1/2019. (IX.26.) Elnöki és Jegyzői Együttes Utasítás
a Baranya Megyei Önkormányzat és
a Baranya Megyei Önkormányzati Hivatal
Adatvédelmi és Adatkezelési Szabályzatának kiadásáról

A Baranya Megyei Önkormányzat és a Baranya Megyei Önkormányzati Hivatal (a továbbiakban együtt: adatkezelő szerv) célja, bogy a tevékenységével összefüggésben felmerülő személyes adatok kezelésével járó folyamatai eljárásai során, biztosítsa a személyes adatok védelmének megfelelő szintjét az Európai Parlament és a Tanács (EU) 2016/679 számú, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló rendelete szerint (általános adatvédelmi rendelet, vagy Rendelet).

Jelen szabályzat célja, hogy ismertesse a személyes adatok és a közérdekű adatok kezelése során érvényesítendő szabályokat és eljárásokat mindazon személyekkel, akik az adatkezelő adatvagyonához hozzáférhetnek az Adatkezelővel munkavégzésre, adatfeldolgozásra irányuló jogviszonyban állnak.

Az adatkezelési műveleteket adatkezelő szerv úgy tervezi meg és hajtja végre, hogy az érintettek magánszférájának védelme megfelelő módon biztosított legyen. A technika mindenkori fejlettségére tekintettel megteszi azokat a technikai és szervezési intézkedéseket és kialakítja azokat az eljárási szabályokat, amelyek az adatbiztonság érvényre juttatásához szükségesek. Az adatokat védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés, az adatok károsodása és véletlen elvesztése, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) 24. § (3) bekezdésében, valamint a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény (a továbbiakban: Nytv.) 30. § (1) bekezdésében kapott felhatalmazás alapján az Adatkezelő általános adatvédelmi és adatbiztonsági szabályait az alábbiakban határozzuk meg.

Jelen utasítás 2019. október 1. napján lép hatályba.

Pécs, 2019. szeptember 26.

Madaras Zoltán s.k.
a közgyűlés elnöke

Dr. Partos János s.k.
megyei jegyző

A BARANYA MEGYEI ÖNKORMÁNYZAT ÉS A BARANYA MEGYEI ÖNKORMÁNYZATI HIVATAL

ADATVÉDELMI ÉS ADATKEZELÉSI SZABÁLYZATA

2019.

I. ÁLTALÁNOS RENDELKEZÉSEK

1. Az adatvédelmi és adatkezelési szabályzat alkalmazása

1.1. Jelen szabályzat az információszabadságról szóló 2011. évi CXII. törvény 25/M. § (1) f) pont és 30. § (6) bekezdésében meghatározottakra a közérdekű adatok nyilvánosságának biztosítására, és a 95/46/EK irányelv hatályon kívül helyezéséről szóló Európai Parlament és Tanács 2016/679 számú rendelete 24. cikk (2) bekezdésében vonatkozó szabályokra figyelemmel a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmére és a közérdekű adatok nyilvánosságárnak biztosítására vonatkozó szabályokat állapít meg. A szabályzatban foglaltakat kell alkalmazni a konkrét személyes és közérdekű adatkezelési tevékenységek során, valamint az adatkezelést szabályozó utasítások és tájékoztatások kiadásakor.

2. Értelmező rendelkezések

2.1. Az utasítás alkalmazásában:

2.1.1. **adatbiztonság:** a személyes adatok jogosulatlan vagy jogellenes kezelése, véletlen elvesztése, megsemmisítése vagy károsodása elleni szervezési, technikai megoldások, valamint eljárási szabályok összessége, az adatkezelés azon állapota, amelyben a kockázati tényezőket – és ezáltal a fenyegetettséget – az alkalmazott védelmi intézkedések a minimálisra csökkentik;

2.1.2. **adathordozó:** bármely alakban, bármilyen eszköz felhasználásával és bármely eljárással előállított, személyes adatot tartalmazó, vagy azt megjelenítő tárgy vagy eszköz;

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

2.1.4. **adatfelelős**: az általános közzétételi, valamint a különös és az egyedi közzétételi listában meghatározott adatok továbbítása és állandó karbantartása érdekében kinevezett személy;

2.1.5. **adatgazda**: aki az adott adatkezelésre vonatkozó döntési jogosultsággal rendelkezik, elsődlegesen az érintett adatkezelő szerv legkisebb önálló szervezeti egységének vezetője, adatvédelmi incidens bejelentés eljárásrendjénél és a hatásvizsgálatnál használt fogalom;

2.1.6. **adatkezelés**: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett barmely 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;

2.1.7. **adatkezelő szerv**: a Baranya Megyei Önkormányzat és a Baranya Megyei Önkormányzati Hivatal;

2.1.8. **adatkezelő szerv vezetője:** Baranya Megyei Közgyűlés Elnöke;

2.1.9. **adatkezelő szervezeti egység**: pénzügyi, ügyrendi és területfejlesztési bizottság; Területfejlesztési Osztály; Pénzügyi Osztály; Szervezési Osztály

2.1.10. **adatvédelem: a** személyes adatok jogszerű kezelését, az érintett személyek védelmét és információs önrendelkezési jogának teljesülését biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összessége;

2.1.11. **adatvédelmi hatásvizsgálat:** az adatkezelő szerv által a valószínűsíthetően magas kockázatot jelentő adatkezelés megkezdése előtt lefolytatott, majd azt követően rendszeresen ismételt eljárás, amelynek célja az érintett természetes személyek jogaira nézve gyakorolt hatások vizsgálata, és a magas kockázatú adatkezelési műveletek jelentette kockázatok mérséklése;

2.1.12. **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;

2.1.13. **adatvédelmi incidens észlelésnek ideje az adatkezelő részéről:** az az időpont, amikor az adatkezelő ésszerű mértékben bizonyossággal bír arról, hogy olyan biztonsági sérülés következett be, mely személyes adatok megsértéséhez vezetett;

2.1.14. **információbiztonsági felelős:** az adatkezelő szerv Informatikai Biztonsági Szabályzatáról szóló utasítás szerinti felelős

2.1.15. **bizalmas jelleg sérülése:** a személyes adatok jogosulatlan, illetve véletlen közzététele vagy az ezekhez való hozzáférés;

2.1.16. **egyedi adat:** olyan adat vagy adatok olyan együttese, amely – a mindenkori legjobb technikai lehetőségek igénybevételével – lehetővé teszi a statisztikai egység közvetlen vagy közvetett azonosítását, illetve azon keresztül eddig nem ismert információ felfedését;

2.1.17. **egységes elektronikus adatvédelmi nyilvántartás**: az adatkezelő szervek által végzett adatkezelési tevékenységeket összesítő egységes nyilvántartás;

2.1.18. **érintett fél**: az a természetes személy, akinek az adatkezelési műveletek érintik a jogait és szabadságait;

2.1.19. Hatóság: a tagállami adatvédelmi törvényben kijelölt szerv;

2.1.20. **hivatalos statisztikai** tevékenység: a Központi Statisztikai Hivatal által rendszeresen felülvizsgált statisztikai adat-előállítási folyamat, valamint az azzal kapcsolatos egyéb tevékenység;

2.1.21. **Hivatalos Statisztikai Szolgálat:** a hivatalos statisztikai tevékenységet ellátó szervezet, melynek tagjait a Központi Statisztikai Hivatal elnöke megjelenteti a Hivatalos Értesítőben;

2.1.22. **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;

2.1.23. **információszabadság joga:** az Alaptörvény VI. cikke alapján mindenkinek joga van a közérdekű adatok megismeréséhez és terjesztéséhez;

2.1.24. **integritás sérülése:** a személyes adatok felhatalmazás nélküli vagy véletlenül bekövetkező módosítása;

2.1.25. **közös adatkezelés**: olyan adatkezelés, amely esetében az adatkezelő szerv a feladatkörébe tartozó adatkezelés céljait és eszközeit más adatkezelő szervvel közösen határozza meg, így különösen a közös elektronikus információs rendszer vagy adatkezelési felület alkalmazása

2.1.26. **közérdekű adat:** az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;

2.1.27. **közérdekből nyilvános adat:** a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli;

2.1.28. **rendelkezésre állás sérülése:** a személyes adatok véletlen vagy jogosulatlan megsemmisítése, a személyes adatok elvesztése;

2.1.29. **Ügyfélszolgálat**: az adatkezelő szerv ügyfélszolgálati tevékenységét ellátó szervezeti egység;

2.1.30. **tájékoztatás**: adatvédelmi incidens gyanújáról bejelentés a Szervezet valamely szervezeti egységének részére, amely bárkitől származhat.

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

2.1.32. **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;

2.1.33. **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;

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

3. A szabályzat hatálya

3.1. A Szabályzat szervi hatálya kiterjed a Baranya Megyei Önkormányzat (a továbbiakban: Önkormányzat) és a Baranya Megyei Önkormányzati Hivatal (a továbbiakban: Hivatal) valamennyi szervezeti egységére, a szervezeti egységek kezelésében lévő közérdekű adatokra és közérdekből nyilvános adatokra vonatkozó, az információszabadsággal kapcsolatos követelmények teljesülésének biztosítására a teljes körű feladat- és hatáskörök ellátása során.

3.2. A Szabályzat személyi hatálya kiterjed az Önkormányzat tisztségviselőire, a Hivatal valamennyi köztisztviselőjére, ügykezelőjére, az Önkormányzat és a Hivatal (a továbbiakban együtt: adatkezelő szerv) valamennyi munkavállalójára, valamint a munkavégzésre irányuló egyéb jogviszony keretében foglalkoztatottakra, továbbá azon személyekre, akik szakmai gyakorlatukat a Szervezet valamely szervezeti egységénél töltik.

3.3. Az adatkezelő szerv adatkezelési tevékenységében állandó vagy eseti jelleggel résztvevő vagy abban közreműködő, az adatkezelő szerv érdekkörében adatfeldolgozóként vagy közös adatkezelőként eljáró természetes és jogi személyekkel, jogi személyiséggel nem rendelkező szervezetekkel kötendő szerződésekben, megállapodásokban érvényesíteni kell a személyes adatok kezelésére vonatkozóan az utasításban meghatározott követelményeket.

3.4. Az utasításban foglaltakat kell alkalmazni a szervezeti egységek által folytatott adatkezelési műveletekre az adatok megjelenési formájától függetlenül, az adatkezelés teljes folyamatára kiterjedően – az adatok megszerzésétől vagy a szervezeti egységnél történő keletkezésétől azok törléséig, illetve megsemmisítéséig –, függetlenül attól, hogy az adatok valamely nyilvántartási rendszer vagy valamely ügyben keletkezett irat részét képezik-e.

3.5. A Szabályzat tárgyi hatálya kiterjed az adatkezelő szerv működése, feladat-, és hatáskörének ellátása során kezelt valamennyi közérdekű adatra, személyes és különleges adatra.

4. A szabályzat célja

4.1. E szabályzat célja, hogy harmonizálja az adatkezelési tevékenységek tekintetében az adatkezelő szerv egyéb belső szabályzatainak előírásait a természetes személyek alapvető jogainak és szabadságainak védelme érdekében, valamint biztosítsa a személyes és közérdekű adatok megfelelő kezelését.

4.2. Az adatkezelő szerv tevékenysége során teljes mértékben meg kíván felelni a személyes adatok kezelésére vonatkozó jogszabályi előírásoknak, különösen a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad firamlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről szóló Európai Parlament és a Tanács (Eli) 2016/679 rendeletében foglaltaknak.

4.3. A szabályzat kiadásának további célja, hogy megismerésével és betartásával az adatkezelő szerv alkalmazottai képesek legyenek a természetes személyek adatainak kezelését jogszerűen végezni.

II. RÉSZLETES RENDELKEZÉSEK

5. Az adatkezelés irányelvei

5.1. Általános rendelkezések:

a) A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.

b) A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet, és a személyes adatok nem kezelhetők ezekkel a célokkal össze nem egyeztethető módon.

c) A személyes adatok kezelésének célja megfelelő és releváns legyen, és csak szükséges mértékű lehet.

d) A személyes adatoknak pontosnak és naprakésznek kell lenniük. A pontatlan személyes adatokat haladéktalanul helyesbíteni vagy törölni kell.

e) A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve;

f) Az adatvédelem elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell.

g) Az adatkezelő szerv adatkezelést végző alkalmazottja fegyelmi, kártérítési, szabálysértési és büntetőjogi felelősséggel tartozik a személyes adatok jogszerűtlen kezeléséért.

h) Amennyiben az alkalmazott tudomást szerez arról, hogy az általa kezelt személyes adat hibás, hiányos, vagy időszerűtlen, köteles azt helyesbíteni, vagy helyesbítését az adat rögzítéséért felelős munkatársál kezdeményezi.

i) Az adatkezelő szerv felelős a személyes adatok kezelésére vonatkozó fenti, elveknek való megfelelésért, továbbá képesnek kell lennie e megfelelés igazolására.

6. Az adatkezelő szerv vezetőjének feladatai

6.1. Az adatvédelmi előírások alkalmazása szempontjából az adatkezelő szerv vezetőjének a Megyei Közgyűlés Elnökét kell tekinteni, az adatvédelmi előírások vonatkozásában irányítási jogkört gyakorol az Önkormányzat és a Hivatal személyi állománya tekintetében.

