Adatkezelési nyilvántartás

Adatkezelő: **Nemzeti Adatvédelmi és Információszabadság Hatóság**

Budapest 1125 Szilágyi Erzsébet fasor 22/c.

Adatvédelmi tisztviselő: **Zsikóné Kendra Klára**

Budapest 1125 Szilágyi Erzsébet fasor 22/c.

dpo@naih.hu

2018. június 25.

1. közfeladatot ellátó szervek iratkezelése	
Adatkezelés célja	Infotv.38. § és (EU) 2016/679 rendelet 57. cikk (1) bek. c)-e) pont szerinti feladatok ellátása
Érintettek kategóriái	- iratot beküldő személy (kérelmező, bejelentő, panaszos, hatósági ügy ügyfele, egyéb ügyfél, megkereső személy vagy ilyen szervezet képviselője); - irat címzettje (kérelmező, bejelentő, panaszos, hatósági ügy ügyfele, egyéb ügyfél) - ügyintézésben, ügykezelésben részt vevő személyek
Személyes adatok kategóriái	beküldő és címzett neve és elérhetősége, ügyintéző, ügykezelő neve
A különböző adatkategóriák törlésére előirányzott határidők	az iratkezeléshez kapcsolódó nyilvántartásban (iktatókönyv) szereplő adatokat a szerv a megszűnéséig, illetve az iktatókönyv levéltárba adásáig kezeli
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

2. személyes adatok védelmével összefüggő ügyben a vizsgálati eljárás, hatósági ellenőrzés vagy hatósági eljárás során történő adatkezelés	
Adatkezelés célja	Infotv.38. §, 30-32. alcím és (EU) 679/2016 rendelet 57-58. cikke szerinti feladatok ellátása és hatáskörök gyakorlása
Érintettek kategóriái	kérelmező, bejelentő, panaszos, hatósági eljárás más ügyfele és egyéb résztvevője, az eljárás tárgyát képező személyesadat-kezelés keretében a tényállás tisztázása során megvizsgált személyes adatok érintettjei
Személyes adatok kategóriái	- kérelmező, illetve bejelentő/panaszos, továbbá az ügyfél és eljárás egyéb résztvevőjének természetes személyazonosító adatai, - az adott ügy jellegétől, az eljárás tárgyától függően a tényállás tisztázásához elengedhetetlenül szükséges más, bármilyen érintetti kategóriához fűződő személyes adat kezelésére sor kerülhet (ideértve az (EU) 2016/679 rendelet alkalmazásában kiszolgáltatott személyeknek minősülő személyek adatait is, illetve a rendelet 9. cikk (1) bek. szerinti különleges, továbbá a rendelet 10. cikkében meghatározott bűnügyi személyes adatokat is).
A különböző adatkategóriák törlésére előirányzott határidők	Az adatokat tartalmazó dokumentumokat (adathordozókat) a közfeladatot ellátó szervek iratkezelésére vonatkozó jogszabályi követelmények (köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény (Ltv.), illetve a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet) szerint iktatja, és az iktatott iratok között az irat irattári tervben meghatározottak szerinti selejtezéséig, illetve – ennek hiányában – levéltárba adásáig kezeli. Az adatokat az ügy lezárását (eljárás megszüntetése, ellenőrzés lezárása hatósági eljárás megindítása nélkül, jelentés készítése, ajánlás, felszólítás kiadása, határozat hozatala) követően a Hatóság zárolja (az adatkezelést korlátozza), azok az ügyet lezáró ajánlás, felszólítás vagy hatósági döntés végrehajtása, a döntésben foglaltak ellenőrzése vagy a döntéssel összefüggő jogorvoslat vagy döntés-felülvizsgálat céljából kezeli addig, amíg ennek jogi lehetősége vagy szükségessége fennáll. Ezt követően az Ltv. szerint levéltárba adandó iratokban foglalt adatok és az iratkezelési rendszerben a jogszabálynál fogva kezelendő személyes adatok kivételével a hatóság az adatot törli, illetve - adott esetben a lefoglalt adathordozót visszaszolgáltatva -- az adatkezelést megszünteti. A levéltárba adással (főszabály szerint 15 év elteltével) a személyes adatok kezelése a Hatóságnál megszűnik.

