Bükki Nemzeti Park Igazgatóság
3304 Eger, Sánc utca 6. - Levélcím: 3301 Eger, Pf.: 116.
Ig. közv.: (36) 422-700
Tel.: (36) 411-581
Fax: (36) 412-791
E-mail: titkarsag@bnpi.hu
Honlap: www.bnpi.hu

Igazgatóhelyettesek,
Osztályvezetők
Tájegységvezetők

Tárgy: adatvédelmi intézkedési terv

Üisz: 3621/1/2020.
Üint: dr. Barta Levente
Mell: 4 db (nyilvántartás, tájékoztató, hatás-vizsgálat, incidensbejelentés)

3621/1/2020. (X. 30.) számú igazgatói utasítás
adatvédelmi intézkedések megtételéről

Bevezető rendelkezések, az utasítás hatálya, alapelvek

1. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (a továbbiakban: Info. tv.), valamint a AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről, általános adatvédelmi rendelet, a továbbiakban: GDPR) rendelkezéseinek történő megfelelés céljából a Bükki Nemzeti Park Igazgatóságon (a továbbiakban: Igazgatóság) a következő intézkedések megtételét rendelem el.

2. Jelen utasítás kormánytisztviselőkkel, munkavállalókkal történő megismertetése az osztályvezetők, tájegységvezetők feladata. Az utasítás személyi hatálya az Igazgatóságon dolgozó kormánytisztviselőkre, munkavállalókra egyaránt kiterjed (a továbbiakban együtt: munkatársak).

3. Az utasítás tárgyi hatálya kiterjed minden, az Igazgatóságon végzett adatkezelésre, a bűnüldözési, honvédelmi, nemzetbiztonsági célú adatkezelések kivételével.

4. A természetes személyek személyes adatainak védelme alapvető jog. A természetes személyek adatainak kezelésével összefüggő védelméhez kapcsolódó elvek és szabályok tiszteletben tartása és biztosítása az Igazgatóság minden dolgozójának kötelessége. A személyes adatok kezelése csak a vonatkozó európai és magyar jogi szabályok megtartásával lehetséges.

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.

6. A személyes adatok kezelésének jogszerűnek és tisztességesnek kell lennie. A természetes személyek számára átláthatónak kell lennie, hogy a rájuk vonatkozó személyes adataikat hogyan gyűjtik, használják fel, azokba hogy tekintenek bele vagy

milyen egyéb módon kezelik, valamint azzal összefüggésben, hogy a személyes adatokat milyen mértékben kezelik vagy fogják kezelni.

7. Az adatkezelés szabályszerűségét az adatkezelőnek kell bizonyítani.

8. Az adatkezelésnek meg kell felelnie a következő elveknek:

   - tisztességes eljárás,
   - jogszerűség,
   - átláthatóság,
   - célhoz kötöttség,
   - adattakarékosság,
   - pontosság,
   - korlátozott tárolhatóság,
   - integritás és bizalmas jelleg,
   - elszámoltathatóság.

I. rész
Értelmező rendelkezések

1. Ezen utasítás alkalmazása során:
   1.: érintett: bármely információ alapján azonosított vagy azonosítható természetes személy;
   1a. azonosítható természetes személy: az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;
   2. személyes adat: az érintettre vonatkozó bármely információ;
   3. különleges adat: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok,
   3a. genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered;
   3b. biometrikus adat: egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat;
   3c. egészségügyi adat: egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;

4. bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;
5. hozzájárulás: az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez;
6. adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;
6a. közös adatkezelő: az az adatkezelő, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - az adatkezelés céljait és eszközeit egy vagy több másik adatkezelővel közösen határozza meg, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket egy vagy több másik adatkezelővel közösen hozza meg és hajtja végre vagy hajtatja végre az adatfeldolgozóval;
7. adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;
8. adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;
8. közvetett adattovábbítás: személyes adatnak valamely harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére továbbítása útján valamely más harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére történő továbbítása;
8b. nemzetközi szervezet: a nemzetközi közjog hatálya alá tartozó szervezet és annak alárendelt szervei, továbbá olyan egyéb szerv, amelyet két vagy több állam közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre;
9. nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele;
10. adattörlés: az adat felismerhetetlenné tétele oly módon, hogy a helyreállítása többé nem lehetséges;
11. adatkezelés korlátozása: a tárolt adat zárolása az adat további kezelésének korlátozása céljából történő megjelölése útján;
12. adatmegsemmisítés: az adatot tartalmazó adathordozó teljes fizikai megsemmisítése;
13. adatfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége;
14. adatfeldolgozó: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió

kötelező jogi aktusában meghatározott keretek között és feltételekkel - az adatkezelő megbízásából vagy rendelkezése alapján személyes adatokat kezel;
15. adatállomány: az egy nyilvántartásban kezelt adatok összessége;
16. harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy 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 irányuló műveleteket végeznek;
17. EGT-állam: az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez;
18. harmadik ország: minden olyan állam, amely nem EGT-állam;
19. adatvédelmi incidens: az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi;
20. profilalkotás: személyes adat bármely olyan - automatizált módon történő - kezelése, amely az érintett személyes jellemzőinek, különösen a munkahelyi teljesítményéhez, gazdasági helyzetéhez, egészségi állapotához, személyes preferenciáihoz vagy érdeklődéséhez, megbízhatóságához, viselkedéséhez, tartózkodási helyéhez vagy mozgásához kapcsolódó jellemzőinek értékelésére, elemzésére vagy előrejelzésére irányul;
21. címzett: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely részére személyes adatot az adatkezelő, illetve az adatfeldolgozó hozzáférhetővé tesz;
22. álnevesítés: személyes adat olyan módon történő kezelése, amely - a személyes adattól elkülönítve tárolt - további információ felhasználása nélkül megállapíthatatlanná teszi, hogy a személyes adat mely érintettre vonatkozik, valamint műszaki és szervezési intézkedések megtételével biztosítja, hogy azt azonosított vagy azonosítható természetes személyhez ne lehessen kapcsolni;

II. rész
Adatvédelmi tisztviselő

1. Az Igazgatóságon az adatvédelmi tisztviselő Kovács Károly informatikus.

2. Az adatvédelmi tisztviselőt, és a személyét illető változást a Nemzeti Adatvédelmi és Információbiztonság Hatóság (a továbbiakban: Hatóság) nyilvántartásába be kell jelenteni.

3. A bejelentés megtételéért az Üzemeltetési Osztály vezetője a felelős. Az utasítás hatálybalépését követően az adatvédelmi tisztviselő személyét illető változást annak megtörténtét követő legkésőbb 8 napon belül kell bejelenteni a Hatóság részére.

III. rész
Az adatkezelések felmérése, adatkezelői nyilvántartás

1. Az Igazgatóságon történő minden adatkezelést fel kell mérni.

2. Az osztályvezetők jelen utasítás hatályba lépését követően legkésőbb 15 nappal felmérnek minden, az osztályukat érintő adatkezelést.

3. A jelen utasítás hatálya alá tartozó adatkezeléseket az osztályvezetőknek be kell jelenteni az integritás tanácsadónak a jelen utasítás 1. számú mellékletét képező adatkezelői nyilvántartás vonatkozó részeinek kitöltésével és megküldésével.

4. Az adatkezelői nyilvántartásba bejelentett, valamint be nem jelentett adatkezelésekért a szervezeti egységek vezetői felelősek.

5. A jelen utasítás hatályba lépését követően megkezdett adatkezelésekre a III. 3. pontban foglaltakat értelemszerűen alkalmazni kell.

6. Az adatkezelési tevékenységek felfüggesztése, megszüntetése esetén az adatkezelési tevékenységet folytató szervezeti egység vezetője az integritás tanácsadóval és az adatvédelmi tisztviselővel köteles előzetesen egyeztetni. Az integritás tanácsadó és az adatvédelmi tisztviselő iránymutatást ad az adatkezelés megszüntetését és az adatok törlését illetően.

7. Az Igazgatóság a kezelésében lévő személyes adatokkal kapcsolatos adatkezeléseiről, az adatvédelmi incidensekről és az érintett hozzáférési jogával kapcsolatos intézkedésekről nyilvántartást vezet (a továbbiakban együtt: adatkezelői nyilvántartás). Az adatkezelői nyilvántartás mintáját az 1. számú melléklet határozza meg. Az adatkezelői nyilvántartásra vonatkozó rendelkezések az adatfeldolgozót is terhelik az Infotv. 25/E.§ (2) bekezdésben foglalt eltérésekkel.

8. Az adatkezelői és az adatfeldolgozói nyilvántartást írásban vagy elektronikus úton rögzített formában kell vezetni és azt - kérésére - a Hatóság rendelkezésére kell bocsátani.

9. A személyes adatokkal elektronikus úton végzett adatkezelési műveletek jogszerűségének ellenőrizhetősége céljából az adatkezelő és az adatfeldolgozó automatizált adatkezelési rendszerben (a továbbiakban: elektronikus napló) rögzíti
   a) az adatkezelési művelettel érintett személyes adatok körének meghatározását,
   b) az adatkezelési művelet célját és indokát,
   c) az adatkezelési művelet elvégzésének pontos időpontját,
   d) az adatkezelési műveletet végrehajtó személy megjelölését,
   e) a személyes adatok továbbítása esetén az adattovábbítás címzettjét.