6.2. Az adatkezelő szerv vezetője az általa vezetett adatkezelő szerv vonatkozásában felel:

a) az adatvédelmi és adatbiztonsági intézményrendszer kiépítéséért és működtetéséért;

b) a személyes adatok védelméhez és az információszabadsággal kapcsolatos követelmények érvényesüléséhez szükséges személyi, tárgyi és technikai feltételek biztosítását célzó, hatáskörébe tartozó intézkedések meghozataláért;

c) az általa irányított személyi állomány adatvédelmi oktatásáért és rendszeres továbbképzéséért;
d) a rendszeres adatvédelmi ellenőrzésért, az ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, ennek érdekében a hatáskörébe tartozó eljárások lefolytatásáért;
e) az érintett jogainak gyakorlásához, valamint tájékoztatásához szükséges feltételek biztosításáért;
f) az adatvédelmi hatásvizsgálatok lefolytatásáért és rendszeres felülvizsgálatáért, valamint az ahhoz szükséges feltételek biztosításáért;
g) az adatvédelmi hatásvizsgálat eredményének függvényében előzetes konzultáció kezdeményezéséért a Hatóság felé;
h) az adatvédelmi incidensek nyilvántartásáért, a jogszabályi feltételek fennállása esetén a Hatóság részére határidőben történő bejelentéséért, valamint az adatvédelmi incidenssel érintettek tájékoztatásáért;
i) az adatvédelmi feladatok ellátására alkalmas adatvédelmi tisztviselő kijelöléséért, nevének és elérhetőségének a Hatóság részére történő bejelentéséért;
j) az adatvédelmi tisztviselő feladatainak végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáféréshez, valamint az adatvédelmi tisztviselő szakértői szintű ismereteinek fenntartásához szükséges feltételek és források biztosításáért;
k) az adatvédelmi tevékenységgel kapcsolatos közzétételi kötelezettség teljesítéséért;
l) a közérdekű adatokra és közérdekből nyilvános adatokra irányuló adatigénylések határidőben történő megválaszolásáért.

6.3. Az adatkezelő szerven belül a különleges és személyes, valamint nem nyilvános adat védelméért, a nyilvántartás megőrzéséért, az adatvédelmi tevékenység megszervezéséért a szervezet vezetője felelős. Ezen felelősségét a jelen szabályzat, illetve az adatkezelő szerv egyéb szabályzataiban meghatározottak szerint, az azokban meghatározott munkakört ellátó személyekre ruházhatja. Az adatkezelő szerv vezetője az adatvédelmi feladatok biztosításáért egy fő adatvédelmi tisztviselőt bíz meg, aki munkáját eredeti munkaköre ellátása mellett látja el.

6.4. Az adatkezelő szerv vezetője jogosult az adatvédelmi tisztviselő és az adatgazdák kijelölésére és tevékenységük ellenőrzésére.

7. Az adatvédelmi tisztviselő

7.1. Az adatvédelmi tisztviselőt a személyes adatok védelme területén szerzett ismeretei és gyakorlati tapasztalatai, valamint a számára jogszabályban vagy normában meghatározott feladatok ellátására való alkalmasság alapján, írásban jelöli ki az adatkezelő szervezet vezetője.

7.2. Az adatkezelő szerv vezetője az adatvédelmi tisztviselő számára a szabályzatban meghatározottak végrehajtásában való közreműködése érdekében feladatot határozhat meg.

7.3. Nem lehet olyan személyt kijelölni adatvédelmi tisztviselőnek, aki az adatkezelő szervnél adatkezeléssel kapcsolatos döntések meghozatalára jogosult személynek a Polgári Törvénykönyvről szóló 2013. évi V. törvény 8:1. §. 2. pontja szerinti hozzátartozója.

7.4. Az adatvédelmi tisztviselő ellátja az adatkezelő szerv közérdekből nyilvános és közérdekű adatok, valamint a nem nyilvános adatok kezelésével összefüggő feladatok szakmai irányítását.

7.5. Az adatvédelmi tisztviselő munkaköri leírásának tartalmaznia kell a főbb ellátandó feladatait.

7.6. Az adatvédelmi tisztviselő nevéről és elérhetőségéről az adatkezelő szervnél foglalkoztatottakat tájékoztatni kell, valamint a Hatóság nyilvántartásába be kell jelenteni.

7.7. Amennyiben szükséges, az adatvédelmi tisztviselő számára feladatainak ellátása céljából, biztosítani kell a minősítéssel védhető közérdek körébe tartozó iratokba való betekintést, és az ennek jogszerű gyakorlásához szükséges személyi biztonsági feltételeknek történő megfelelést.

7.8. Adatvédelmi tisztviselőnek felsőfokú végzettséggel rendelkező személy jelölhető ki.

7.9. Az adatkezelő szerv vezetője biztosítja az adatvédelmi tisztviselő számára meghatározott feladata kapcsán eljárva a hozzáférést a feladatai végrehajtásához szükséges elektronikus rendszerekhez, iratokhoz, egyéb adathordozókhoz, valamint a szakmai ismeretei naprakészen tartásához szükséges feltételeket, jogosultságokat és erőforrásokat rendelkezésére bocsátja.

7.10. Az adatkezelő szerv vezetője biztosítja annak lehetőségét, hogy az adatkezelő szervvel bármely jogszabály alapján foglalkoztatási jogviszonyban álló személyek a személyes adatai kezeléséhez és jogai gyakorlásához kapcsolódó valamennyi kérdésben a hivatali út betartása nélkül, közvetlenül és egyszerű módon fordulhassanak az adatvédelmi tisztviselőhöz.

7.11. Az adatvédelmi tisztviselő az adatkezelő szervnél más feladatokat is elláthat, azonban az adatkezelő szerv köteles biztosítani, hogy ezekből a más feladatokból adódóan ne keletkezzen összeférhetetlenség, és az egyéb munkaköri feladatok ellátása nem veszélyeztetheti az adatvédelmi tisztviselői feladatok ellátását.

7.12. Az adatvédelmi tisztviselő munkáját a hatályos jogszabályok, jelen szabályzat alapján látja el. Elsődleges feladata az adatvédelmi szabályok érvényesülésének biztosítása az adatkezelő szervnél. Az adatvédelmi tisztviselő folyamatosan figyelemmel kíséri az adatvédelemre vonatkozó szabályok és előírások érvényesülését, betartását, az adatvédelem helyzetének alakulását az adatkezelő szervezetben. Rendszeresen tájékoztatást nyújt az adatkezelő szerv vezetőjének. Javaslatokat tesz az adatvédelem helyi szintű szabályozására, konkrét feladatok ellátására. Folyamatosan kapcsolatot tart az adatgazdákkal, segítséget nyújt a munkájukhoz.

7.13. Az adatvédelmi tisztviselő elősegíti, hogy az adatkezelő szerv az adatvédelmi követelményeknek – megfelelően dokumentált módon – eleget tegyen, így különösen:

a) az adatvédelemre vonatkozó jogszabályokban, közjogi szervezetszabályozó eszközökben és belső normákban foglalt jogi előírásokról, kötelezettségekről naprakész tájékoztatást, illetőleg érvényesítésüket szolgáló tanácsot ad az adatkezelő szerv munkavállalói számára;

b) részt vesz az adatvédelmet érintő belső normák kidolgozásában és közreműködik az adatkezeléssel járó vagy azt eredményező döntések előkészítésében;

c) elősegíti az adatkezelő szervnél foglalkoztatottak adatvédelmi és adatbiztonsági tudatosságának növelését, ennek érdekében szervezi az adatkezelési folyamatokban részt vevő foglalkoztatottak képzését;

d) a végzett, és az új adatkezelésekkel kapcsolatos döntések következtében az érintettek jogaira nézve megjelenő kockázatok tekintetében előzetes adatvédelmi kockázatelemzést végezhet, részt vesz a valószínűsíthetően magas kockázatot jelentő adatkezelésekre vonatkozó hatásvizsgálat lefolytatásában;

e) szakmai tanácsaival segíti és felügyeli az adatvédelmi hatásvizsgálat lefolytatását, a hatásvizsgálatról szóló jelentés elkészítését, melyet az adatkezelő szerv vezetőjének jóváhagyása után bevezet az adatkezelési tevékenységek nyilvántartásába;

f) közreműködik a Hatósággal az előzetes konzultáció lefolytatásában;

g) tevékenysége során együttműködik az adatkezelés jogszerűségével kapcsolatos eljárások lefolytatására jogosult szervekkel és hatóságokkal, így különösen kapcsolatot tart a Hatósággal, közreműködik az adatkezelő szervet érintő vizsgálatok lefolytatásában és az ezekkel összefüggő megkeresések megválaszolásában;

h) az adatkezelő szerv vezetője által jóváhagyott ellenőrzési tervet készít, a tervben foglaltak szerint – szükség esetén, így különösen adatvédelmi incidens bekövetkezése miatt ezen túlmenően is – ellenőrzi az adatkezelő szervnél az adatvédelmi és adatbiztonsági követelmények megtartását;

i) az adatkezeléssel kapcsolatos előírások megszegésének észlelése esetén az adatvédelmi tisztviselő felhív a jogszerű állapot haladéktalan helyreállítására, és a hiányosságokat – amennyiben emiatt adatvédelmi érdek sérelmet szenvedne, úgy közvetlenül – jelzi az adatkezelő szerv vezetőjének, indokolt esetben kezdeményezi a felelősség megállapításához szükséges eljárás lefolytatását;

j) közreműködik az adatvédelmi incidensek kivizsgálásában, vezeti adatkezelő szervezet adatvédelmi incidens nyilvántartását, és a vizsgálat eredménye alapján a jogszabályi feltételek fennállása esetén bejelenti azt a Hatóság részére.

k) személyes adatot nem tartalmazó kimutatást vezet az érintettnek a személyes adatai kezelésével kapcsolatos hozzáférésre, helyesbítésre, törlésre, tiltakozásra, valamint korlátozásra vonatkozóan benyújtott és elutasított kérelméről, az elutasítás indokairól, amelyekről minden év január 31-ig megküldött éves jelentésben tájékoztatja a Hatóságot, részt vesz a Hatóság által szervezett képzéseken.

l) Koordinálja az adatkezelő szervhez érkező közérdekű adat megismerésre vonatkozó igények teljesítését.

7.14. Az Önkormányzat és a Hivatal közös adatvédelmi tisztviselőt alkalmaz.

7.15. Az adatvédelmi tisztviselő nevét és elérhetőségét a www.baranya.hu honlapon kell közzétenni, a megyei jegyző gondoskodik az adatvédelmi tisztviselő nevének és elérhetőségének a felügyeleti hatósággal történő közlésről.

8. Egyéb felelősségi szabályok

8.1. Az adatkezelő szerv által kezelt személyes adatok védelmének biztosításáért, az adatgazdák és az adatkezelést végzők tevékenységével kapcsolatos közérdekű adatok nyilvánosságra hozásával és a közérdekű adatigényléssel összefüggő adatszolgáltatási feladatok ellátásáért:

a) a megyei jegyző;
b) a megyei jegyző által kijelölt adatvédelmi tisztviselő;
c) a szervezeti egységek vezetői;
d) az adatkezelési és adatfeldolgozást végző munkatársak

felelnek.

8.2. A megyei jegyző felelősségi körén belül:

a) felel a személyes adatok védelmére vonatkozó jogszabályok, valamint jelen szabályzatban foglalt előírások betartásáért, betartatásáért, illetve e követelmények teljesítésének ellenőrzéséért;

b) köteles gondoskodni az adatvédelmi és adatbiztonsági szabályzat kiadásáról, annak évenkénti aktualizálásáról.

8.3. Az adatvédelmi tisztviselő, mint a Hivatal jogi, közigazgatási végzettséggel rendelkező munkatársa felelősségi körén belül:

a) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában;

b) a konkrét ügyekben felmerült adatvédelmi kérdésekben tájékoztatást ad a Hivatal munkatársainak;

c) a megyei jegyző iránymutatása alapján közreműködik a személyes adatok védelmére vonatkozó jogszabályok, valamint jelen szabályzatban foglalt előírások betartásának ellenőrzésében;

d) közreműködik -az adatvédelmi és adatbiztonsági szabályzat elkészítésében, évenkénti felülvizsgálatában;

e) kivizsgálja a hozzá érkezett bejelentéseket, és jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót,
f) vezeti az adattovábbítási nyilvántartást;
g) ismerteti a Hivatal munkatársaival az adatvédelmi követelményeket, szükség esetén oktatást szervez.

8.4. A szervezeti egységek vezetői biztosítják, hogy az általuk vezetett szervezeti egység munkatársai betartsák az adatkezeléssel kapcsolatos jogszabályok, jelen Szabályzat előírásait.

8.5. Adatkezelést és adatfeldolgozást végző munkatárs köteles:
a) az adatkezeléssel és adatvédelemmel kapcsolatos jogszabályok, és a jelen Szabályzat előírásait megismerni és maradéktalanul betartani;
b) tájékoztatni az adatvédelmi tisztviselőt a feladat-, és hatáskörében felmerült adatvédelmi visszásságról;
c) az adatvédelmi tisztviselő észrevétele eseten az adatkezeléssel kapcsolatban feltárt visszásságot haladéktalanul megszüntetni.