Címzettek kategóriái	1. amennyiben az adott eljárásban a tényállás tisztázásához vagy a döntéshozatalhoz szükséges más hatóság, szerv vagy személy megkeresése, a Hatóság -- a megkeresés teljesítéséhez feltétlenül szükséges mértékben -- személyes adatot közölhet - a megkeresett magyar hatósággal, szervvel vagy más EU-tagállamnak az (EU) 2016/679 rendelet szerinti felügyeleti hatóságával, - az (EU) 2016/679 rendelet 56. cikke és VII. fejezete szerinti eljárásokban más EU-tagállam felügyeleti hatósága, az Európai Adatvédelmi Testülettel (a továbbiakban: Testület), illetve a Testület Titkárságával és az Európai Unió Bizottságával, - az adott eljárásban vizsgált adatkezelővel, adatfeldolgozóval, az adattovábbítás címzettjével; 2. a hatósági eljárás ügyfele az iratbetekintési joga gyakorlása keretében megismerheti a nem zártan kezelt személyes adatokat, 3. a hatóság cselekményével szembeni perben eljáró bíróság
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	Amennyiben az adott eljárásban a tényállás tisztázásához vagy a döntéshozatalhoz szükséges más harmadik országbeli hatóság, szerv vagy személy megkeresése, a Hatóság -- a megkeresés teljesítéséhez feltétlenül szükséges mértékben -- személyes adatot közölhet a megkeresett magyar hatósággal, szervvel
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

3. titokfelügyeleti ügyben a vizsgálati eljárás, hatósági ellenőrzés vagy hatósági eljárás során történő adatkezelés	
Adatkezelés célja	Infotv.38. § (2) bek, 30-31. és 33. alcím
Érintettek kategóriái	kérelmező, bejelentő, panaszos, a minősítő és a hatósági eljárás egyéb résztvevője, az eljárás tárgyát képező személyesadat-kezelés keretében a tényállás tisztázása során megvizsgált személyes adatok érintettjei
Személyes adatok kategóriái	- kérelmező, illetve bejelentő/panaszos, továbbá az ügyfél és eljárás egyéb résztvevőjének természetes személyazonosító adatai, - az adott ügy jellegétől, az eljárás tárgyától függően a tényállás tisztázásához elengedhetetlenül szükséges más, bármilyen érintetti kategóriához fűződő személyes adat kezelésére sor kerülhet (ideértve az (EU) 2016/679 rendelet alkalmazásában kiszolgáltatott személyeknek minősülő személyek adatait is, illetve a rendelet 9. cikk (1) bek. szerinti különleges, továbbá a rendelet 10. cikkében meghatározott bűnügyi személyes adatokat is).
A különböző adatkategóriák törlésére előirányzott határidők	Az adatokat tartalmazó dokumentumokat (adathordozókat) a közfeladatot ellátó szervek iratkezelésére vonatkozó jogszabályi követelmények (köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény (Ltv.), illetve a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet) szerint iktatja, és az iktatott iratok között az irat irattári tervben meghatározottak szerinti selejtezéséig, illetve – ennek hiányában – levéltárba adásáig kezeli. Az adatokat az ügy lezárását (eljárás megszüntetése, ellenőrzés lezárása hatósági eljárás megindítása nélkül, jelentés készítése, ajánlás, felszólítás kiadása, határozat hozatala) követően a Hatóság zárolja (az adatkezelést korlátozza), azok az ügyet lezáró ajánlás, felszólítás vagy hatósági döntés végrehajtása, a döntésben foglaltak ellenőrzése vagy a döntéssel összefüggő jogorvoslat vagy döntés-felülvizsgálat céljából kezeli addig, amíg ennek jogi lehetősége vagy szükségessége fennáll. Ezt követően az Ltv. szerint levéltárba adandó iratokban foglalt adatok és az iratkezelési rendszerben a jogszabálynál fogva kezelendő személyes adatok kivételével a hatóság az adatot törli, illetve - adott esetben a lefoglalt adathordozót visszaszolgáltatva -- az adatkezelést megszünteti. A levéltárba adással (főszabály szerint 15 év elteltével) a személyes adatok kezelése a Hatóságnál megszűnik.