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

11. Az elektronikus naplóhoz a Hatóság, továbbá az előző pontban meghatározott célból jogszabályban meghatározott tevékenységet folytató személy és szervezet részére - azok erre irányuló kérelmére - az adatkezelő és az adatfeldolgozó hozzáférést biztosít, abból részükre adatot továbbít.

12. Az adatkezelői és az adatfeldolgozói nyilvántartásban, valamint az elektronikus naplóban rögzített adatokat a kezelt adat törlését követő tíz évig kell megőrizni.

IV. rész
Adatkezelési tájékoztató

1. Az adatkezelési nyilvántartásban szereplő adatkezelésekről szükség a szerinti adatvédelmi tájékoztatót kell kitöltenie az adatokat kezelő szervezeti egység vezetőjének.

2. Az adatkezelési tájékoztatót a 2. számú mellékletben meghatározott segédlet segítségével kell kitölteni.

3. Az adatkezelés jogszerű alappal is csak abban az esetben történhet, amennyiben az érintett az adatok kezeléséhez hozzájárult.

4. Az érintett számára az adatkezeléssel kapcsolatos információkat közérthető módon, világosan kell megadni.

5. Az érintett hozzájárulásaként csakis az érintett akaratának önkéntes, konkrét, és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása fogadható el, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.

6. Az adatkezelésre csak akkor kerülhet sor, ha az érintett egyértelmű megerősítő cselekedettel, például írásbeli – ideértve az elektronikus úton tett –, vagy szóbeli nyilatkozattal önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulását adja a természetes személyt érintő személyes adatok kezeléséhez. Ilyen hozzájárulásnak minősül az is, ha az érintett valamely internetes honlap megtekintése során bejelöl egy erre vonatkozó négyzetet, az információs társadalommal összefüggő szolgáltatások igénybevétele során erre vonatkozó technikai beállításokat hajt végre, valamint bármely egyéb olyan nyilatkozat vagy cselekedet is, amely az adott összefüggésben az érintett hozzájárulását személyes adatainak tervezett kezeléséhez egyértelműen jelzi.

7. A hallgatás, az előre bejelölt négyzet vagy a nem cselekvés ezért nem minősül hozzájárulásnak.

8. A hozzájárulás az ugyanazon cél vagy célok érdekében végzett összes adatkezelési tevékenységre kiterjed.

9. Ha az adatkezelés egyszerre több célt is szolgál, akkor a hozzájárulást az összes adatkezelési célra vonatkozóan meg kell adni.

10. Ha az érintett hozzájárulását elektronikus felkérést követően adja meg, a felkérésnek egyértelműnek és tömörnek kell lennie, és az nem gátolhatja szükségtelenül azon szolgáltatás igénybevételét, amely vonatkozásában a hozzájárulást kérik.

11. Személyes adat akkor kezelhető, ha
a) azt törvény vagy - törvény felhatalmazása alapján, az abban meghatározott körben, különleges adatnak vagy bűnügyi személyes adatnak nem minősülő adat esetén - helyi önkormányzat rendelete közérdeken alapuló célból elrendeli,
b) az a) pontban meghatározottak hiányában az az adatkezelő törvényben meghatározott feladatainak ellátásához feltétlenül szükséges és az érintett a személyes adatok kezeléséhez kifejezetten hozzájárult,
c) az a) pontban meghatározottak hiányában az az érintett vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét vagy javait fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges és azzal arányos, vagy
d) az a) pontban meghatározottak hiányában a személyes adatot az érintett kifejezetten nyilvánosságra hozta és az az adatkezelés céljának megvalósulásához szükséges és azzal arányos.

12. Különleges adat
a) a IV.11. c)-d) pontjában meghatározottak szerint, vagy
b) akkor kezelhető, ha az törvényben kihirdetett nemzetközi szerződés végrehajtásához feltétlenül szükséges és azzal arányos, vagy azt az Alaptörvényben biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűncselekmények megelőzése, felderítése vagy üldözése érdekében vagy honvédelmi érdekből törvény elrendeli.

13. Annak érdekében, hogy a személyes adatok kezelése jogszerű legyen, annak az érintett hozzájárulásán kell alapulnia, vagy valamely egyéb jogszerű, jogszabály által megállapított alappal kell rendelkeznie, ideértve az adatkezelőre vonatkozó jogi kötelezettségeknek való megfelelés szükségességét, az érintett által kötött esetleges szerződés teljesítését, illetve az érintett által kért, a szerződéskötést megelőzően megteendő lépéseket. Jogszerű az adatkezelés abban az esetben is, ha az érintett személy életének vagy más természetes személynek érdekeinek védelme céljából történik.