III. SZEMÉLYES ADATOK VÉDELME

9. adatkezelés irányelvei

9.1. A személyes adatok kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.
9.2. A személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történhet.
9.3. A személyes adatok kezelésének célja megfelelő és releváns legyen, és csak a szükséges mértékű lehet.
9.4. A személyes adatoknak pontosnak és naprakésznek kell lenniük. A pontatlan személyes adatokat haladéktalanul törölni kell.
9.5. A személyes adatok tárolásának olyan formában kell történnie, hogy az érintettek azonosítását csak szükséges ideig tegye lehetővé. A személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, ha a tárolás közérdekű archiválási céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történik.
9.6. A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.
9.7. Az adatvédelem elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell.
9.8. Az adatkezelő szerv adatkezelést végző alkalmazottja fegyelmi, kártérítési, szabálysértési és bűntetőjogi felelősséggel tartozik a személyes adatok jogszerű kezeléséért. Amennyiben az alkalmazott tudomást szerez arról, hogy az általa kezelt személyes adat hibás, hiányos, vagy időszerűtlen, köteles azt helyesbíteni, vagy helyesbítését az adat rögzítéséért felelős munkatársa kezdeményezni.

10. Személyes adatok kezelése

10.1. Az adatkezelő feladatellátása során személyes adat kezelésére jogszabályban meghatározott feladat-, és hatáskörének gyakorlásához szükséges célból, jog gyakorlása vagy kötelezettség teljesitése érdekében kerülhet sor, kizárólag a cél megvalósulásához szükséges mértékben és ideig.
10.2. Az adatkezelés és az adatfeldolgozás során mindvégig szem előtt kell tartani a személyes adatok kezelésének célhoz kötöttséget, a feladatellátás során kezelt adatokat csak az adott ügy elintézése érdekében szabad kezelni, felhasználni, más eljárásokkal, illetve adatokkal nem kapcsolhatók össze. Az adatkezelő által kezelt személyes adatok magáncélra való felhasználása tilos.

11. Az adatkezelés jogszerűsége

11.1. Mivel a természetes személyek összefüggésbe hozhatók az általuk használt készülékek, alkalmazások, eszközök és protokollok által rendelkezésre bocsátott online azonosítókkal, például IP-címükkel és cookie, süti-azonosítókkal, ezért ezek az adatok egyéb információkkal összekapcsolva alkalmasak és felhasználhatók a természetes személyek profiljának létrehozására és az adott személy azonosítására.

11.2. Az adatkezelésre csak akkor kerülhet sor, ha az érintett személy egyértelmű megerősítő cselekedettel, például írásbeli ideértve az elektronikus úton tett vagy szóbeli nyilatkozattal önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulását adja az adatok kezeléséhez.

11.3. Az adatkezeléshez való hozzájárulásnak minősül az is, ha az érintett személy az internetes honlap megtekintése során bejelöl egy erre vonatkozó négyzetet. Az elhallgatás, az előre bejelölt négyzet vagy a nem cselekvés nem minősül hozzájárulásnak. Hozzájárulásnak minősül az is, ha valamely felhasználó az elektronikus szolgáltatások igénybevétele során erre vonatkozó technikai beállításokat hajt végre, vagy olyan nyilatkozatot, illetve cselekedet tesz, amely az adott összefüggésben az érintett személy hozzájárulását személyes adatainak kezeléséhez egyértelműen jelzi.

11.4. Az egészségügyi személyes adatok körébe tartoznak az érintett egészségi állapotára vonatkozó olyan adatok, amelyek információt hordoznak az érintett múltbeli, jelenlegi vagy jövőbeli testi vagy pszichikai egészségi állapotáról. Ide tartoznak az alábbiak:

a) egészségügyi szolgáltatások céljából történő nyilvántartásba vétel;
b) a természetes személy egészségügyi célokból történő egyéni azonosítása érdekében hozzá rendelt szám, jel vagy adat;
c) valamely testrész vagy a testet alkotó anyag beleértve a genetikai adatokat és a biológiai mintákat is - teszteléséből vagy vizsgálatából származó információk;
d) az érintett betegségével, fogyatékosságával, betegségkockázatával, kórtörténetével, klinikai kezelésével vagy fiziológiai vagy orvosbiológiai állapotával kapcsolatos információ, függetlenül annak forrásától, amely lehet például orvos vagy egyéb egészségügyi dolgozó, kórház, orvostechnikai eszköz vagy diagnosztikai teszt. A genetikai adatot olyan, a természetes személy örökölt vagy szerzett genetikai jellemzőivel összefüggő személyes adatként kell meghatározni, amely az érintett személytől vett biológiai minta elemzésének különösen kromoszómaelemzésnek, illetve a dezoxiribonukleinsav (DNS) vagy a ribonukleinsav (RNS) vizsgálatának, vagy az ezekből nyerhető információkkal megegyező információk kinyerését lehetővé tevő bármilyen más elem vizsgálatának - az eredménye.

11.5. A gyermekek személyes adatai különös védelmet érdemelnek, mivel ők kevésbé lehetnek tisztában a személyes adatok kezelésével összefüggő kockázatokkal, következményeivel és az ahhoz kapcsolódó garanciákkal és jogosultságokkal. Ezt a különös védelmet főként a gyermekek személyes adatainak olyan felhasználására kell alkalmazni, amely marketingcélokat, illetve személyi vagy felhasználói profilok létrehozását nem szolgálja.

11.6. A személyes adatokat olyan módon kell kezelni, amely biztosítja azok megfelelő szintű biztonságát és bizalmas kezelését, többek között annak érdekében, hogy megakadályozza a személyes adatokhoz és a személyes adatok kezeléséhez használt eszközökhöz való jogosulatlan hozzáférést, illetve azok jogosulatlan felhasználását.

11.7. A pontatlan személyes adatok helyesbítése vagy törlése érdekében minden észszerű lépest meg kell tenni.

11.8. A személyes adatok kezelése akkor jogszerű, ha az alábbiak valamelyike teljesül:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek,

11.9. A 11.8. pontban foglaltak értelmében az adatkezelés jogszerűnek minősül, ha arra valamely szerződés vagy szerződéskötési szándék keretében van szükség.

11.10. Ha az adatkezelésre az adatkezelőre vonatkozó jogi kötelezettség teljesítése keretében kerül sor, vagy ha az közérdekű feladat végrehajtásához, illetve közhatalmi jogosítvány gyakorlásához szükséges, az adatkezelésnek az uniós jogban vagy valamely tagállam jogában foglalt jogalappal kell rendelkeznie,

11.11. Az adatkezelést jogszerűnek kell tekinteni akkor, amikor az az érintett életének vagy más fent említett természetes személy érdekeinek védelmében történik. Más természetes személy létfontosságú érdekeire hivatkozással személyes adatkezelésre elvben csak akkor kerülhet sor, ha a szóban forgó adatkezelés egyéb jogalapon nem végezhető.

11.12. A személyes adatkezelés néhány típusa szolgálhat egyszerre fontos közérdeket és az érintett létfontosságú érdekeit is, például olyan esetben, amikor az adatkezelésre humanitárius okokból, ideértve, ha arra a járványok és terjedéseik nyomon követéséhez, vagy humanitárius vészhelyzetben, különösen természeti vagy ember által okozott katasztrófák esetében van szükség.

11.13. Az adatkezelő ideértve azt az adatkezelőt is, akivel a személyes adatokat közölhetik- vagy valamely harmadik fél jogos érdeke jogalapot teremthet az adatkezelésre. Az ilyen jogos érdekről lehet szó például olyankor, amikor releváns és megfelelő kapcsolat áll fenn az érintett és az adatkezelő között, például olyan esetekben, amikor az érintett az adatkezelő ügyfele vagy annak alkalmazásában áll.

11.14. Személyes adatoknak a csalások megelőzése céljából feltétlenül szükséges kezelése szintén az érintett adatkezelő jogos érdekének minősül. Személyes adatok közvetlen üzletszerzési célú kezelése szintén jogos érdeken alapulónak tekinthető.

11.15. A jogos érdek fennállásának megállapításához mindenképpen körültekintően meg kell vizsgálni többek között azt, hogy az érintett a személyes adatok gyűjtésének időpontjában és azzal összefüggésben számíthat-e észszerűen arra, hogy adatkezelésre az adott célból kerülhet sor. Az érintett érdekei és alapvető jogai elsőbbséget élvezhetnek az adatkezelő érdekével szemben, ha a személyes adatokat olyan körülmények között kezelik, amelyek közepette az érintettek nem számítanak további adatkezelésre.

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

11.17. A személyes adatoknak a gyűjtésük eredeti céljától eltérő egyéb célból történő kezelése csak akkor megengedett, ha az adatkezelés összeegyeztethető az adatkezelés eredeti céljaival, amelyekre a személyes adatokat eredetileg gyűjtötték. Ebben az esetben nincs szükség attól a jogalaptól eltérő, külön jogalapra, mint amely lehetővé tette a személyes adatok gyűjtését.

12. Az érintett személy hozzájárulása, feltételek

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

12.2. Ha az érintett a hozzájárulását olyan írásbeli nyilatkozat keretében adja meg, amely más ügyekre is vonatkozik, a hozzájárulás iránti kérelmet ezektől a más ügyektől egyértelműen megkülönböztethető módon kell közölni.

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

12.4. Annak megállapítása során, hogy a hozzájárulás önkéntes-e, a lehető legnagyobb mértékben figyelembe kell venni azt a tényt egyebek mellett, hogy a szerződés teljesítésének — beleértve a szolgáltatások nyújtását is — feltételül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez.

12.5. Közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában végzett személyes adatok kezelése akkor jogszerű, ha a gyermek a 16. életévét betöltötte. A 16. életévét be nem töltött gyermek esetén, a gyermekek személyes adatainak kezelése csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte.

12.6. A faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok kezelése tilos, kivéve a GDPR 9. cikk (2) bekezdésében meghatározott eseteket.

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

13. Azonosítást nem igénylő adatkezelés

13.1. Ha azok a célok, amelyekből az adatkezelő a személyes adatokat kezeli, nem vagy már nem teszik szükségessé az érintettnek az adatkezelő általi azonosítását, az adatkezelő nem köteles kiegészítő információkat megőrizni, beszerezni annak érdekében, hogy pusztán azért azonosítsa az érintettet, bogy megfeleljen a GDPR előírásainak.

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

14. Az érintett személy tájékoztatáshoz fűződő joga

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

14.2. Ha a személyes adatokat az érintettől gyűjtik, az érintettet arról is tájékoztatni kell, bogy köteles-e a személyes adatokat közölni, valamint, hogy az adatszolgáltatás elmaradása milyen következményekkel jár. Ezeket az információkat szabványosított

ikonokkal is ki lehet egészíteni annak érdekében, hogy az érintett a tervezett adatkezelésről jól látható, könnyen érthető és jól olvasható formában általános tájékoztatást kapjon.

14.3. Az érintettre vonatkozó személyes adatok kezelésével összefüggő tájékoztatást az adatgyűjtés időpontjában kell az érintett részére megadni, illetve ha az adatokat nem az érintettől, hanem más forrásból gyűjtötték, az ügy körülményeit figyelembe véve, észszerű határidőn belül kell rendelkezésre bocsátani.

14.4. Az érintett jogosult, hogy hozzáférjen a rá vonatkozóan gyűjtött adatokhoz, valamint arra, hogy egyszerűen és észszerű időközönként, az adatkezelés jogszerűségének megállapítása és ellenőrzése érdekeben gyakorolja e jogát. Minden érintett számára biztositani kell a jogot arra, bogy megismerje különösen a személyes adatok kezelésének céljait, továbbá, ha lehetséges azt, hogy a személyes adatok kezelése milyen időtartamra vonatkozik.

14.5. Az érintett jogosult különösen arra, hogy személyes adatait töröljék és a továbbiakban ne kezeljék, ha a személyes adatok gyűjtésére vagy más módon való kezelésére az adatkezelés eredeti céljaival összefüggésben mar nincs szükség, vagy ha az étintettek visszavonták az adatok kezeléséhez adott hozzájárulásukat.

14.6. Ha a személyes adatok kezelése közvetlen üzletszerzés érdekében történik, az érintett számára biztosítani kell a jogot arra, hogy bármikor díjmentesen tiltakozzon a rá vonatkozó személyes adatok e célból történő kezelése ellen.

15. A személyes adatok kezelésének felülvizsgálata

15.1. Annak biztosítása érdekében, hogy a személyes adatok kezelése és tárolása a szükséges időtartamra korlátozódjon, az adatkezelő szerv vezetője törlési vagy rendszeres adatkezelési felülvizsgálati határidőket állapít meg.

15.2. Az adatkezelő szerv esetében a megállapított rendszeres adatkezelési felülvizsgálati határidő: 1 év.

16. Az adatkezelő feladatai

16.1. Az adatkezelő a jogszerű adatkezelés érdekében megfelelő belső adatvédelmi szabályokat alkalmaz. Ez a szabályozás kiterjed az adatkezelő hatáskörére és felelősségére.

16.2. Az adatkezelő kötelessége, hogy megfelelő és hatékony intézkedéseket hajtson végre valamint, hogy képes legyen igazolni azt, bogy az adatkezelési tevékenységek a hatályos jogszabályoknak megfelelnek. Ezt a szabályozást az adatkezelés jellegének, hatókörének, körülményeinek és céljainak, valamint a természetes személyek jogait és szabadságait érintő kockázatnak a figyelembevételével kell megvalósítani.