Címzettek kategóriái	1. amennyiben az adott eljárásban a tényállás tisztázásához vagy a döntéshozatalhoz szükséges más hatóság, szerv vagy személy megkeresése, a Hatóság – a megkeresés teljesítéséhez feltétlenül szükséges mértékben – személyes adatot közölhet - a megkeresett magyar hatósággal, szervvel vagy más EU-tagállamnak az (EU) 2016/679 rendelet szerinti felügyeleti hatóságával, - az (EU) 2016/679 rendelet 56. cikke és VII. fejezete szerinti eljárásokban más EU-tagállam felügyeleti hatósága, az Európai Adatvédelmi Testülettel (a továbbiakban: Testület), illetve a Testület Titkárságával és az Európai Unió Bizottságával, - az adott eljárásban vizsgált adatkezelővel, adatfeldolgozóval, az adattovábbítás címzettjével; 2. a hatósági eljárás ügyfele az iratbetekintési joga gyakorlása keretében megismerheti a nem zártan kezelt személyes adatokat, 3. a hatóság cselekményével szembeni perben eljáró bíróság
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	Amennyiben az adott eljárásban a tényállás tisztázásához vagy a döntéshozatalhoz szükséges más harmadik országbeli hatóság, szerv vagy személy megkeresése, a Hatóság – a megkeresés teljesítéséhez feltétlenül szükséges mértékben – személyes adatot közölhet a megkeresett magyar hatósággal, szervvel
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • biztonsági terület, • biztonsági tárolók, • kompromittáló elektromágneses kisugárzás ellen védett informatikai rendszer, • Képzés, tudatosítás

4. közérdekű adatok nyilvánosságával összefüggő vizsgálati eljárás során történő adatkezelés	
Adatkezelés célja	Infotv.38. § (2) bek, 30-31. alcím
Érintettek kategóriái	kérelmező, bejelentő, panaszos, hatósági eljárás más ügyfele és egyéb résztvevője, az eljárás tárgyát képező személyesadat-kezelés keretében a tényállás tisztázása során megvizsgált személyes adatok érintettjei
Személyes adatok kategóriái	- bejelentő/panaszos eljárás egyéb résztvevőjének természetes személyazonosító adatai, - az adott ügy jellegétől, az eljárás tárgyától függően, amelyek az eljárással összefüggnek, illetve amelyek kezelése az eljárás eredményes lefolytatása érdekében szükséges más, bármilyen érintetti kategóriához fűződő személyes adat kezelésére sor kerülhet (ideértve az (EU) 2016/679 rendelet alkalmazásában kiszolgáltatott személyeknek minősülő személyek adatait is, illetve a rendelet 9. cikk (1) bek. szerinti különleges, továbbá a rendelet 10. cikkében meghatározott bűnügyi személyes adatokat is).
A különböző adatkategóriák törlésére előirányzott határidők	Az adatokat tartalmazó dokumentumokat (adathordozókat) a közfeladatot ellátó szervek iratkezelésére vonatkozó jogszabályi követelmények (köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény (Ltv.), illetve a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet) szerint iktatja, és az iktatott iratok között az irat irattári tervben meghatározottak szerinti irattári tervben meghatározottak szerinti selejtezéséig, illetve – ennek hiányában – levéltárba adásáig kezeli. Az adatokat az ügy lezárását ajánlás, felszólítás kiadása, vizsgálat megszüntetése) követően a Hatóság zárolja (az adatkezelést korlátozza), azok az ügyet lezáró ajánlás, felszólítás végrehajtásának ellenőrzése az Infotv. 59. §-a szerinti jelentés készítése céljából kezeli addig, amíg ennek jogi lehetősége vagy szükségessége fennáll. Ezt követően az Ltv. szerint levéltárba adandó iratokban foglalt adatok és az iratkezelési rendszerben a jogszabálynál fogva kezelendő személyes adatok kivételével a hatóság az adatot törli, illetve - adott esetben a lefoglalt adathordozót visszaszolgáltatva – az adatkezelést megszünteti. A levéltárba adással (főszabály szerint 15 év elteltével) a személyes adatok kezelése a Hatóságnál megszűnik.

Címzettek kategóriái	1. amennyiben az adott eljárásban a tényállás tisztázásához vagy a döntéshozatalhoz szükséges más hatóság, szerv vagy személy megkeresése, a Hatóság – a megkeresés teljesítéséhez feltétlenül szükséges mértékben -- személyes adatot közölhet - a megkeresett magyar hatósággal, szervvel vagy más EU-tagállamnak az (EU) 2016/679 rendelet szerinti felügyeleti hatóságával, - az (EU) 2016/679 rendelet 56. cikke és VII. fejezete szerinti eljárásokban más EU-tagállam felügyeleti hatósága, az Európai Adatvédelmi Testülettel (a továbbiakban: Testület), illetve a Testület Titkárságával és az Európai Unió Bizottságával, - az adott eljárásban vizsgált adatkezelővel, adatfeldolgozóval, az adattovábbítás címzettjével; 2. a hatósági eljárás ügyfele az iratbetekintési joga gyakorlása keretében megismerheti a nem zártan kezelt személyes adatokat, 3. a hatóság cselekményével szembeni perben eljáró bíróság
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