14. Az érintett jogosult arra, hogy az adatkezelő és az annak megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adatai vonatkozásában az e törvényben meghatározott feltételek szerint
a) az adatkezeléssel összefüggő tényekről az adatkezelés megkezdését megelőzően tájékoztatást kapjon (a továbbiakban: előzetes tájékozódáshoz való jog),
b) kérelmére személyes adatait és az azok kezelésével összefüggő információkat az adatkezelő a rendelkezésére bocsássa (a továbbiakban: hozzáféréshez való jog),
c) kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatait az adatkezelő helyesbítse, illetve kiegészítse (a továbbiakban: helyesbítéshez való jog),

d) kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatai kezelését az adatkezelő korlátozza (a továbbiakban: az adatkezelés korlátozásához való jog),
e) kérelmére, valamint az e fejezetben meghatározott további esetekben személyes adatait az adatkezelő törölje (a továbbiakban: törléshez való jog).

V. rész
Adatvédelmi hatásvizsgálat

1. A tervezett adatkezelés megkezdését megelőzően fel kell mérni, hogy a tervezett adatkezelés annak körülményeire, így különösen céljára, az érintettek körére, az adatkezelési műveletek során alkalmazott technológiára tekintettel várhatóan milyen hatásokat fog gyakorolni az érintetteket megillető alapvető jogok érvényesülésére.

2. Ha az V.1. pont alapján elvégzett kockázatbecslés alapján a tervezett adatkezelés valószínűsíthetően az érintetteket megillető, valamely alapvető jog érvényesülését lényegesen befolyásolja (a továbbiakban: magas kockázatú adatkezelés), az adatkezelő – a kötelező adatkezelés kivételével - az adatkezelés megkezdését megelőzően írásban elemzést készít arról, hogy a tervezett adatkezelés az érintetteket megillető alapvető jogok érvényesülésére milyen várható hatásokat fog gyakorolni (a továbbiakban: adatvédelmi hatásvizsgálat).

3. Ha a Hatóság valamely meghatározott adatkezelés-típust magas kockázatú adatkezelésnek minősít és e megállapítását közzéteszi, valamint a tervezett adatkezelés e megállapítással érintett adatkezelés-típus során alkalmazottal azonos vagy ahhoz hasonló típusú művelet vagy műveletsorozat alkalmazásával jár, a tervezett adatkezelés tekintetében annak magas kockázatát vélelmezni kell.

4. Ha a Hatóság valamely meghatározott adatkezelés-típus tekintetében azt állapítja meg, hogy az nem minősül magas kockázatú adatkezelésnek és e megállapítását közzéteszi, valamint a tervezett adatkezelés kizárólag e megállapítással érintett adatkezelés-típus során alkalmazottal azonos vagy ahhoz hasonló típusú művelet vagy műveletsorozat alkalmazásával jár, a tervezett adatkezelés tekintetében azt kell vélelmezni, hogy az nem minősül magas kockázatú adatkezelésnek.

5. Az adatvédelmi hatásvizsgálat tartalmazza legalább a tervezett adatkezelési műveletek általános leírását, az érintettek alapvető jogainak érvényesülését fenyegető, az adatkezelő által azonosított kockázatok leírását és jellegét, az e kockázatok kezelése céljából tervezett, valamint a személyes adatokhoz fűződő jog érvényesülésének biztosítására irányuló, az adatkezelő által alkalmazott intézkedéseket. Az adatvédelmi hatásvizsgálatot a 3. számú mellékletben szereplő minta alkalmazásával kell végezni. A hatásvizsgálat lefolytatásába az integritás tanácsadót és az adatvédelmi tisztviselőt be kell vonni.

6: Ha a tervezett adatkezelés
a) vonatkozásában lefolytatott adatvédelmi hatásvizsgálat eredménye alapján megállapítható, hogy a tervezett adatkezelés - az adatkezelő által az adatkezeléssel

járó kockázatok mérsékléséhez szükséges intézkedések megtételének hiányában - magas kockázatú lenne, vagy
b) magas kockázatát az V.3. pont szerint vélelmezni kell,
az adatkezelő vagy tevékenysége keretei között az adatfeldolgozó - a kötelező adatkezelés kivételével - az adatkezelés megkezdését megelőzően konzultációt kezdeményez a Hatósággal (a továbbiakban: előzetes konzultáció).

7. Az adatkezelő vagy tevékenysége keretei között az adatfeldolgozó az előzetes konzultáció kezdeményezésével egyidejűleg a Hatóság rendelkezésére bocsátja az adatvédelmi hatásvizsgálat eredményét, továbbá felvilágosítást nyújt a Hatóság részére minden olyan körülményről, amelynek tisztázását a Hatóság az előzetes konzultáció eredményes lefolytatása érdekében szükségesnek tartja.