16.3. Az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre. E szabályzat alapján az egyéb belső szabályzatokat felülvizsgálja és szükség esetén naprakésszé teszi.

16.4. Az adatkezelő vagy az adatfeldolgozó megfelelő nyilvántartást vezet a hatásköre alapján végzett adatkezelési tevékenységekről. Minden adatkezelő és adatfeldolgozó köteles a felügyeleti hatósággal együttműködni és ezeket a nyilvántartásokat kérésre hozzáférhetővé tenni az érintett adatkezelési műveletek ellenőrzése érdekében.

17. Az adatkezeléssel kapcsolatos jogok

17.1. Az adatkezeléssel kapcsolatos jogok a következők:

a) A tájékoztatás kéréshez való jog;
b) a helyesbítéshez való jog;
c) a törléshez való jog;
d) a zároláshoz, korlátozáshoz való jog;
e) a tiltakozáshoz való jog.

17.2. A tájékoztatás kéréshez való jog: Bármely személy a www.baranya.hu honlapon a közzétételi listában megadott elérhetőségeken (a továbbiakban: Megadott elérhetőségeken) keresztül tájékoztatást kérhet arról, hogy az adatkezelő szerv milyen adatait, milyen jogalapon, milyen adatkezelési cél miatt, milyen forrásból, mennyi ideig kezeli. A kérelmére haladéktalanul, de legfeljebb 30 napon belül, a megadott elérhetőségre tájékoztatást kell küldeni, közérthető formában.

17.3. Az érintett tájékoztatást kérhet személyes adatainak kezeléséről, annak céljáról, jogalapjáról, időtartamáról, az adatfeldolgozó nevéről, elérhetőségéről és az adatkezeléssel összefüggő tevékenységéről, az adatvédelmi incidens körülményeiről, hatásairól és az elhárítására tett intézkedésekről, továbbá az érintett személyes adatainak továbbítása esetén az adattovábbítás jogalapjáról és címzettjéről.

17.4. A helyesbítéshez való jog: Bármely személy a megadott elérhetőségeken keresztül kérheti bármely adatának módosítását. Erről kérelmére haladéktalanul, de legfeljebb 30 napon beül intézkedni kell és a megadott elérhetőségre tájékoztatást kell küldeni, közérthető formában. A valóságnak meg nem felelő adatot - amennyiben rendelkezésre áll a helyes adat - az adatkezelő helyesbíteni köteles.

17.5. A törléshez való jog: Bármely személy a megadott elérhetőségeken keresztül kérheti adatának törlését. Kérelmére ezt haladéktalanul, de legfeljebb 30 napon belül meg kell tenni és a megadott elérhetőségre tájékoztatást kell küldeni, közérthető formában.

17.6. A zároláshoz, korlátozáshoz való jog: Bármely személy a megadott elérhetőségeken keresztül kérheti adatának zárolását. A zárolás addig tart, amig a megjelölt indok szükségessé teszi az adatok tárolását. A kérelemre ezt haladéktalanul, de legfeljebb 30 napon belül meg kell tenni és a megadott elérhetőségre tájékoztatást kell küldeni, közérthető formában.

17.7. A tiltakozáshoz való jog: Bármely személy a megadott elérhetőségeken keresztül tiltakozhat az adatkezelés ellen. A tiltakozást a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 15 napon belül meg kell vizsgálni, annak megalapozottsága kérdésében az Önkormányzat esetében a Baranya Megyei Közgyűlés elnökének, a Hivatal esetében a megyei jegyzőnek döntést kell hozni és a döntésről a megadott elérhetőségre tájékoztatást kell küldeni. Amennyiben a tiltakozás indokolt, az adatkezelő köteles az adatkezelést beleértve a további adatfelvételt és az adat továbbítását is megszüntetni és az adatokat zárolni, valamint a tiltakozásról és az annak alapján tett intézkedésekről értesíteni mindazokat, akik részére a tiltakozással érintett személyes adatot korábban továbbította, és akik kötelesek intézkedni a tiltakozási jog érvényesítése érdekében.

17.8. Ha az érintett az adatkezelő döntésével nem ért egyet, illetve ha az a határidőt elmulasztja, jogérvényesítés érdekében az alábbi Hatósághoz fordulhat:

Nemzeti Adatvédelmi és Információszabadság Hatóság.
Postacím: 1530 Budapest, Pf.: 5.
Cím: 1125 Budapest, Szilágyi Erzsébet fasor
Telefon: ±36(1) 391-1400
Fax: +36 (1) 391-1410
E-mail: ugyfelszolgalat@naih.hu
URL https://naih.hu

17.9. Az érintett a jogainak megsértése esetén bírósághoz fordulhat.

18. A Szervezet feladatai a megfelelő adatvédelem érdekében

18.1. Az adatvédelmi tudatosság: Biztosítani kell a szakmai felkészültséget a jogszabályoknak való megfeleléshez. Ezért elengedhetetlen a munkatársak szakmai felkészítése és az adatvédelmi és adatvédelmi szabályzat megismerése.

18.2. Át kell tekinteni az adatkezelés célját, szempontrendszerét, a személyes adatkezelés koncepcióját. Az adatvédelmi és adatkezelési szabályzattal összhangban kell biztosítani jogszerű adatkezelést és adatfeldolgozást.

18.3. Figyelni kell arra, hogy ha az adatkezelés az érintett hozzájárulásán alapul, kétség esetén az adatkezelőnek kell bizonyítania azt, hogy az adatkezeléshez az érintett személy hozzájárult.

18.4. Az érintett személynek nyújtott tájékoztatás tömör, könnyen hozzáférhető és könnyen érthető legyen, ezért azt világos és közérthető nyelven kell megfogalmazni és megjeleníteni.

18.5. Az átlátható adatkezelés követelménye, hogy az érintett személy tájékoztatást kapjon az adatkezelés tényéről és céljáról, a tájékoztatást az adatkezelés megkezdése elött kell megadni és a tájékoztatáshoz való jog az adatkezelés során annak megszűnéséig megilleti az érintettet.

18.6. Ezzel összefüggésben az adatkezelésben érintett személy főbb jogai a következők:

a) a rá vonatkozó személyes adatokhoz való hozzáférés;
b) a személyes adatok helyesbítése;
c) a személyes adatok törlése;
d) a személyes adatok kezelésének korlátozása;
e) a profilalkotás és az automatizált adatkezelés elleni tiltakozás; az adathordozhatósághoz való jog.

18.7. Az adatkezelő indokolatlan késedelem nélkül, de legkésőbb a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet. Szükség eseten, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható, A tájékoztatási kötelezettség biztosítható egy olyan biztonságos online rendszer üzemeltetésével, amelyen keresztül az érintett könnyen és gyorsan hozzáférhet a szükséges információhoz.

18.8. Át kell tekinteni az adatkezelő szerv által végzett adatkezeléseket, biztosítani kell az információs önrendelkezési jog érvényesülését. Az érintett személy kérésére adatait késedelem nélkül törölni kell, amennyiben az érintett személy visszavonja az adatkezelés alapját képező hozzájárulást.

18.9. Az érintett személy hozzájárulásából félreérthetetlenül ki kell derülnie, hogy az érintett beleegyezik az adatkezelésbe. Ha az adatkezelés az érintett hozzájárulásán alapul, kétség esetén az adatkezelőnek kell bizonyítania, bogy az adatkezelési művelethez az érintett hozzájárult.

18.10. Gyermekek személyes adatkezelése esetén kiemelt figyelmet kell fordítani az adatkezelési szabályok betartására. Közvetlenül gyermekeknek kínált, információs társadalommal összefüggő szolgáltatások vonatkozásában végzett személyes adatok kezelése akkor jogszerű; ha a gyermek a 16. életévét betöltötte. A 16. életévét be nem töltött gyermek eseten, a gyermekek személyes adatainak kezelése csak akkor és olyan mértekben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte.

18.11. A személyes adat jogellenes kezelése vagy feldolgozása esetén bejelentési kötelezettség keletkezik a felügyelő hatóság felé. Az adatkezelőnek indokolatlan késedelem nélkül, ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, meg kell tenni a bejelentést a felügyeleti hatóságnak, kivéve akkor, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személy jogait tekintve.

18.12. Bizonyos esetekben indokolt lehet az adatkezelőnek az adatkezelést megelőzően adatvédelmi hatásvizsgálatot lefolytatni. A hatásvizsgálat során meg kell vizsgálni, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik. Ha az adatvédelmi hatásvizsgálat megállapítja, bogy az adatkezelés valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az adatkezelőnek konzultálnia kell a felügyeleti hatósággal.

18.13. Tekintettel arra, bogy az adatkezelő szerv fő tevékenysége közfeladat ellátása, adatvédelmi tisztviselőt kell kinevezni. Az adatvédelmi tisztviselő kinevezése az adatbiztonság megerősítését célozza.

19. Adatbiztonság

19.1. A személyes adatokat megfelelő intézkedésekkel védeni kell különösen jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés; valamint a véletlen megsemmisülés és sérülés, továbbá az alkalmazott technika megváltozásából fakadó hozzáférhetetlenné válás ellen.

19.2. A nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében megfelelő technikai megoldással biztosítani kell, hogy a nyilvántartásokban az adatok közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők,

19.3. Az adatbiztonság megtervezésekor és alkalmazásakor tekintettel kell: lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek.

19.4. Az ügyiratokat az adatkezelő Iratkezelési Szabályzatában előírtak szerint kell kezelni és tárolni. Az ügyiratok kezelése, tárolása során biztosítani kell, hogy azokba arra jogosulatlan személy ne tekinthessen be.

19.5. Személyes adatokat is tartalmazó iratot vagy más adathordozót a hivatalból kivinni - munkaköri feladat ellátásának kivételével - csak indokolt esetben a felettes vezető tudomásával és engedélyével lehet, ügyelve arra, hogy az ne vesszen el, ne rongálódjon vagy semmisüljön meg és tartalma illetéktelen személy tudomására ne jusson.

19.6. Az ügyintézőnél vagy az irattárban lévő iratokba az ügyintézőn kívül más személy az érintett törvény szerinti betekintési jogán túl csak akkor tekinthet be, ha ezt jogszabály számára lehetővé, vagy az adatkezelő tevékenységével összefüggő feladatellátás szükségessé teszi. Az iratbetekintés és másolat készítése során úgy kell eljárni, hogy ezáltal mások jogai ne sérülhessenek, azaz más személyre vonatkozó személyes, vagy védett adatokat ki kell takarni vagy más módon megismerhetetlenné tenni.

19.7. A közgyűlés és a bizottságok üléseiről készült testületi jegyzőkönyvek közül a zárt ülések jegyzőkönyveit és az azokról készült hangfelvételeket elkülönítetten, zártan kell kezelni, betekintésre csak a zárt ülésen részvételi joggal rendelkező személyek jogosultak. A közgyűlési és bizottsági előterjesztések, jegyzőkönyvek megőrzéséről a Szervezési Osztály kijelölt munkatársa útján - az Iratkezelési Szabályzatnak megfelelően - a megyei jegyző gondoskodik.

19.8. Az iratokat munkaidőn túl - és amelyeket lehetséges munkaidőben is – zárt irodabútorban, vagy szekrényben kell tartani, az asztalon és az irodában egyéb helyen hivatalos iratok csak a munkavégzés céljából és annak tartama alatt tárolhatók.

19.9. A számítógépes és az ahhoz alkalmazott adathordozókat úgy kell kezelni, tárolni, hogy a védelmet igénylő adatokat illetéktelen személy ne ismerhesse meg. A munkaidő végeztével a számítógépet ki kell kapcsolni.

19.10. A számítástechnikai eljárás során keletkezett munkapéldányt, vagy egyéb okból feleslegessé vált példányokat meg kell semmisíteni.

19.11. Az adatkezelő adatszerveréhez távoli hozzáféréssel rendelkező munkatársaknak fokozott gondossággal kell eljárniuk a személyes adatokat is tartalmazó iratok használatakor. Az adatszerverhez való hozzáférés befejeztével a rendszerből haladéktalanul ki kell lépni.

19.12. A tűz elleni védekezés rendjét és az elhárítása érdekében szükséges intézkedéseket a Tűzvédelmi Szabályzat tartalmazza.

20. Adatvédelmi incidens

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

20.2. Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést okozhat.

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

20.4. Az érintett személyt késedelem nélkül tájékoztatni kell, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személy jogaira és szabadságára nézve, annak érdekében, hogy megtehesse a szükséges óvintézkedéseket.

21. Ügyviteli és nyilvántartási célú adatkezelés

21.1. A Szervezet a tevékenységéhez tartozó esetekben, illetve ügyviteli és nyilvántartási célból is kezelhet személyes adatokat.

21.2. Az adatkezelés alapjául az érintett személy megfelelő tájékoztatásán alapuló önkéntes és határozott hozzájárulás szolgál. Az a részletes tájékoztatás, amely kiterjed az adatkezelés céljára, jogalapjára és időtartamára, valamint az érintett személy jogaira. Az érintettet figyelmeztetni kell az adatkezelés önkéntes jellegére is. Az adatkezeléshez való hozzájárulást írásban kell rögzíteni.

