskedjen aláhúzni

5. SZÁMÚ MELLÉKLET

A SZEMÉLYES ADATOK KEZELÉSÉHEZ

HOZZÁJÁRULÓ NYILATKOZAT VISSZAVONÁSA

Alulírott, ... az Európai Parlament és a Tanács (EU) 2016/679 rendeletének 6. cikk (1) a) pontja alapján a **Bokod Község Önkormányzata/ Bokodi Polgármesteri Hivatal** részére az alábbi meghatározott személyes adataim adatkezeléshez való hozzájárulásomat,-

kezelt személyes adatok: .....

-melyet ..... napján tettem, a jelen nyilatkozat aláírásával minden külső befolyás nélkül, szabad akarat elhatározásból a megfelelő tájékoztatás ismeretében visszavonom, mely hozzájárulást abból a célból tettem, hogy a **Bokod Község Önkormányzata/ Bokodi Polgármesteri Hivatal** az alábbi célból az adatait kezelhesse:

.....

Bokod Község Önkormányzata/ Bokodi Polgármesteri Hivatal a jelen visszavonó nyilatkozat alapján, **az Ön személyes adatai hozzájáruláson alapuló további kezelését - amennyiben annak jogszabályi akadálya nincs** - megszünteti és a személyes adatait a **nyilvántartásából töröli**, valamint ennek megtörténtéről írásban értesíti a nyilatkozó személyt.

Kelt.: ....., 201.....

.....

Nyilatkozó

Megismerési nyilatkozat

A 2020. március 1. napjától hatályos adatvédelmi szabályzatot megismertem. Tudomásul veszem, hogy az abban leírtakat a munkám során köteles vagyok betartani.

Név	Beosztás	Dátum	Aláírás
Tóthné Szám Tünde Katalin	általános igazgatási főmunkatárs	2020 FEBR 2 8.	
Gerencsér Judit	adóügyi főmunkatárs	2020 FEBR 2 8.	
Baloghné Vajay Adrienn	pénzügyi főelőadó	2020 FEBR 2 8.	
Lázár Erika	általános igazgatási előadó	2020 FEBR 2 8.	
Baumann Péter	pályázati pénzügyi előadó	2020 FEBR 2 8.	
Dienes Erzsébet	hivatalsegéd	2020 FEBR 2 8.	
Ligártová Anetta	vezető gondozó	2020 FEBR 2 7.	
Bomba Katalin	gondozó	2020 FEBR 2 7.	
Kissné Erdős Analda	gondozó	2020 FEBR 2 7.	
Csillag Sándorné	védőnő	2020 FEBR 2 7.	
Szöllősi Miklós	alpolgármester	2020 FEBR 2 7.	
Trescsikné Magyar Tünde	takarító	2020 FEBR 2 7.	
Kulcsár Attila	karbantartó	2020 FEBR 2 7.	
Kiss Róbert András	karbantartó	2020 FEBR 2 7.	
Gyöngyösi György	karbantartó	2020 FEBR 2 7.	