8. Ha a Hatóság az előzetes konzultáció során arra a megállapításra jut, hogy a tervezett adatkezelés vonatkozásában az arra irányadó jogszabályban meghatározott előírások nem érvényesülnek maradéktalanul - különösen, ha álláspontja szerint az adatkezelő az adatkezeléssel járó kockázatokat nem megfelelően azonosította vagy nem megfelelően mérsékelte -, a feladat- és hatáskörébe tartozó bármely egyéb intézkedés megtétele mellett vagy helyett a feltárt hiányosságok megszüntetésére alkalmas lépéseket határoz meg és azok végrehajtására tesz javaslatot az adatkezelő, illetve - annak tevékenységi körére korlátozva - az adatfeldolgozó részére.

VI. rész
Adatkezelési incidens

1. Adatvédelmi incidens bekövetkezése esetén meg kell tenni a jelen részben foglalt intézkedéseket a bekövetkezett vagy fenyegető sérelmek mértékének csökkentése végett és törekedni kell arra, hogy a továbbiakban incidens ne fordulhasson elő.

2. Incidens bekövetkezése esetén az azt észlelő személynek nyomban értesítenie kell az integritás tanácsadót a 4. számú mellékletben foglalt nyomtatvány kitöltésével.

3. Az integritás tanácsadó értesítését az észlelést követően úgy kell megtenni, hogy kellő idő álljon rendelkezésre a belső intézkedések megtételére, és a Hatóság, valamint az érintett tájékoztatására.

4. Adatvédelmi incidens bekövetkezését haladéktalanul, de legkésőbb az észlelést követő 72 órán belül be kell jelenteni a Hatóságnak. A bejelentés megtételéért az adatvédelmi tisztviselő a felelős.

5. Amennyiben a bejelentést akadályoztatás miatt határidőben nem lehetett megtenni, az akadály megszűnését követően haladéktalanul teljesíteni kell. Ez esetben a bejelentéshez mellékelni kell a késedelem okait feltáró nyilatkozatot is.

6. Az adatvédelmi incidenst nem kell bejelenteni a Hatóságnak, ha valószínűsíthető, hogy nem jár kockázattal az érintettek jogainak érvényesülésére.

7. Adatvédelmi incidens bekövetkezése esetén rögzíteni kell az incidens bekövetkezésének körülményeit, így az incidenst észlelő személy

   - ismerteti az adatvédelmi incidens jellegét, beleértve - ha lehetséges - az érintettek körét és hozzávetőleges számát, valamint az incidenssel érintett adatok körét és hozzávetőleges mennyiségét,
   - tájékoztatást nyújt az adatvédelmi tisztviselő nevéről és elérhetőségi adatairól,
   - ismerteti az adatvédelmi incidensből eredő, valószínűsíthető következményeket, és
   - ismerteti az adatkezelő által az adatvédelmi incidens kezelésére tett vagy tervezett - az adatvédelmi incidensből eredő esetleges hátrányos következmények mérséklését célzó és egyéb - intézkedéseket.

8. Ha az adatvédelmi incidens valószínűsíthetően az érintettet megillető valamely alapvető jog érvényesülését lényegesen befolyásoló következményekkel járhat (a továbbiakban: magas kockázatú adatvédelmi incidens), az adatvédelmi tisztviselő az érintettet az adatvédelmi incidensről haladéktalanul tájékoztatja.

9. Nem kell tájékozatni az érintettet, ha
   a) az adatkezelő az adatvédelmi incidenssel érintett adatok tekintetében az adatvédelmi incidenst megelőzően megfelelő - így különösen az adatokat a jogosulatlan személy általi hozzáférés esetére értelmezhetetlenné alakító, azok titkosítását eredményező - műszaki és szervezési védelmi intézkedéseket alkalmazott,
   b) az adatkezelő az adatvédelmi incidensről való tudomásszerzését követően alkalmazott intézkedésekkel biztosította, hogy az adatvédelmi incidens folytán az érintettet megillető valamely alapvető jog érvényesülését lényegesen befolyásoló következmények valószínűsíthetően nem következnek be,
   c) az érintett közvetlen tájékoztatása csak az Igazgatóság aránytalan erőfeszítésével lenne teljesíthető, ezért az Igazgatóság az érintettek részére az adatvédelmi incidenssel összefüggő megfelelő tájékoztatást bárki által hozzáférhető módon közzétett információk útján biztosítja, vagy
   d) törvény a tájékoztatást kizárja.

10. Adatvédelmi incidens bekövetkezése esetén az adatfeldolgozó is értelemszerűen köteles a jelen részben foglaltak teljesítésére, azzal, hogy az incidens bekövetkeztét az Igazgatóság integritás tanácsadójának kell jeleznie.

VII. rész
Elhunyt személy adatainak védelme

1. Az érintett halálát követő öt éven belül a 14. pontban, illetve - az általános adatvédelmi rendelet hatálya alá tartozó adatkezelési műveletek esetén – a GDPR 15-18. és 21. cikkében meghatározott, az elhaltat életében megillető jogokat az érintett által arra ügyintézési rendelkezéssel, illetve közokiratban vagy teljes bizonyító erejű magánokiratban foglalt, az adatkezelőnél tett nyilatkozattal - ha az érintett egy adatkezelőnél több nyilatkozatot tett, a későbbi időpontban tett nyilatkozattal - meghatalmazott személy jogosult érvényesíteni.