21.3. Az ügyviteli és nyilvántartási célból történő adatkezelés az alábbi célokat szolgálja:

a) a Szervezet tagjainak, illetve munkavállalóinak adatkezelése, amely jogszabályi kötelezettségen alapul;
b) a szervezettel megbízási jogviszonyban álló személyek adatkezelése kapcsolattartási, elszámolási és nyilvántartási célból;
c) az adatkezelő szervezettel üzleti kapcsolatban álló más szervezetek, intézmények és vállalkozások kapcsolattartói adatai, amelyek természetes személyek elérhetőségi és azonosítási adatai is lehetnek;

21.4. A 21.3. pont szerinti adatkezelés egyrészről jogszabályi kötelezettségen alapul, másrészről pedig ha az érintett személy kifejezetten hozzájárult adatai kezeléséhez (például munkaszerződés céljából vagy weboldalon partnerként regisztrált, stb.).

21.5. Az adatkezelő szervhez írásos formában eljuttatott személyes adatokat is tartalmazó dokumentumok (például önéletrajz, álláskeresési jelentkezés, egyéb beadvány, stb.) esetében az érintett személy hozzájárulását vélelmezni kell. Az ügy lezárulta után további felhasználásra vonatkozó hozzájárulás hiányában az iratokat meg kell semmisíteni. A megsemmisítés tényét jegyzőkönyvben kell rögzíteni.

21.6. Az ügyviteli célú adatkezelés esetében a személyes adatok kizárólag az adott ügy irataiban és a nyilvántartásokban szerepelnek. Ezen adatok kezelése a kezelés alapjául szolgáló irat selejtezéséig tart.

21.7. Az ügyviteli és nyilvántartási célból történő adatkezelést - annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, - évente felül kell vizsgálni, a pontatlan személyes adatokat haladéktalanul törölni kell.

21.8. Az ügyviteli és nyilvántartás célból történő adatkezelés esetében is biztosítani kell a jogszabályoknak való megfelelést,

22. Egyéb célból történő adatkezelés

22.1. Amennyiben az adatkezelő szerv olyan adatkezelést kíván végezni, amely ebben a szabályzatban nem szerepel, előzetesen ezen belső szabályzatát kell megfelelően kiegészíteni, illetve az új adatkezelési célnak megfelelő kiegészítő szabályokat kell kialakítani.

23. Az adatvédelmi hatásvizsgálat lefolytatása és az előzetes konzultáció kezdeményezése

23.1. Az adatgazda abban az esetben végez előzetes hatásvizsgálatot tervezett vagy folyamatban lévő adatkezelésnél, ha az adatkezelés valamely – különösen új technológiákat alkalmazó – típusa, figyelemmel annak jellegére, hatókörére, körülményére és céljaira, valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve vagy, az adatkezelés kockázatának és lényeges körülményének, különösen az adatkezelés technológiájának a megváltoztatása esetén.

23.2. Az adatgazda a kockázatelemzési feladata kapcsán kikérheti a tervezett, illetve megváltozott adatkezelés által érintett személyek véleményét.

23.3. Az adatgazda a kockázatelemzési feladata kapcsán kikéri a döntés végrehajtásáért felelős szakterületnek, az elektronikus információs rendszert üzemeltető szervezetnek és az elektronikus biztonságért felelős személynek (IBF), valamint az adatvédelmi tisztviselőnek a véleményét. Ezt követően megválaszolja kockázatelemzési dokumentációban foglalt kérdéseket.

23.4. Ha a tervezett adatkezelés annak körülményeire, így különösen céljára, az érintettek körére, az adatkezelési műveletek során alkalmazott technológiára tekintettel – az adatkezeléssel várhatóan érintett személyek jogaira és szabadságaira nézve – valószínűsíthetően magas kockázatot nem azonosít, vagy megállapítást nyer, hogy az adatkezelés az adatvédelmi hatásvizsgálat lefolytatása alóli mentesítést tartalmazó valamely jogszabályban meghatározott kivételi körbe tartozik, úgy ennek tényét az adatgazda írásban rögzíti.

23.5. Az adatgazda köteles az előkészített adatkezelés esetén az adatkezelési tevékenységek nyilvántartásról szóló dokumentumot, és az adatbiztonsági és a felelősségi körökre vonatkozó adatlapot kitölteni, és azt az adatvédelmi tisztviselőnek megküldeni. Az adatvédelmi tisztviselő a megküldött dokumentumokat az adatkezelési tevékenységek nyilvántartásába bejegyzi.

23.6. Amennyiben az adatgazda az adatkezeléssel várhatóan érintett személyek jogaira és szabadságaira nézve magas kockázatot azonosít vagy jogszabályi rendelkezés alapján adatvédelmi hatásvizsgálattal kötelezően vizsgálandó adatkezelési tevékenységek esete áll fenn – a döntése alapjául szolgáló legfontosabb szempontokat írásban megjelölve – adatvédelmi hatásvizsgálat lefolytatását kezdeményezi az adatkezelő szerv vezetőjénél.

23.7. Az adatkezelő szerv vezetője az adatgazda javaslatára elrendeli az adatvédelmi hatásvizsgálat lefolytatását vagy írásban rögzíti mellőzésének okait, és az adatvédelmi tisztviselő kapcsolódó álláspontját. Az adatvédelmi hatásvizsgálat lefolytatásáig, vagy az annak elmaradásával kapcsolatos okok írásban történő rögzítéséig az adatkezelésről szóló döntés nem hozható meg.

23.8. Az adatvédelmi hatásvizsgálat lefolytatásában az adatkezelő szerv vezetője által meghatározott szakterületek részéről kijelölt személyek vesznek részt. Az adatvédelmi hatásvizsgálat lefolytatását az adatvédelmi tisztviselő támogatja. Az adatvédelmi hatásvizsgálat során keletkezett iratok az adatkezelő szerv döntését előkészítő adatokat tartalmaznak, ezért azokon „Nem nyilvános!" jelzést kell elhelyezni.

23.9. Az adatgazda és a kijelölt személyek az adatvédelmi hatásvizsgálat eredményeiről, „Nem nyilvános!" jelzéssel ellátott összefoglaló jelentést készítenek.

23.10. Az adatvédelmi hatásvizsgálatról szóló összefoglaló jelentést az adatkezelő szervezeti egység vezetője hagyja jóvá.

23.11. Az adatvédelmi tisztviselő a jelentés alapján az adatkezelést bevezeti az adatkezelési tevékenységek nyilvántartásába.

23.12. Ha az adatvédelmi hatásvizsgálat arra az eredményre jut, hogy a tervezett adatkezelés jelentette kockázat nem mérsékelhető a rendelkezésre álló technológiák és a végrehajtási költségek szempontjából ésszerű módon – vagy azt jogszabály kötelezően előírja –, akkor az adatkezelő szerv előzetes konzultációt kezdeményez a Hatóságnál.

24. Az adatkezelési tevékenységek nyilvántartása

24.1. Az adatkezelő szerv az adatkezelési tevékenységek nyilvántartását papír alapon végzi az adatvédelmi tisztviselő (DPO) felügyeletével és kontrolja alatt álló biztonságos zárható rendszerben. Az adatkezelési tevékenységek nyilvántartását az adatvédelmi tisztviselő vezeti és felel biztonságáért és védelméért. Az adatkezelési tevékenységek nyilvántartásába az adatkezelő szervezeti egység vezetője az alábbi adatokat küldi meg:

a) az előkészített, megváltozott és megszűnt adatkezelések esetén a melléklet szerinti adatokat;

b) hatásvizsgálat elvégzése esetén a melléklet szerinti adatokat;

c) a jogszabályi rendelkezés alapján adatvédelmi hatásvizsgálattal kötelezően vizsgálandó adatkezelési tevékenységek esetében csak abban az esetben szükséges a hatásvizsgálatot megküldeni, ha az adatkezelő az adatkezelő szerv.

24.2. Az adatkezelő szerv központi honlapján közzétett adatkezelési és adatvédelmi tájékoztatókkal kapcsolatban a közzététellel érintett szervezeti egység kikéri az adatvédelmi tisztviselő véleményét.

25. Az adatigénylés és a lekérdezés során irányadó szabályok

25.1. Az adatkezelő szerv szervezeti egységének érintett dolgozója a szerv feladataihoz kapcsolódó egyes eljárások során az országos hatósági nyilvántartásokból vagy más célból kezelt adatbázisokból lekért vagy átvett, de az ügy szempontjából érdektelenné vált, vagy fel nem használt személyes adatok esetében köteles az ügyirat továbbítását, illetőleg irattárba helyezését megelőzően gondoskodni azok dokumentált törléséről, illetve megsemmisítéséről.

25.2. Az olyan elektronikus információs rendszernél, ahol az adatkezelés célja, az adatkezelést folytató személy azonosítása, valamint az adatoknak és az elvégzett műveleteknek a folyamatos és zárt rendszerben történő naplózása nem biztosított, a törvényi előírások teljesítése érdekében más módon – így különösen manuálisan vezetett lekérdezési napló vagy a nyilvántartásból történő lekérdezéshez alkalmazott információs rendszerben történő rögzítéssel – kell gondoskodni az adatkezelési művelet céljának dokumentálásáról.

26. Adattovábbítás

26.1. Az adatkezelő szerv szervezeti egysége az adattovábbítás feltételeinek meglétét minden egyes személyes adattal összefüggésben köteles ellenőrizni, így különösen azt, hogy az igényelt adatokra vonatkozóan az adatok kezelőjének minősül-e.

26.2. Adatvédelmi szempontból akkor tekinthető az adattovábbítás jogszerűnek, ha a személyes adatot kezelő szerv vagy személy jogosult annak továbbítására, az adattovábbítás címzettje (adatkérő) pedig rendelkezik az adat kezeléséhez szükséges jogalappal vagy az érintett írásos – a vonatkozó jogszabályi elvárásoknak megfelelő tartalmú – hozzájárulásával és az adatkérés célja mindezzel összhangban van. Az adattovábbítás feltételeinek megléte és a célhoz kötöttség a jogszerűség együttes követelménye.

26.3. Harmadik személy vagy szerv által benyújtott adattovábbítási kérelem elbírálása – a törvényben kötelezően előírt adattovábbítás esetét kivéve – az adatkezelő szerv vezetőjének vagy az általa kijelölt vezetőnek a hatáskörébe tartozik, amellyel kapcsolatban kikérheti az adatvédelmi tisztviselő véleményét. Az adatigénylés abban az esetben teljesíthető, ha az tartalmazza:

a) az adatigénylés célját, jogalapját;

b) a kért adatok körének pontos meghatározását;

c) az érintett személy azonosításához szükséges adatokat, több személyre vonatkozó adatigénylés esetén az érintettek azonosításához szükséges csoportképző ismérveket.

26.4. Az adattovábbítás történhet kérelem alapján egyedi adatszolgáltatással, illetőleg – törvény ilyen tartalmú rendelkezése vagy erre vonatkozó megállapodás alapján – közvetlen hozzáférés biztosításával.

27. Adattovábbítási nyilvántartás

27.1. Ha olyan adat továbbítására kerül sor, amellyel kapcsolatban az adattovábbítást végző adatkezelő szerv szervezeti egysége – a személyes adat érintettjének a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló Európai Parlament és Tanács 2016/679 számú rendelete (a továbbiakban: GDPR rendelet), vagy az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Infotv.) által biztosított jogait érintő – adatkezelési korlátozást jelzett, az adatkezelési korlátozást szerepeltetni kell az adattovábbítási nyilvántartásban.

27.2. Az olyan elektronikus információs rendszerek esetében, ahol a folyamatos és zárt rendszerben történő naplózás nem biztosított, valamint manuális adatkezelések esetén az adatkezelés célját, az érintett adatokat, illetve az adatkezelést folytató személy azonosítását lehetővé tevő adatokra és az elvégzett műveletekre vonatkozóan papír alapú adattovábbítási nyilvántartás vezetéséről kell gondoskodni.

28. *A közvetlen lekérdezés*

28.1. A közvetlen lekérdezést biztosító rendszert – a lekérdezés és a felhasználás jogszerűségének dokumentálása érdekében – úgy kell kialakítani, hogy:

a) a személyes adatokhoz történő hozzáférés egyedi azonosító és jelszó megadásához kötötten történjen;

b) a lekérdezés naplózása biztosított legyen;

c) a hozzáférésre felhatalmazott munkatárs a lekérdezéskor a rendszer erre a célra kialakított állományában rögzíteni tudja az adatkérés céljára utaló adatot, így különösen az ügyszámot.

IV. ADATVÉDELMI INCIDENSKEZELÉSI ELJÁRÁSREND

29. Az adatvédelmi incidens észlelése

29.1. Az adatkezelő szervnél és az adatfeldolgozónál bekövetkezett adatvédelmi incidens gyanúját észlelő személynek a tájékoztatást az adatgazdához, amennyiben az elektronikus információbiztonság körében következett be, az információbiztonsági felelőshöz (IBF) kell megtenni. A tájékoztatásnak a jogszabályokban előírt, (az incidens azonosítására alkalmas) adatokat kell tartalmaznia.

29.2. Az adatkezelő szerv részére megküldött, külső észlelő személytől származó, az adatkezelő szerv adatkezelésére vagy az adatfeldolgozóra vonatkozó adatvédelmi incidens gyanújának tárgyában érkezett tájékoztatást az adatkezelő szerv tisztviselője haladéktalanul továbbítja a feladat és hatáskörrel rendelkező adatfeldolgozó szervezeti egység vezetőjének, az információbiztonsági felelősnek és az adatvédelmi tisztviselőnek.