5. konzultációkérésre, állásfoglalás kiadása, jogszabály-véleményezés iránti megkeresésre vonatkozó, vagy máshol külön nem említett ügyben történő adatkezelés	
Adatkezelés célja	Infotv.38. § (2) bek., (4) bek d) pontja és (EU) 2016/679 rendelet 57. cikk (1) bek. c)-e) pont szerinti feladatok ellátása
Érintettek kategóriái	a hatóság eljárását tevékenységét kezdeményező vagy annak címzettjeként megjelenő természetes személy (cég, egyéb szervezet képviselője, kapcsolattartója)
Személyes adatok kategóriái	az érintett neve és elérhetősége (esetlegesen egyéb olyan személyazonosító adata, amelyeket a kezdeményezéskor megad)
A különböző adatkategóriák törlésére előirányzott határidők	Az ügyhöz kapcsolódó iratokat a Hatóság a közfeladatot ellátó szervek iratkezelésére vonatkozó jogszabályi követelmények (Ltv., illetve a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet) szerint iktatja, és az iktatott iratok között az irat irattári tervben meghatározottak szerinti selejtezéséig, illetve – ennek hiányában – levéltárba adásáig kezeli. Az adatok a konzultáció lezárást követően a Hatóság zárolja (korlátozott adatkezelés). Az adatokat az iratokkal együtt selejtezésig, illetve levéltárba adásig kezeli a Hatóság archiválási céllal. Ezt követően az Ltv. szerint levéltárba adandó iratokban foglalt adatok és az iratkezelési rendszerben a jogszabálynál fogva kezelendő személyes adatok kivételével a hatóság az adatot törli (iratokat selejtezi), illetve a levéltárba adással (főszabály szerint 15 év elteltével) a személyes adatok kezelése a Hatóságnál megszűnik.
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

6. Nemzetközi bűnügyi ügyekhez kapcsolódó adatkezelések (SIS, VIS, Eurodac, Europol, TFTP)	
Adatkezelés célja	A Hatóság jogszabályban meghatározott felügyeleti feladatainak ellátása [Nemzetközi bűnügyi ügyekhez kapcsolódó adatkezelések (SIS, VIS, Eurodac, Europol, TFTP)]
Érintettek kategóriái	az eljárást kezdeményezők, az eljárással érintett harmadik személyek, az eljárásban részt vevő harmadik személyek
Személyes adatok kategóriái	név, személyazonosító adatok, elérhetőségi adatok (cím, e-mail cím, e-kapcsolattartási cím, telefon/faxszám, adószám, beosztás, ezen túlmenően minden egyéb információ, melyet a természetes személy a Hatóság rendelkezésére bocsát, ami különleges adatot, továbbá bűnügyi személyes adatot is tartalmazhat)
A különböző adatkategóriák törlésére előirányzott határidők	Az adatokat tartalmazó dokumentumokat (adathordozókat) a közfeladatot ellátó szervek iratkezelésére vonatkozó jogszabályi követelmények (köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény (Ltv.), illetve a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet) szerint iktatja, és az iktatott iratok között az irat irattári tervben meghatározottak szerinti selejtezéséig, illetve – ennek hiányában – levéltárba adásáig kezeli. Az adatokat az ügy lezárását (eljárás megszüntetése, ellenőrzés lezárása hatósági eljárás megindítása nélkül, jelentés készítése, ajánlás, felszólítás kiadása, határozat hozatala) követően a Hatóság zárolja (az adatkezelést korlátozza), azok az ügyet lezáró ajánlás, felszólítás vagy hatósági döntés végrehajtása, a döntésben foglaltak ellenőrzése vagy a döntéssel összefüggő jogorvoslat vagy döntés-felülvizsgálat céljából kezeli addig, amíg ennek jogi lehetősége vagy szükségessége fennáll. Ezt követően az Ltv. szerint levéltárba adandó iratokban foglalt adatok és az iratkezelési rendszerben a jogszabálynál fogva kezelendő személyes adatok kivételével a hatóság az adatot törli, illetve - adott esetben a lefoglalt adathordozót visszaszolgáltatva – az adatkezelést megszünteti. A levéltárba adással (főszabály szerint 15 év elteltével) a személyes adatok kezelése a Hatóságnál megszűnik.