2. Ha az érintett nem tett az 1 bekezdésnek megfelelő jognyilatkozatot, a Polgári Törvénykönyv szerinti közeli hozzátartozója annak hiányában is jogosult az adott adatkezelési műveletek esetén a meghatározott, az elhaltat életében megillető jogokat érvényesíteni az érintett halálát követő öt éven belül.

3. Az érintett jogainak előző pont szerinti érvényesítésére az a közeli hozzátartozó jogosult, aki ezen jogosultságát elsőként gyakorolja.

4. Az érintett jogait ezen rész alapján érvényesítő személyt e jogok érvényesítése - így különösen az adatkezelővel szembeni, valamint a Hatóság, illetve bíróság előtti eljárás - során az e törvény által az érintett részére megállapított jogok illetik meg és kötelezettségek terhelik.

5. Az érintett jogait érvényesítő személy az érintett halálának tényét és idejét halotti anyakönyvi kivonattal vagy bírósági határozattal, valamint saját személyazonosságát - és a közeli hozzátartozói minőségét - közokirattal igazolja.

6. Az Igazgatóság kérelemre tájékoztatja az érintett Polgári Törvénykönyv szerinti közeli hozzátartozóját az ezen rész alapján megtett intézkedésekről, kivéve, ha azt az érintett az 1. pontban meghatározott nyilatkozatában megtiltotta.

VIII. rész
Adatbiztonsági intézkedések

1. Az Igazgatóságon az adatvédelmi tisztviselő felel a megfelelő adatbiztonsági intézkedések kialakításáért és megtartásáért.

2. Ennek keretében olyan intézkedéseket kell hozni, amelyek az adatkezeléseket védik a külső beavatkozásoktól, megelőzik az adattartalmak nem szándékolt megváltozását, biztosítják, hogy az adatokhoz az érintetten kívül csak az férhessen hozzá, akinek feladata ellátásához szükséges.

3. Az adatvédelmi tisztviselő az adatkezelés jogszerűségének biztosítása érdekében az adatkezelés összes körülményéhez, így különösen céljához, valamint az érintettek alapvető jogainak érvényesülését az adatkezelés által fenyegető kockázatokhoz igazodó műszaki és szervezési intézkedéseket tesz, ideértve indokolt esetben az álnevesítés alkalmazását. Ezeket az intézkedéseket az adatkezelő rendszeresen felülvizsgálja és szükség esetén megfelelően módosítja.

4. Ezen intézkedéseket úgy kell kialakítani, hogy azok
a) a tudomány és technológia mindenkori állásának és az intézkedések megvalósítása költségeinek figyelembevételével észszerűen elérhető módon a személyes adatok kezelésére vonatkozó követelmények, így különösen az adatkezelés alapelvei és az érintettek jogai hatékony érvényesülését szolgálják, valamint
b) alkalmasak és megfelelőek legyenek annak biztosítására, hogy alapértelmezés szerint

ba) kizárólag olyan és annyi személyes adat kezelésére kerüljön sor, olyan mértékben és időtartamban, amely az adatkezelés célja szempontjából szükséges, és
bb) az adatkezelő által kezelt személyes adatok az érintett erre irányuló kifejezett akarata hiányában ne válhassanak nyilvánosan hozzáférhetővé.

5. A jelen résznek megfelelő intézkedéseket az adatvédelmi tisztviselő az Igazgatóság Informatikai Biztonsági Szabályzata figyelembevételével határozza meg.

6. Az adatvédelmi tisztviselő a kezelt személyes adatok megfelelő szintű biztonságának biztosítása érdekében az érintettek alapvető jogainak érvényesülését az adatkezelés által fenyegető - így különösen az érintettek különleges adatainak kezelésével járó - kockázatok mértékéhez igazodó műszaki és szervezési intézkedéseket tesz.

7. Ezen intézkedések kialakítása és végrehajtása során figyelembe veszi az adatkezelés összes körülményét, így különösen a tudomány és a technológia mindenkori állását, az intézkedések megvalósításának költségeit, az adatkezelés jellegét, hatókörét és céljait, továbbá az érintettek jogainak érvényesülésére az adatkezelés által jelentett változó valószínűségű és súlyosságú kockázatokat.