29.3. Ha az adatkezelő szerv ellenőrzésre jogosult szervezeti egysége a feladata ellátása során adatvédelmi incidens gyanúját észleli, haladéktalanul értesíti az érintett adatkezelő szervezeti egység vezetőjét, és az információbiztonsági felelőst.

29.4. Az elektronikus információs rendszert üzemeltető szervezet az információbiztonsági felelős véleményének kikérése mellett megvizsgálja, hogy:

d) a tájékoztatás alapján fennáll-e a gyanúja az adatvédelmi incidens bekövetkezésének;

e) az adatvédelmi incidens az informatikai rendszert érintően következett-e be;

f) mely szervezeti egységeket kell bevonni az intézkedések megtételére.

29.5. Az elektronikus információs rendszert üzemeltető szervezet – amennyiben az incidens gyanúja felmerül – a döntés előkészítésére szolgáló anyagot megküldi az adatkezelő szervezeti egység vezetője számára. Ha az adatkezelő szervezeti egység vezetője nem állapítható meg, akkor az üzemeltetést végző szervezet az incidenskezelési eljárásnak megfelelően jár el.

29.6. Ha nem állapítható meg adatvédelmi incidens, de egyéb incidens bekövetkezése igen, akkor a feladat és hatáskört figyelembe véve kerül sor a további eljárás folytatására.

29.7. Az adatgazda vizsgálja a feladat és hatáskörébe tartozó nem informatikai rendszert érintő adatvédelmi incidens gyanújával érintett tájékoztatásokat**.**

30. A tájékoztatás vizsgálata és az adatvédelmi incidens kezelése

30.1. Ha az adatvédelmi incidens a rendelkezésre álló adatok alapján egyértelműen megállapítható az adatgazda a bejelentett adatokat megküldi az adatvédelmi tisztviselőnek, aki 72 órán belül intézkedik a hatósági nyilvántartásba való bejelentésről.

30.2. Ha a rendelkezésre álló adatok alapján az adatgazda egyértelműen nem tudja megállapítani az adatvédelmi incidens bekövetkezését, de feltételezhető, hogy az esemény magas kockázattal járt az adatvédelmi tisztviselő véleményének megkérése mellett haladéktalanul összehívja az alábbi tagokból álló adatvédelmi incidens bizottságot (a továbbiakban: bizottság):

g) adatvédelmi tisztviselő;

h) információ biztonsági felelős;

i) ellenőrzésre jogosult szervezeti egység tagja;

j) érintett adatkezelő (adatgazda) szervezeti egység vezetője;

k) kommunikációért felelős szervezeti egység tagja;

l) informatikai feladatokat biztosító szerződött szervezet vezetője.

30.3. A vizsgálat az adatvédelmi tisztviselő véleményének, szakértői tanácsának kikérésével és annak figyelembevételével történik.

30.4. A bizottság a tájékoztatást megvizsgálja a tájékoztatótól, valamint az adatfeldolgozótól szükség esetén további adatszolgáltatást kér, amelyet az érintettek kötelesek haladéktalanul teljesíteni. A bizottság gondoskodik az elsődleges intézkedések megtételéről. Ha a vizsgálat során a bizottság megállapítja az érintettek jogaival és szabadságaival kapcsolatban a magas kockázat fennállását, akkor az adatokat az adatvédelmi tisztviselő közreműködésével a Hatóság részére 72 órán belül megküldi az erre rendszeresített elektronikus felület igénybevételével.

30.5. Az adatvédelmi incidens bekövetkezése esetén a bizottság döntése alapján adatkezelő szervezet kommunikációs szervezeti egységének tagja tájékoztatja a jogszabályokban meghatározott adatokról az incidenssel érintetteket.

30.6. Az adatvédelmi tisztviselő a bizottság vagy az adatgazda által megküldött adatvédelmi incidens adatait bevezeti adatkezelő szervezet adatvédelmi incidens nyilvántartásba.

V. KÖZÉRDEKŰ ADATOK[1]

VI. OKTATÁS VIZSGÁZTATÁS

31. Követelmények

31.1. Az adatkezelő szerv állományába kerülő személyeket az adatvédelmi tisztviselő – az adatkezelő szerv személyzeti feladatot ellátó szervezeti egységének tájékoztatása alapján – köteles az állományba vételt követő két hónapon belül adatvédelmi oktatásban részesíteni. Az oktatásra kötelezett részére a szükséges jogszabályokat, közjogi intézményszabályozó eszközöket, belső normákat és egyéb segédanyagokat rendelkezésre kell bocsátani, vagy ezek tekintetében az elektronikus hozzáférés lehetőségét és módját ismertetni kell.

31.2. Az oktatást követően 30 napon belül az adatkezelő szervnél foglalkoztatottaknak az adatvédelmi ismeretekből vizsgát kell tenni, amelyről szóló igazolást az érintett személyi iratai mellé kell elhelyezni. Eredménytelen vizsga esetén az érintett személyt megfelelő határidő kitűzésével pótvizsgára kell bocsátani, a pótvizsga sikertelensége esetén a vizsga letételéig személyes adatok kezelésével járó feladatokat nem láthat el. Az adatkezelő szervnél foglalkoztatottak szükség szerint évente, de legalább két évente részt kell venniük az adatvédelmi tisztviselő által szervezett adatvédelmi oktatáson vagy tájékoztatón, melyet aláírásukkal kell igazolniuk.

31.3. Az adatvédelmi tisztviselő az adatkezelő szerv személyes adatok kezelését végző foglalkoztatottaknak a bekövetkezett adatvédelmi tárgyú jogszabály- és normaváltozásokról köteles tájékoztatást adni, indokolt esetben – különösen a jelentősebb adatvédelmi tárgyú normaváltozásoknál vagy az ellenőrzés során feltárt visszatérő, vagy egyébként súlyos hiányosságoknál és súlyos adatvédelmi incidenst követően – az érintett szervezeti egységnél adatvédelmi oktatás kell tartani.

[1] Hatályon kívül helyzete a …/2019. (…) számú jegyzői utasítás.

1. melléklet

Adatkezelési és adatfeldolgozói tevékenységek nyilvántartása

Adatkezelői /adatfeldolgozói tevékenységek nyilvántartásainak felmérési adatlapja	
Az adatkezelés /adatfeldolgozás megnevezése	
Az adatkezelő/ adatfeldolgozó szerv neve és elérhetősége	
A közös adatkezelő és az adatkezelő szervezeti egység megnevezése	
Az adatvédelmi tisztviselő neve és elérhetősége	
Az adatkezelés/adatfeldolgozás célja	
Adatkezelés/adatfeldolgozás jogalapja	
Az érintett személyek köre	
A személyes adatok kategóriái	
A címzettek kategóriái	
Harmadik országba történő adattovábbítás/ harmadik ország vagy nemzetközi szervezet megnevezése	
Az adatkategóriák törlési határideje	
Adatok forrása	
Az adatbiztonsággal összefüggő szervezeti és technikai intézkedések általános leírása	
Adatkezelési tájékoztató van-e? (Ha hozzájárulás a jogalap, feltétlenül szükséges készíteni.)	**<u>Lehetséges válaszok:</u>** 1. Nincs rá szükség, mert jogszabályi tájékoztatás van. 2. Nincs, azonban feltétlenül szükséges lenne.(Indoklás) 3. Igen van.

Elsődleges adattárolási hely (ideértve az adatbiztonsági kockázatokat, javaslatokat is, ha vannak)	Ezen pont kitöltésénél az elektronikus információs rendszert üzemeltető szervezet fog iránymutatást adni.
Vannak-e együtt tárolt adatok?	Igen/Nem.
Célhoz kötöttség elve érvényesül-e? Indoklással, szükség esetén javaslattal!	1. Igen, a jogszabályoknak megfelelően. 2. Nem, vagy csak részben. (Nem válasz esetén indoklás, javaslat szükséges)
Adattakarékosság elve érvényesül-e? Indoklással, szükség esetén javaslattal!	1. Igen, a személyes adatok az adatkezelés céljának megfelelnek, relevánsak, és szükségesek. 2. Nem. (Nem válasz esetén indoklás, javaslat szükséges)
Pontosság elve releváns, érvényesül-e? Indoklással, szükség esetén javaslattal!	1. Igen, a személyes adatok pontosak, naprakészek. 2. Nem. (Nem válasz esetén indoklás, javaslat szükséges)
Korlátozott tárolhatóság elve érvényesül-e? Indoklással, szükség esetén javaslattal!	1. Igen, a személyes adatok kezelésére csak a cél eléréséhez szükséges ideig kerül sor, amelyet jogszabály állapít meg. 2. Igen, a személyes adatok kezelésére csak a cél eléréséhez szükséges ideig kerül sor, amelyet az adatkezelő határoz meg (Hozzájárulás esetén) 3. A személyes adatok kezelésére közérdekű archiválás, tudományos és történelmi kutatás vagy statisztikai célból az eredeti adatkezelési céltól eltérő ideig kerül sor. (az első kettővel is alkalmazható) 4. Nem. (Nem válasz esetén indoklás, javaslat szükséges)
Adatbiztonság elve érvényesül-e? Indoklással, szükség esetén javaslattal!	1. Igen, a személyes adatok megfelelő biztonsága biztosított. 2. Nem. (Nem válasz esetén indoklás, javaslat szükséges)
Tájékoztatás megfelelő, tartalmazza valamennyi kötelező elemet? Indoklással, szükség esetén javaslattal!	1. A tájékoztatás a törvényi előírásnak megfelelő. 2. Az adatkezelés hozzájáruláson alapul. A tájékoztatás megfelelő. 3. Az adatkezelés nem az érintett hozzájárulásán alapul. A tájékoztatás megfelelő. 4. Az adatkezelés……alapul, tájékoztatás nincs/nem megfelelő. (Nem válasz esetén indoklás, javaslat szükséges)
Törlés, elfeledtetés joga gyakorolható-e? Indoklással, szükség esetén javaslattal!	Ezek a jogok nem gyakorolhatók, ha a jogalap jogi kötelezettség teljesítése, vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlás keretében végzett feladat végrehajtása. 1. Igen gyakorolható. 2. Nem. (Nem válasz esetén indoklás, javaslat szükséges)

Korlátozás joga gyakorolható-e? Indoklással, szükség esetén javaslattal!	Az érintett ezzel a jogával a kötelező, és a hozzájáruláson alapuló adatkezelések esetében is élhet. A *kötelező* esetében csak akkor, ha az adatok pontosságát vitatja, a GDPR rendeletben szereplő felsorolás többi pontja szerint nem. 1. Igen. 2. Igen, de mivel az adatkezelés jogalapja jogszabályon alapul, csak az adatok pontosságát vitahatja. 3. Nem. (Nem válasz esetén indoklás, javaslat szükséges)
Adathordozhatóság joga gyakorolható-e? Indoklással, szükség esetén javaslattal!	Csak a hozzájáruláson, vagy szerződésen alapuló adatkezelések esetén alkalmazható. További feltétel, hogy az adatkezelés automatizált módon történjen. Nem alkalmazható a közérdekű, és a közhatalmi feladatok keretében végzett adatkezeléseknél! **1.** Igen. **2.** Nem. (Nem válasz esetén indoklás, javaslat szükséges)
Tiltakozás joga gyakorolható-e? Indoklással, szükség esetén javaslattal!	Az érintett csak kivételes esetben! a közérdekű és a közhatalmi feladatok keretében végzett adatkezelések, és a jogos érdeken alapuló adatkezelések esetén élhet ezzel a joggal. (6. cikk (1) e. és f. pont) 1. Igen, mert a jogalap……. 2. Nem. (Nem válasz esetén indoklás, javaslat szükséges)
Van-e adatfeldolgozási megállapodás az adatfeldolgozóval?	

Gyakorlati útmutató:

1. **Az adatkezelés megnevezése:** A nyilvántartásban történő keresés lehetővé tétele céljából - röviden kell megnevezni. A nyilvántartásnak az adatkezelést létrehozó törvény által meghatározott elnevezését kell megjelölni, amennyiben azonban rendelkezik egy általánosan használt fantázianévvel, akkor ezt az elnevezést is fel kell tüntetni. Az azonos adattartalommal rendelkező adatkezeléseket egységes elnevezéssel kell szerepeltetni.
2. Az adatkezelő nevét, címét, székhelyét, telefonszámát, e-mail címét kell beírni.
3. Csak akkor kell kitölteni, ha van közös adatkezelő, illetve van az adatkezelőnek képviselője.
4. Az adatkezelés céljának rövid megfogalmazása.
5. **Hozzájárulás** vagy **GDPR rendelet 6. cikk (1) bekezdésében** foglalt jogalapok valamelyike.
   Pontosan meg kell jelölni a fentieken kívül azt is, hogy **milyen jogszabály (**jogszabályi helyet is kérjük feltüntetni!) által meghatározott feladat teljesítése érdekében van erre szükség. Ilyen esetben a feladat meghatározást tartalmazó ágazati jogszabály megfelelő hivatkozási alapnak tekinthető.
6. **Az érintettek kategóriái lehetnek**: azon csoportok, amelyek tagjainak személyes adataival az adatkezelő szerv adatkezelést végez. Pl. az adatkezeléssel érintett személyek/nagykorú állampolgárok/gyermekek, egyéni vállalkozók, gépjármű üzemben tartói stb.
7. Például: személyes adat, különleges adat, bűnügyi személyes adat, nemzeti adatvagyon, minősített adat.
8. **Címzettek:** akikkel a személyes adatot közölték, vagy közölni fogják, ideértve a harmadik országbeli címzetteket, vagy nemzetközi szervezeteket.
9. **Harmadik ország:** minden olyan ország, ami nem EU és EGT tag.
10. Ha jogszabály másképp nem rendelkezik, az adatokat az adatkezelés céljának elérésével, illetve az érintett kérésére törölni kell.
11. A kezelt adatok forrásának megjelölése (pl. érintett, más adatkezelőtől adatátvétellel).
    Más adatkezelőtől történő adatátvétel esetén az adatokat továbbító adatkezelő adatvédelmi nyilvántartási számát is meg kell jelölni.
12. Lásd GDPR rendelet 32. cikk (1) bekezdés.
13. Ha az adatkezelés a NAIH részére már bejelentésre került.