Címzettek kategóriái	adatkezelést végző szervek, felügyeleti hatóságok, SIRENE Iroda, Rendőrség, 1. amennyiben az adott eljárásban a tényállás tisztázásához vagy a döntéshozatalhoz szükséges más hatóság, szerv vagy személy megkeresése, a Hatóság -- a megkeresés teljesítéséhez feltétlenül szükséges mértékben -- személyes adatot közölhet - a megkeresett magyar hatósággal, szervvel vagy más EU-tagállamnak az (EU) 2016/679 rendelet szerinti felügyeleti hatóságával, - az (EU) 2016/679 rendelet 56. cikke és VII. fejezete szerinti eljárásokban más EU-tagállam felügyeleti hatósága, az Európai Adatvédelmi Testülettel (a továbbiakban: Testület), illetve a Testület Titkárságával és az Európai Unió Bizottságával, - az adott eljárásban vizsgált adatkezelővel, adatfeldolgozóval, az adattovábbítás címzettjével; 2. a hatósági eljárás ügyfele az iratbetekintési joga gyakorlása keretében megismerheti a nem zártan kezelt személyes adatokat, 3. a hatóság cselekményével szembeni perben eljáró bíróság
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	Amennyiben az adott eljárásban a tényállás tisztázásához vagy a döntéshozatalhoz szükséges más harmadik országbeli hatóság, szerv vagy személy, illetve nemzetközi szervezet megkeresése, a Hatóság -- a megkeresés teljesítéséhez feltétlenül szükséges mértékben -- személyes adatot közölhet a megkeresett magyar hatósággal, szervvel
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

7. közérdekű adatigénylések nyilvántartása	
Adatkezelés célja	a közérdekű és közérdekből nyilvános adatok igénylésével és továbbításával kapcsolatos nyilvántartás, az egy éven belül ismétlődő azonos tárgykörben, azonos adatigénylőtől érkező kérések kiszűrése céljából
Érintettek kategóriái	adatigénylést benyújtó ügyfél
Személyes adatok kategóriái	igénylő neve, értesítési címe (e-mail, postacím, www.kimittud.atlatszo.hu-n regisztrált e-mail cím), benyújtott adatigénylés adatköre
A különböző adatkategóriák törlésére előirányzott határidők	Az adatigénylésre vonatkozó adatok a beérkezést követő 1 év elteltével törlésre kerülnek. A beérkezett adatigénylések (ügyféli beadvány) adatkezelési időtartamát a Hatóság általános iratkezelési szabályzata határozza meg.
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

8.	belső adatvédelmi felelősök nyilvántartása
Adatkezelés célja	kapcsolattartás a bejelentett belső adatvédelmi felelősökkel [Infotv. 25. § (5)-(6)]
Érintettek kategóriái	bejelentett adatvédelmi felelősök
Személyes adatok kategóriái	név, postai és elektronikus levélcím, telefonszám
A különböző adatkategóriák törlésére előirányzott határidők	a belső adatvédelmi felelős e megbízatásának megszűnéséről való tudomásszerzésig
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