8. Ennek keretében meghatározott intézkedésekkel biztosítja
a) az adatkezeléshez használt eszközök (a továbbiakban: adatkezelő rendszer) jogosulatlan személyek általi hozzáférésének megtagadását,
b) az adathordozók jogosulatlan olvasásának, másolásának, módosításának vagy eltávolításának megakadályozását,
c) az adatkezelő rendszerbe a személyes adatok jogosulatlan bevitelének, valamint az abban tárolt személyes adatok jogosulatlan megismerésének, módosításának vagy törlésének megakadályozását,
d) az adatkezelő rendszerek jogosulatlan személyek általi, adatátviteli berendezés útján történő használatának megakadályozását,
e) azt, hogy az adatkezelő rendszer használatára jogosult személyek kizárólag a hozzáférési engedélyben meghatározott személyes adatokhoz férjenek hozzá,
f) azt, hogy ellenőrizhető és megállapítható legyen, hogy a személyes adatokat adatátviteli berendezés útján mely címzettnek továbbították vagy továbbíthatják, illetve bocsátották vagy bocsáthatják rendelkezésére,
g) azt, hogy utólag ellenőrizhető és megállapítható legyen, hogy mely személyes adatokat, mely időpontban, ki vitt be az adatkezelő rendszerbe,
h) a személyes adatoknak azok továbbítása során vagy az adathordozó szállítása közben történő jogosulatlan megismerésének, másolásának, módosításának vagy törlésének megakadályozását,
i) azt, hogy üzemzavar esetén az adatkezelő rendszer helyreállítható legyen, valamint
j) azt, hogy az adatkezelő rendszer működőképes legyen, a működése során fellépő hibákról jelentés készüljön, továbbá a tárolt személyes adatokat a rendszer hibás működtetésével se lehessen megváltoztatni.

9. A különböző nyilvántartásokban elektronikusan kezelt adatállományok védelme érdekében az adatvédelmi tisztviselő megfelelő műszaki megoldással biztosítja,

hogy a nyilvántartásokban tárolt adatok - kivéve, ha azt törvény lehetővé teszi - közvetlenül ne legyenek összekapcsolhatók és az érintetthez rendelhetők.

10. A GDPR 32. cikkében foglalt előírásoknak megfelelően az Igazgatóság garantálja az általa végzett adatkezelés jellegének, hatókörének, körülményeinek és céljainak megfelelő adatbiztonságot, azaz:

- a bizalmasságot, amelynek értelmében kizárólag az arra jogosultak ismerhetik meg a személyes adatokat;
- a sértetlenséget/integritást, vagyis a személyes adatok az adatkezelés teljes időtartama alatt az eredeti állapotnak megfelelnek;
- a rendelkezésre állást, vagyis az adatok az adatkezelés teljes folyamata során rendelkezésre állnak, amikor rájuk szükség van.

Adatkezelő az információbiztonsági intézkedésekkel megteremti a kezelt személyes adatok fizikai logikai és adminisztratív kontrollját.

11. Fizikai kontroll:
- Az Igazgatóság székhelye riasztórendszerrel felszerelt épületben található, szerződött kivonuló szolgálattal;
- Az ügyfelekkel kötött szerződések és a munkaügyi személyi anyagok kinyomtatva, lefűzve egy-egy zárható szekrényben kerültek elhelyezésre.
- Az igazgatóság adatkezelést végző munkatársi a nap folyamán kizárólag úgy hagyhatják el azt a helyiséget, ahol az adatkezelés zajlik, hogy a rá bízott adathordozókat elzárják, a számítógépeiket jelszóval zárolják, vagy az irodát bezárják.
- Adatkezelő szervere az épületben egy elzárt szobában található, amelynek kulcsával kizárólag az igazgató és az adatvédelmi tisztviselő rendelkezik.
- A szerződésekhez az adatkezelést végző munkakörben foglalkoztatott munkatársak, a személyi anyagokhoz az álláshelyen ellátandó feladat alapján érintett munkatárs rendelkezik hozzáféréssel, azokat más személyek nem ismerhetik meg, nem férhetnek hozzá.
- Amennyiben a papír alapon tárolt személyes adat kezelésének célja megvalósult, intézkedni kell a papír megsemmisítéséről.

12. Informatikai védelem (mint a fizikai kontroll része):
- Az adatkezelés során használt számítógépek az Igazgatóság tulajdonát képezik;
- Helyi számítógépre adatmentés nem végezhető, a személyes adatokat tartalmazó dokumentumokat, nyilvántartásokat, egyéb adatbázisokat a. központi szerverekre kell menteni.
- A hálózati kiszolgáló gépen tárolt adatokhoz csak a megfelelő jogosultsággal rendelkező és arra kijelölt személyek férhetnek hozzá;
- A hálózaton tárolt adatok biztonsága érdekében a szerverek esetén magas rendelkezésre állású infrastruktúrán történő mentésekkel és archiválással kerüli el az Adatkezelő az adatvesztést;
- A lementett adatokat tároló mágneses adathordozó az erre a célra kialakított páncélszekrényben tűzbiztos helyen és módon tárolt;
- Adatkezelő a rendelkezésre álló számítástechnikai eszközökkel, azok alkalmazásával megakadályozza az illetéktelen személyek hálózati hozzáférését;