2. melléklet

Kérdőív az előzetes kockázatelemzéshez

Első rész: Szükséges-e a hatásvizsgálat lefolytatása?
(Előzetes adatvédelmi kockázatelemzés)

1. Használ vagy fejleszt-e olyan adatkezelő rendszert, amely személyes adatokat kezel?
Igen □ Nem □
2. Szükséges-e személyes adatokat gyűjteni a szolgáltatás működtetéséhez?
Igen □ Nem □
3. Megvalósul-e a korábbiaktól eltérő célú adatkezelés már meglévő személyes adatokkal kapcsolatban?
Igen □ Nem □
a) Alkalmaz új adatköröket gyűjtő technológiát, amely jelentős mértékben megváltoztatja az adatkezelést?
Igen □ Nem □
b) Ha releváns szervezeti változás következik be:
- az egyesülés, beolvadás vagy egyéb szervezeti átalakulás hatással van-e az adatbázisokra?
  Igen □ Nem □
- ez a változás eredményezi új adatok kezelését vagy új nyilvánosságra hozatali eljárásokat?
  Igen □ Nem □

c) Ha ez az információ már korábban be lett gyűjtve:
- érint-e új vagy nagy létszámú érintett csoportot?
  Igen □ Nem □
- rögzít-e ezen felül további személyes adatot?
  Igen □ Nem □

4. A szolgáltatás korlátozza-e az érintettek személyes adataikhoz való hozzáféréséhez fűződő jogait?
Igen □ Nem □
5. Tervezi-e egymást követő 12 hónapból álló időszak során nagyszámú érintettekre vonatkozó személyes adatainak kezelését?
Igen □ Nem □
6. Megvalósul-e különleges adatok, tartózkodási helyre utaló adatok, illetve gyermekekre vagy munkavállalókra vonatkozó, széleskörű nyilvántartási rendszerekben tárolt adatok kezelése?
Igen □ Nem □
7. Megvalósul-e profilalkotás, amelyre az érintett személy tekintetében joghatással bíró vagy az egyént hasonlóan jelentős mértékben érintő intézkedések épülnek?
Igen □ Nem □
8. Megvalósul-e egészségügyi ellátás nyújtására, járványügyi kutatásokra, mentális vagy fertőző betegségekre irányuló felmérésekre vonatkozó személyes adatok kezelése, amennyiben az adatok feldolgozására meghatározott egyénekre széles körben vonatkozó intézkedések vagy döntések meghozatala érdekében kerül sor?
Igen □ Nem □
9. Megvalósul-e nyilvánosság számára hozzáférhető területek (közterületek) nagyarányú, automatizált nyomon követése?
Igen □ Nem □
10. Megvalósul-e olyan adatkezelés, amely során a személyes adatok megsértése várhatóan hátrányosan érintené az érintett személyes adatainak, magánéletének, jogainak vagy jogos érdekeinek védelmét?
Igen □ Nem □

11. Az adatkezelő vagy adatfeldolgozó fő tevékenységei olyan eljárásokat foglalnak-e magukban, amelyek jellegüknél, alkalmazási területüknél, illetve céljaiknál fogva az érintettek rendszeres és rendszerszerű megfigyelését igénylik?
Igen □ Nem □
12. A személyes adatokat olyan jelentős számú személy számára teszi-e hozzáférhetővé, amely észszerűen elvárható módon nem korlátozható?
Igen □ Nem □
13. Létrejön-e új azonosító vagy hozzáférési jogosultságot ellenőrző rendszer, például biometrikus azonosítás?
Igen □ Nem □
14. Megfigyelés alatt állnak-e az érintettek helyváltoztatás, másokkal való kommunikáció vagy egyéb magatartás tanúsítása közben?
Igen □ Nem □
15. Megvalósul-e automatizált adatfeldolgozás?
Igen □ Nem □
16. Személyes adatok védelmének növelése érdekében előír-e (ha volt ilyen) a korábbinál magasabb szintű adatbiztonsági követelményeket?
Igen □ Nem □
17. Személyes adatokkal való visszaélés megelőzése érdekében bevezetésre kerülnek-e új vagy módosított előírások?
Igen □ Nem □
18. Személyes adatok tárolásával kapcsolatban bevezetésre kerülnek-e új vagy módosított előírások?
Igen □ Nem □
19. Megvalósul-e tudományos kutatási vagy statisztikai célból történő adatkezelés?
Igen □ Nem □
20. Az adatkezelés kiterjed-e különleges adatokra?
Igen □ Nem □
21. Megvalósul-e bármilyen más, magánszférát érintő magatartás?
Igen □ Nem □
22. Végeztek-e már korábban hatásvizsgálatot? Ha a válasz igen, csatolja a dokumentumot!
Igen □ Nem □

Második rész: hatásvizsgálat

Hatásvizsgálat lefolytatásához szükséges adatszolgáltatás	
I. Általános adatok	
1. Az adatkezelés rövid bemutatása	Mutassa be röviden az adatkezelést, ennek körében ismertesse különösen a személyes adatok kezelésének célját, jogalapját, a kezelt személyes adatok körét és az adatkezelés egyéb lényeges körülményeit.
2. Az adatkezeléshez kapcsolódó felelősségi viszonyok bemutatása	Ismertesse az adatkezelésben közreműködő felek – az adatkezelő, az esetleges adatfeldolgozók és a közös adatkezelők – egymáshoz való viszonyát az adatkezelésért való felelősség viselésének szempontjából.
3. Rendelkezik-e az adatkezelésre alkalmazandó valamilyen szabályzattal?	Sorolja fel az adatkezelésre vonatkozó szabályzatokat, jóváhagyott magatartási kódexeket és adatvédelmi tanúsítványokat, amennyiben ilyennel rendelkezik.
4. A kezelt személyes adatok köre	Sorolja fel a gyűjtött és kezelt adatokat. Egyenként határozza meg a tárolás időtartamát, a címzetteket és azokat a személyeket, akik az adatokhoz hozzáférnek.
5. Az adatkezelési folyamatok bemutatása	Mutassa be az adatkezelés folyamatát (az adatgyűjtéstől az adatok megsemmisítéséig, az adatkezelés különböző szakaszait, a tárolást stb.), használjon például a személyes adatok útját - adatfolyamot - bemutató ábrát (melyet mellékletként csatolhat).
6. Melyek a személyes adatok kezelésére szolgáló eszközök?	Sorolja fel a személyes adatok kezelésére szolgáló eszközöket (operációs rendszerek, alkalmazások, adatbázis-kezelő rendszerek, helyiségek, egyéb eszközök stb.)
II.Alapelvek *Ez a rész az adatvédelmi elveknek való megfelelés kereteinek bemutatására szolgál.*	
7. ARÁNYOSSÁG ÉS SZÜKSÉGESSÉG	Ez a rész az érintettek jogérvényesítésének biztosítása érdekében alkalmazott eszközök ismertetését tartalmazza.
7.1 Az adatkezelés céljai meghatározottak-e, egyértelműek-e és jogszerűek-e?	Fejtse ki, hogy mitől meghatározottak, egyértelműek és jogszerűek az adatkezelés céljai.
7.2 Mi az adatkezelés jogalapja?	Ismertesse az adatkezelés jogalapját (hozzájárulás, szerződés teljesítése, jogi kötelezettség teljesítése, létfontosságú érdekek védelme stb.)
7.3 A gyűjtött adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak-e, valamint a szükségesre korlátozódnak-e (adattakarékosság)?	Mutassa be, hogy az egyes gyűjtött adatok miért szükségesek az adatkezelés céljára.
7.4 Pontosak-e az adatok, naprakész állapotban tartják-e azokat?	Ismertesse az adatminőséget biztosító intézkedéseket.
7.5 Mi az adatmegőrzés időtartama?	Mutassa be, hogy milyen jogi követelmények és/vagy adatkezelési szükségletek indokolják a tárolás időtartamát.

8. AZ ÉRINTETTEK JOGAINAK BIZTOSÍTÁSÁRA SZOLGÁLÓ INTÉZKEDÉSEK	Ez a rész az érintettek jogérvényesítésének biztosítása érdekében alkalmazott eszközök ismertetését tartalmazza.
8.1 Milyen módon tájékoztatják az érintetteket az adatkezelésről?	Ismertesse az érintetteknek adott tájékoztatást és annak módját.
8.2 Amennyiben az adatkezelés hozzájáruláson alapul, milyen módon szerzik be az érintettek hozzájárulását?	Mutassa be az annak biztosítására szolgáló eljárásokat, hogy az érintettek hozzájárulásának beszerzése megtörténik.
8.3 Milyen módon érvényesíthetik az érintettek a hozzáférési, illetve az adathordozhatósághoz való jogukat?	Ismertesse azokat az intézkedéseket, amelyek biztosítják, hogy az érintettek hozzáférhessenek az adataikhoz, megkapják és továbbíthassák azokat.
8.4 Hogyan gyakorolhatják az érintettek a helyesbítéshez és törléshez való jogukat?	Ismertesse azokat az intézkedéseket, amelyek biztosítják, hogy az érintettek helyesbíttethessék és töröltethessék adataikat.
8.5 Hogyan gyakorolhatják az érintettek az adatkezelés korlátozásához, valamint tiltakozáshoz való jogukat?	Ismertesse azokat az intézkedéseket, amelyek biztosítják, hogy az érintettek kérhessék az adatkezelés korlátozását, illetve tiltakozhassanak személyes adataik kezelése ellen.
8.6 Az adatfeldolgozók kötelezettségeit egyértelműen rögzíti-e az adatfeldolgozási szerződés?	Ismertesse az egyes adatfeldolgozók kötelezettségeit (időtartam, hatáskör, célok, dokumentált utasítások a feldolgozóknak stb.), illetve jelölje meg azok feladatait és kötelezettségeit meghatározó szerződéseket, magatartási kódexeket és tanúsítványokat.
8.7 Az Európai Unión kívülre történő adattovábbítás esetén megfelelő védelemben részesülnek-e a személyes adatok?	Nevezze meg mindazokat az Európai Unión kívüli országokat, amelyekben adatkezelés és -tárolás történik, továbbá jelölje meg, hogy azok megfelelő védelmi szintet biztosítanak -e (más esetben is írja le az adattovábbításra vonatkozó rendelkezéseket)
III.Kockázatok *Végezze el az adatkezelés kockázatainak felmérését a meglévő vagy tervezett intézkedések figyelembevételével.*	
9. TERVEZETT VAGY MEGLÉVŐ INTÉZKEDÉSEK	Ez a rész tartalmazza azon meglévő vagy tervezett intézkedéseket, amelyek hozzájárulnak az adatbiztonság megteremtéséhez.
10. AZ ADATOKHOZ VALÓ JOGOSULATLAN HOZZÁFÉRÉS	Milyen főbb következményekkel járna az érintettekre, ha a kockázat bekövetkezne?
10.1Milyen főbb következményekkel járna az érintettekre, ha a kockázat bekövetkezne?	Sorolja fel a lehetséges következményeket.
10.2Mely fő fenyegető veszélyek idézhetik elő a kockázatot?	Sorolja fel a fenyegető veszélyeket.