9. bejelentett adatvédelmi tisztviselők nyilvántartása	
Adatkezelés célja	kapcsolattartás a bejelentett adatvédelmi tisztviselőkkel, bejelentési kötelezettség teljesítésének ellenőrzése [(EU) 2016/679 rendelet 37. cikk]
Érintettek kategóriái	a bejelentésre szolgáló elektronikus rendszert használni kívánó regisztráló, a nyilvántartásba bejelentést tevő, az adatvédelmi tisztviselő, a bejelentett adatvédelmi tisztviselőt kijelölő adatkezelő/adatfeldolgozó
Személyes adatok kategóriái	- a regisztráló: felhasználó neve, e-mail címe, jelszava; - a bejelentő: neve, e-mail címe, telefonszáma, - az adatvédelmi tisztviselő: neve, levelezési címe, e-mail címe, telefonszáma; - a bejelentett adatvédelmi tisztviselőt kijelölő adatkezelő/adatfeldolgozó: neve, lakcíme, e-mail címe; a rendszer által naplózott adatok: IP cím, bejelentkezés időpontja
A különböző adatkategóriák törlésére előirányzott határidők	A bejelentést a közfeladatot ellátó szervek iratkezelésére vonatkozó jogszabályi követelmények (köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény (Ltv.), illetve a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet) szerint iktatja, és az iktatott iratok között az irat irattári tervben meghatározottak szerinti selejtezéséig, illetve – ennek hiányában – levéltárba adásáig kezeli. Ezt követően az Ltv. szerint levéltárba adandó iratokban foglalt adatok és az iratkezelési rendszerben a jogszabálynál fogva kezelendő személyes adatok kivételével a hatóság az adatot törli, illetve - adott esetben a lefoglalt adathordozót visszaszolgáltatva – az adatkezelést megszünteti. A levéltárba adással (főszabály szerint 15 év elteltével) a személyes adatok kezelése a Hatóságnál megszűnik. Az adatkezelő/adatfeldolgozó, valamint a tisztviselő adatainak kezelése tekintetében a fentiektől a Hatóság eltérhet, amennyiben bármely bejelentés vonatkozásában az adott adat még releváns. A bejelentésre szolgáló rendszerbe regisztráló adatainak törlésére a hozzájárulásának visszavonásakor kerül sor. Az IP cím és a bejelentkezés időpontjának automatikus törlésére a keletkezésüktől számított 6. hónap eltelte után kerül sor.
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–

Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

10. Minősített adat kezelésével, felhasználásával összefüggő adatkezelés	
Adatkezelés célja	- minősített adat birtokban tartásával kapcsolatban: igazolatlan távollét, jogviszony megszűnés esetén az elszámoltathatóság, - érintett feladatai ellátásához nemzetközi kötelezettségvállalás alapján biztonsági ellenőrzéssel védendő adatok megismerése, - rendelkezési jogosultságok meghatározása, - titoktartási nyilatkozat, felhasználói engedély nyilvántartása, adminisztrálása - a Hatósághoz érkező nemzeti és külföldi minősített küldemények átvételére jogosító meghatalmazás
Érintettek kategóriái	A Hatóság azon munkatársai, illetve közreműködő, akik nemzetbiztonsági ellenőrzés alá eső munkakört töltenek be, illetve akiknek a hatóságnál személyi biztonsági tanúsítványa van, biztonsági vezető, rendszerbiztonsági felügyelő, rendszeradminisztrátor, nyilvántartó munkatársa
Személyes adatok kategóriái	- felhasználói engedély: természetes személyazonosító adatok, nyilvántartási száma, kelte, érvényességi ideje, legmagasabb minősítési szint; - titoktartási nyilatkozat: név, lakcím, felhasználói engedély száma, kiállításának dátuma, aláírás, ennek dátuma; - Személyi biztonsági tanúsítvány: természetes személyazonosító adatok, beosztás, állampolgárság, nyilvántartási száma, kelte, érvényességi ideje, legmagasabb megismerhető minősítési szint biztonsági vezető, rendszerbiztonsági felügyelő, rendszeradminisztrátor: neve, telefonszáma, fax száma, e-mail címe, személyi biztonsági tanúsítványának száma, érvényességi ideje - nyilvántartó munkatársának aláírásmintája
A különböző adatkategóriák törlésére előirányzott határidők	- a felhasználói engedély és a titoktartási nyilatkozat esetén 90/2010. (III. 26.) Korm. rendelet 15. § (4) bek.: 1978. évi IV. törvény (régi Btk.) 221. § szerinti visszaélés szigorúan titkos és titkos minősítésű adattal, ill. 2012. évi C. törvény (Btk.) 265. § szerinti minősített adattal visszaélés bűncselekményre meghatározott büntetési tétel felső határának megfelelő ideig (15. ill. 8 év), ezt követően selejtezés és törlés kötelező. - személyes biztonsági tanúsítvány esetén 90/2010. (III. 26.) Korm. rendelet 10. § (4) bek., ill. 11. § (8) a személyi biztonsági tanúsítvány visszavonásáig vagy érvényességi ideje lejártáig, ezt követően selejtezni, és törölni kell; - biztonsági vezető, rendszerbiztonsági felügyelő, rendszeradminisztrátor, nyilvántartó munkatársa e feladatának megszűnéséig