- A számítógépeken található adatokhoz csak érvényes, személyre szóló, azonosítható jogosultsággal – minimum felhasználónévvel és jelszóval – lehet hozzáférni, a jelszavak időszakonkénti cseréjéről a felhasználó gondoskodik;
- Amennyiben az adatkezelés célja megvalósult, az adatkezelés határideje letelt, úgy az adatot tartalmazó fájlt visszaállíthatatlanul törölni kell, az adat útja vissza nem nyerhető;
- A teljes szerver összes anyaga vonatkozásában napi mentést végez, a mentés mágneses adathordozóra történik;
- Adatkezelő a személyes adatokat kezelő hálózaton a vírusvédelemről folyamatosan gondoskodik;
- Adatkezelő a szerver(eke)t külön erre a célra kialakított, zárható helyiségben helyezi el, amelybe belépési engedéllyel kizárólag az adatvédelmi tisztviselő, valamint az igazgató és az általa erre írásban felhatalmazott személy rendelkezik;

13. Adminisztratív kontroll:

- Adatkezelő a jelen utasításnak megfelelően kialakította azokat az eljárási szabályokat, amelyek biztosítják a jogszabályi rendelkezések érvényre juttatását. Felülvizsgálta és kiegészítette továbbá az adatfeldolgozási szerződéseket, és munkatársi oktatásával is biztosítja az adminisztratív kontrollt.
- Az igazgatóság rendelkezik érvényes Informatikai Biztonsági Szabályzattal (továbbiakban: IBSZ), amely biztonságkezelési elveket, követelményeket és szabályokat tartalmaz az Igazgatóságon tevékenykedő személyek (bizonyos feltételek esetén külső közreműködők) számára, akik felelősek az információbiztonság fejlesztéséért, megvalósításáért és megtartásáért. Az IBSZ hatékonyan támogatja az Igazgatóság biztonságkezelésének mindennapi gyakorlatát, illetve megfelelő kereteket biztosít az Igazgatóság teljes körű biztonsági szabályozásához.

14. Logikai kontroll

- A természetes személyek személyes adatai egymástól elkülönítetten kezelt, megfelelő IT biztonsági intézkedésekkel védett adatbázisban találhatók, amelyekhez kizárólag az arra jogosultak rendelkeznek hozzáféréssel.

IX. Rész
Felelősség az adatvédelmi rendelkezések megsértéséért

1. A jelen utasításban foglaltak be nem tartása esetén az Igazgatóság a Ptk.-ban rögzítettek szerint tartozik felelősséggel.

2. Az előző pontban rögzítettek nem zárják ki a közigazgatási bírságért való felelősséget.

3. Az Igazgatóság egyes munkatársai a fegyelmi, illetve munkajogi felelősségen túl személyes büntetőjogi felelőséggel is tartoznak a Btk. 219.§; (személyes adattal visszaélés) 422.§ (tiltott adatszerzés) szerint.

4. Az adatkezelő szerv vezetője az Igazgató, aki felelős
   - *a)* az Igazgatóság által kezelt személyes adatok védelméhez szükséges személyi, tárgyi és technikai feltételek biztosítását célzó, hatáskörébe tartozó intézkedések megtételéért,
   - *b)* az irányítása és felügyelete alá tartozó személyi állomány adatvédelmi oktatásáért az adatvédelmi tisztviselő és az integritás tanácsadó bevonásával,
   - *c)* az irányítása és felügyelete alá tartozó szerv tevékenységének rendszeres adatvédelmi ellenőrzéséért, az ellenőrzés során esetlegesen feltárt hiányosságok vagy jogszabálysértő körülmények megszüntetéséért, a személyi felelősség megállapításához szükséges eljárás kezdeményezéséért, illetve lefolytatásáért,
   - *d)* az érintettek Infotv.-ben meghatározott jogainak gyakorlásához szükséges feltételek biztosításáért.

5. Az egyes szervezeti egységek vezetői, az adatvédelmi tisztviselő és az integritás tanácsadó jelen utasításban foglaltak szerint felel az utasítás betartásáért.

X. rész
Záró rendelkezések

1. Ezt a utasítást 2020. november 1. napján lép hatályba.

2. Az utasítás hatályba lépésével egyidejűleg az 5-4/2015. számú igazgatói utasítás hatályát veszti.

Eger, 2020. október 30.

BÜKKI NEMZETI PARK Igazgatóság 5. Eger

Rónai Kálmánné
igazgató

Mellékletek:
1.- Adatkezelési nyilvántartás
2.- Adatkezelési tájékoztató
3.- Adatvédelmi hatásvizsgálat
4.- Incidensbejelentés