10.3Melyek a kockázat forrásai?	Sorolja fel a kockázatok forrásait.
10.4A megadott intézkedések közül melyek szolgálnak a kockázat kezelésére?	Sorolja fel a kockázatkezelő intézkedéseket.
10.5Hogyan becsüli meg a kockázat súlyosságát, különösen a lehetséges következményekre és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?	Lehetséges válaszok: Elhanyagolható; Korlátozott; Jelentős; Maximális
10.6Hogyan becsüli meg a kockázat valószínűségét, különösen a fenyegető veszélyekre, a kockázatforrásokra és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?	Lehetséges válaszok: Elhanyagolható; Korlátozott; Jelentős; Maximális
11. AZ ADATOK VÉLETLEN VAGY JOGELLENES MEGVÁLTOZTATÁSA	Elemezze a nem kívánt adatmódosítás okait és következményeit, becsülje meg a súlyosságát és valószínűségét.
11.1Milyen főbb következményekkel járna az érintettekre, ha a kockázat bekövetkezne?	Sorolja fel a lehetséges következményeket.
11.2 Milyen fő fenyegető veszélyek idézhetik elő a kockázatot?	Sorolja fel a fenyegető veszélyeket.
11.3 Melyek a kockázat forrásai?	Sorolja fel a kockázatok forrásait.
11.4A megadott intézkedések közül melyek megfelelőek a kockázatok kezelésére?	Sorolja fel a kockázatkezelő intézkedéseket.
11.5Hogyan becsüli meg a kockázat súlyosságát, különösen a lehetséges következményekre és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?	Lehetséges válaszok: Elhanyagolható; Korlátozott; Jelentős; Maximális

11.6Hogyan becsüli meg a kockázat valószínűségét, különösen a fenyegető veszélyekre, a kockázatforrásokra és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?	Lehetséges válaszok: Elhanyagolható; Korlátozott; Jelentős; Maximális
12. ADATVESZTÉS	Elemezze az adatvesztés okait és következményeit, becsülje meg a súlyosságát és valószínűségét.
12.1Milyen főbb következményekkel járna az érintettekre, ha a kockázat bekövetkezne?	Sorolja fel a lehetséges következményeket.
12.2Milyen fő fenyegető veszélyek idézhetik elő a kockázatot?	Sorolja fel a fenyegető veszélyeket.
12.3Melyek a kockázat forrásai?	Sorolja fel a kockázatok forrásait.
12.4A megadott intézkedések közül melyek szolgálnak a kockázat kezelésére?	Sorolja fel az intézkedéseket.
12.5Hogyan becsüli meg a kockázat súlyosságát, különösen a lehetséges következményekre és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?	Lehetséges válaszok: Elhanyagolható; Korlátozott; Jelentős; Maximális
12.6Hogyan becsüli meg akockázat valószínűségét, különösen a fenyegető veszélyekre, a kockázatforrásokra és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?	Lehetséges válaszok: Elhanyagolható; Korlátozott; Jelentős; Maximális
12.7A kockázatok áttekintése	Alkosson teljes és összefoglaló képet arról, hogy a kockázatok kezelését célzó intézkedések milyen hatást fejtenek ki az általuk célzott kockázatokra.
13. JÓVÁHAGYÁS	Ez a rész tartalmazza az adatvédelmi hatásvizsgálat jóváhagyásának előkészítő lépéseit.
13.1A kockázatok feltérképezése	Össze kell vetni a kockázatok elhelyezkedését egymás közt, a védelmi intézkedések alkalmazása előtt és után.
13.2Intézkedési terv készítése	Az intézkedési terv létrehozása előtt át kell tekinteni a vizsgálat eredményét.
13.3Adatvédelmi tisztviselő szakmai tanácsa.	Az adatvédelmi tisztviselőnek át kell tekintenie a vizsgálat eredményét.

3. melléklet
(adatkezelő szerv megnevezése)

A személyes adatokat kezelő nyilvántartások adatbiztonsági felmérése

A felmérés fókuszában a GDPR rendelet szerinti személyes adatokat kezelő nyilvántartások felmérésével és a hatásvizsgálat elvégzésével összefüggésben a magas kockázatú adatkezelés megállapítása áll, a 29. cikk alapján létrehozott adatvédelmi munkacsoport (17/HU WP 248 rev.01) iránymutatásai alapján.

A személyes adatokat kezelő nyilvántartások adatbiztonsági felmérésének súlyponti kérdései a nyilvántartások bizalmassága sértetlensége és rendelkezésre állása oly módon, hogy a felmérés eredményei alapján megállapítható legyen, hogy az adatkezelés a GDPR rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e, valamint a kockázatok kezelését célzó alkalmazott védelmi intézkedések és mechanizmusok(szervezeti intézkedések) biztosítják e az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat.

A felmérés során számba kell venni, hogy az „adatkezelések” során milyen személyi, adminisztratív, fizikai és elektronikus biztonsági intézkedéseket alkalmaznak az adatbiztonsági kockázatok csökkentése érdekében:

……
……
……
……
……
……
…….

Készült: 201…….- n a *(adatkezelő szerv megnevezése)* hivatalos helyiségében.

Jelen vannak:

…….
adatkezelő szervezeti egység vezetője,

……...……..……
felmérést végző bizottság tagja,

…….
felmérést végző bizottság tagja.

4. melléklet

Bejelentő lap az adatkezelő részére adatvédelmi incidens esetén

1. Az adatvédelmi incidenst bejelentő Tájékoztató adatai:

Név:……
E-mail cím:…….
Cím:……
Telefonszám:……..

Kapcsolattartó megnevezése, elérhetősége (telefonszám, e-mail):
……
……
…….

1.1. Az adatkezelőn kívüli felek részvétele az adatvédelmi incidenssel érintett szolgáltatásban.

1.2. Részt vesz-e az adatkezelőn kívül más az adatvédelmi incidenssel érintett szolgáltatásban:……
……
…….

1.3.Az adatkezelőn kívüli fél megnevezése és minősége:
……
……
…….

2. Az adatvédelmi incidenssel kapcsolatos időpontok:

Kezdő időpont:……...

Záró időpont:…….

Az adatvédelmi incidens továbbra is fennáll:……..

Az incidensről való tudomásszerzés időpontja:……..

Az incidens észlelésének módja:…….

Az adatfeldolgozó általi értesítés időpontja:…….

A késedelmes tájékoztatás indokai:
……
……
……
……
…….

Egyéb megjegyzések az incidens időpontját illetően:
……
……
……
……
…….

3. Az adatvédelmi incidens adatai (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

3.1.Sérülés jellege:

- bizalmas jelleg:
- integritás:
- rendelkezésre állás:

3.2.Az adatvédelmi incidens jellege (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

- eszköz elvesztése vagy ellopása:
- informatikai rendszer feltörése (hackelés):
- papír alapú dokumentum nem megfelelő módon történő megsemmisítése:
- papír alapú dokumentum elvesztése, ellopása vagy olyan helyen hagyása, amely nem minősül biztonságosnak
- rosszindulatú számítógépes programok pl. zsarolóprogram
- elektronikus hulladék (a személyes adatok rajta maradnak az elavult eszközön):
- személyes adatok téves címzett részére történő küldése:
- levél elvesztése vagy jogosulatlan felnyitása
- adathalászat
- személyes adatok nagy nyilvánosság előtti jogellenes közzététele
- személyes adatok jogosulatlan szóbeli közlése
- egyéb:……..……
  ……
  ……

4. <u>Az adatvédelmi incidens okai (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):</u>

- szervezeten belüli, rosszhiszeműnek nem minősülő cselekmény (belső szabályzat megsértése által):
- szervezeten belüli, rosszhiszemű cselekmény:
- külső, rosszhiszeműnek nem minősülő cselekmény:
- külső, rosszhiszemű cselekmény:
- egyéb:……..……
  ……..……
  ……
  …….

<u>Az adatvédelmi incidenssel érintett személyes adatok köre:</u>

4.1.Személyes adatok (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

- személyazonossághoz kapcsolódó adatok:
- elérhetőségi adatok:
- azonosító adatok:
- személyi szám:
- hivatalos okmányok:

- helymeghatározó adatok:
- gazdasági, pénzügyi adatok:
- büntetett előélettel, bűncselekményekkel vagy büntetéssel, intézkedéssel kapcsolatos adatok:
- különleges adatok:

4.2. Különleges adatok (legalább egy kiválasztása kötelező):

- faji eredetre, nemzetiséghez tartozásra vonatkozó adatok:
- politikai véleményre vonatkozó adatok:
- vallásos vagy más világnézeti meggyőződésre vonatkozó adatok:
- érdek-képviseleti szervezeti tagságra vonatkozó adatok:
- szexuális életre vonatkozó adatok:
- egészségügyi adatok:
- genetikai adatok:
- biometrikus adatok:
- még nem ismert:
- egyéb:……..……
  ……
  ……-

4.3.Az adatvédelmi incidenssel érintett személyes adatok becsült száma:…….

5. Az érintettek jellege (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):
   - alkalmazottak:
   - felhasználók:
   - feliratkozók:
   - diákok:
   - katonai állomány tagjai:
   - ügyfelek (jelenlegi és potenciális):
   - páciensek:
   - kiskorúak:
   - kiszolgáltatott személyek:
   - hatósági eljárás vagy intézkedés alá vont, vagy azok által érintett személyek:
   - még nem ismert:
   - egyéb:……
     ……
     …….

5.1.Az incidenssel érintett adatalanyok részletes leírása (pl. adatbázisokban szereplő munkavállalók leírása):

……
……
…….

5.2. Az adatvédelmi incidenssel érintettek becsült száma:…….

6. Az incidens előtt alkalmazott intézkedések leírása (pl. tűzfal, vírusellenőrzés, adatszivárgás elleni védelmi rendszer) :
……
……
……
……

7. Következmények:

8.1. Bizalmas jelleg sérülése (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

- Szélesebb körű hozzáférés, mint ami szükséges, vagy amihez az érintett hozzájárult:
- Az adat összekapcsolhatóvá vált az érintett egyéb adatával:
- Az adatot más célokból történő, tisztességtelen módon történő kezelése lehetséges:
- egyéb:……
……..…..…
…….

8.2. Integritás sérülése: (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket)

- Az adat módosíthatóvá vált annak ellenére, hogy archivált vagy elavult volt:
- Az adatot valószínűsíthetően módosították egyébként pontos adatokra, és azokat eltérő célokra használhatták:
- egyéb:…….……
……
…….....
.....

8.3 Rendelkezésre állás sérülése: (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket)

- Az érintettek számára történő kritikus szolgáltatásnyújtás képességének módosulása:
- egyéb:……
……..……
……
……
…….

8.4. Az érintetteket ért fizikai, anyagi vagy nem vagyoni károk, vagy egyéb jelentős következmények:
……
……
……
……..

8.5. Az incidens valószínűsíthető hatásai az érintettekre (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket):

- személyes adatok feletti rendelkezés elvesztése:
- érintett jogainak korlátozása:
- hátrányos megkülönböztetés:
- személyazonosság-lopás:
- személyazonossággal való visszaélés:
- pénzügyi veszteség:

- álnevesítés engedély nélküli feloldása:
- jó hírnév sérelme:
- szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülése:
- egyéb:……
  ……..……
  ……..

8.6. A valószínűsíthető következmények súlyossága: (kérem, húzza alá a megfelelő választ, amennyiben szükséges fejtse ki a részleteket)

- elhanyagolható:
- korlátozott:
- jelentős:
- maximális:

8. Az incidens orvoslására megtett intézkedések:

8.1. Megtett intézkedések (az adatvédelmi tisztviselő vagy a bizottság tölti ki)

9. Egyéb:

……
……
……
……
……
……

10. Egyéb bejelentések:

……
……
……

Más hatóságoknak (EU tagállami) vagy tagállamnak bejelentette-e az adatvédelmi incidenst?

.....
.....
.....

5. melléklet

Az érintett tájékoztatása az adatvédelmi incidensről
(GDPR 34. cikk)

1. Az adatvédelmi incidens időpontja:……..
2. Jellege:

   ……
   ……
   ……
   ……
   ……
   ……
   ……

3. Az adatvédelmi tisztviselő /kapcsolattartó neve:

   ……
   Elérhetősége: …….

4. Az adatvédelmi incidensből eredő valószínűsíthető következmény(ek):

   ……
   ……
   ……
   ……
   ……
   ……
   ……

5. Az adatvédelmi incidens kezelésével kapcsolatban tervezett, illetve megtett intézkedések (ide értve a hátrányos következmények enyhítését célzó intézkedéseket):

……
……
……
……
……
……
……
……

6. Az érintett számára javasolt intézkedések megtétele a bekövetkezett kár enyhítése érdekében……..

   ……
   ……
   ……
   ……
   ……
   ……
   ……

6. melléklet

Az adatvédelmi incidensek nyilvántartása és bejelentése
(GDPR 33. cikk)

1. **Az Adatkezelő (Bejelentő adatai):**

Név:……
Ország:…….
Irányítószám és hely:
……..
Utca neve és száma:
…….

2. Az adatvédelmi tisztviselő /kapcsolattartó neve:
……
Elérhetősége: …….

3. Az Incidens időpontja

Kezdete:…….
Tudomásra jutás időpontja
…….

4. Az incidens jellege

Az Incidens leírása (nem jár kockázattal, kockázattal jár, magas kockázattal jár):
……
……
……

5. Az incidensben érintett adatok

Az adatok kategóriáinak leírása (különleges, bűnügyi adatok kiemelése):
……
……
……

7. Az incidensben érintett személyek kategóriái

Az érintettek csoportjának leírása:
……
……
……

7. A megelőzésre tett védelmi intézkedések

Az incidens megelőzésére tett védelmi intézkedések rögzítése:
……
……
……
……

8. Az incidens következményei

Az érintettre gyakorolt bekövetkezett hatások leírása (fizikai, vagyoni, nem vagyoni):
……
……
……
…….....

9. Az Incidens valószínűsíthető következményei

Az érintettre gyakorolt lehetséges hatások leírása. (fizikai, vagyoni, nem vagyoni):
……
……
……
……

10. Megtett intézkedések

A megtett védelmi intézkedések leírása:
……..……
……
……
……

Az érintettek tájékoztatása (tájékoztatás ideje, tartalma, érintetteknek javasolt intézkedések):
……..
……..
……..

Egyéb:
……
……
……

7. melléklet[2]
8. melléklet[3]

[2] Hatályon kívül helyezet a …/2019. (…) jegyzői utasítás.
[3] Hatályon kívül helyezet a …/2019. (…) jegyzői utasítás.