Címzettek kategóriái	A személyi biztonsági tanúsítvány: a minősített adattal kapcsolatos vizsgálati eljárásban, titokfelügyeleti hatósági eljárásban az ügyfél (minősítő). A biztonsági vezető, rendszerbiztonsági felügyelő, rendszeradminisztrátor elérhetőségei: a rendszerengedély-, illetve minősített adat kezelésének engedélyezésének kérelme végett a Nemzeti Biztonsági Felügyelet. A biztonsági vezető elérhetőségei: EU Központi Nyilvántartó. A nyilvántartó munkatársainak aláírásmintája: EU Központi Nyilvántartó és az Állami Futárszolgálat nemzeti vagy külföldi minősített küldemény átvételének, átadásának igazolására.
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

11. nemzetbiztonsági ellenőrzéssel kapcsolatos adatkezelés	
Adatkezelés célja	Nemzetbiztonsági ellenőrzés kezdeményezéséhez, Nemzetbiztonsági kérdőív és a nemzetbiztonsági ellenőrzéssel összefüggésben a lényeges adatokban bekövetkezett változás bejelentéséhez kapcsolódó adminisztratív teendők,
Érintettek kategóriái	- A Hatóság azon munkatársai, akik nemzetbiztonsági ellenőrzés alá eső munkakört töltenek be, - biztonsági megbízott
Személyes adatok kategóriái	- természetes személyazonosító adatok, állampolgárság - biztonsági szakvélemény: Nbtv. 71/C. § (1) bek. szerinti adatok - biztonsági megbízott neve, személyi igazolvány száma, BIM mobil telefonszáma, e-mail címe
A különböző adatkategóriák törlésére előirányzott határidők	kezdeményezés, változásbejelentés esetén: általános iratkezelési szabályok szerint selejtezésig, biztonsági szakvélemény esetén: érvényességi idejének lejártáig, biztonsági megbízott tekintetében: általános iratkezelési szabályok szerint selejtezésig
Címzettek kategóriái	Nemzetbiztonsági szolgálat (Alkotmányvédelmi Hivatal)
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

12. biztonsági területre belépés adminisztrálásával összefüggő adatkezelés	
Adatkezelés célja	a biztonsági területre belépéshez, az elektronikus jelzőrendszer élesítéséhez, hatástalanításához szükséges kulcsok (kulcsdoboz), tartalékkulcsok, kódok és kódcserék nyilvántartásával, adminisztrálásával kapcsolatos feladatok
Érintettek kategóriái	A Hatóság azon munkatársai, akik a biztonsági területre jogosultak belépni, illetve akik a biztonsági tároló kulcsdobozainak átadására (reagáló erő) és átvételére jogosultak
Személyes adatok kategóriái	- kulcsdoboz megnevezése, felvételére jogosultak személye - kulcsdoboz megnevezése, felvevő személy olvasható aláírása, felvétel dátuma, időpontja, leadás ideje, visszaadó olvasható aláírása, visszavevő olvasható aláírása, visszaadás dátuma, időpontja - kulcsok, kódok esetén: név, jogosultsági kód - Számkombinációk és kódok megváltoztatásának ténye, valamint időpontja
A különböző adatkategóriák törlésére előirányzott határidők	általános iratkezelési szabályok szerint selejtezésig
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

13. a közszolgálati jogviszony létesítése feltételeinek ellenőrzése	
Adatkezelés célja	a közszolgálati jogviszony létesítése feltételeinek ellenőrzése
Érintettek kategóriái	a Hatóságnál közszolgálati jogviszonyt létesíteni szándékozók
Személyes adatok kategóriái	a Kttv. 39-42. §-ában meghatározott adatok, ideértve a bűnügyi előéletre vonatkozó személyes adatokat tartalmazó, a bűnügyi nyilvántartó szerv által kiállított hatósági bizonyítványt is
A különböző adatkategóriák törlésére előirányzott határidők	jogviszony létesítéséről meghozott döntés időpontja vagy - közszolgálati jogviszony létesítése és fennállása esetén - a közszolgálati jogviszony megszűntetésétől ötven év, a bűnügyi személyes adatok tekintetében a közszolgálati jogviszony megszüntetése
Címzettek kategóriái	a jogviszony létesítése és fennállása esetén a Kttv. 180. § (1) bekezdésében meghatározott címzettek
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

14. közszolgálati alapnyilvántartás	
Adatkezelés célja	a közszolgálati jogviszonyból származó jogok gyakorlásához és kötelezettségek teljesítéséhez szükséges adatok kezelésének biztosítása a közszolgálati jogviszony alanyai számára
Érintettek kategóriái	a Hatóság köztisztviselői állománya
Személyes adatok kategóriái	a Kttv. 2. mellékletében meghatározott adatkör
A különböző adatkategóriák törlésére előirányzott határidők	a jogviszony megszűnésétől számított ötven év
Címzettek kategóriái	a Kttv. 180. §-181. §-ában meghatározott címzettek
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

15. személyi anyag	
Adatkezelés célja	a közszolgálati jogviszonyból származó jogok gyakorlásához és kötelezettségek teljesítéséhez szükséges adatok kezelésének biztosítása a közszolgálati jogviszony alanyai számára
Érintettek kategóriái	a Hatóság köztisztviselői állománya
Személyes adatok kategóriái	a Kttv. 184. § (1) bekezdésében meghatározott adatkör
A különböző adatkategóriák törlésére előirányzott határidők	a jogviszony megszűnésétől számított ötven év
Címzettek kategóriái	a Kttv. 180. § (1) bekezdésében meghatározott címzettek
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

16. munkaviszonyban állók (munkavállalók) személyügyi nyilvántartása	
Adatkezelés célja	a munkaviszonyból származó jogok gyakorlásához és kötelezettségek teljesítéséhez szükséges adatok kezelésének biztosítása a munkaviszony alanyai számára
Érintettek kategóriái	a Hatóság munkavállalói állománya
Személyes adatok kategóriái	a munkaviszony létesítéséhez és fenntartásához szükséges adatok
A különböző adatkategóriák törlésére előirányzott határidők	a munkaszerződések selejtezésének időpontja a munkaviszony megszűnését követő 50 év
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

17. Személyi anyag	
Adatkezelés célja	jogviszony megszűnésével, megszűntetésével kapcsolatos adatkezelés
Érintettek kategóriái	A Hatóság köztisztviselői, munkavállalói állománya.
Személyes adatok kategóriái	Kttv. 177. § (1) bekezdésében foglaltak értelmében, a törvény 2. számú melléklet, illetve az Mt. 10.§ (2) bekezdésében foglaltak alapján
A különböző adatkategóriák törlésére előirányzott határidők	a munkaszerződések selejtezésének időpontja a munkaviszony megszűnését követő 50 év
Címzettek kategóriái	Más közigazgatási szerv.
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

18. munkabalesetek nyilvántartása	
Adatkezelés célja	a több mint három munkanapon át munkaképtelenséget okozó munkabalesetek, valamint a foglalkozási megbetegedések és a fokozott expozíciós esetek jogkövetkezményeinek alkalmazásához, azok megelőzéséhez szükséges információk rendelkezésre állása
Érintettek kategóriái	a Hatóság köztisztviselői, munkavállalói állománya
Személyes adatok kategóriái	a munkavédelemről szóló 1993. évi XCIII törvény 64. § (3) bekezdése, 1. számú melléklete; a munkavédelemről szóló 1993. évi XCIII. törvény egyes rendelkezéseinek végrehajtásáról szóló 5/1993. (XII. 26.) MüM rendelet 5. §
A különböző adatkategóriák törlésére előirányzott határidők	a munkavédelemről szóló 1993. évi XCIII. 67. §-a szerinti 3 év elévülési idő lejártát követően
Címzettek kategóriái	munkavédelmi hatóság
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

19. szociális segélykérelmekkel, kegyeleti gondoskodással kapcsolatos nyilvántartás	
Adatkezelés célja	visszatérítendő, illetve vissza nem térítendő szociális jóléti, kulturális, egészségügyi juttatás nyújtásához és elszámolásához szükséges információk rendelkezésre állása
Érintettek kategóriái	a Hatóság köztisztviselői állománya
Személyes adatok kategóriái	a Kttv. 152. §-153/A. §-ban meghatározott egyéb juttatások nyújtásához és elszámolásához kapcsolódó adatok
A különböző adatkategóriák törlésére előirányzott határidők	a juttatások, illetve azok elszámolásához kapcsolódó jogi igények elévülésének időpontja (5 év)
Címzettek kategóriái	lakás építéséhez, vásárlásához hitelintézettől igényelt állami kamattámogatású kölcsön, állami kezességvállalás esetén a köztisztviselővel szerződő hitelintézet, állami adóhatóság [Kttv. 153. §-153/A. §]
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

20. vagyonnyilatkozat-tételi kötelezettséggel érintettek nyilvántartása	
Adatkezelés célja	z alapvető jogok és kötelességek pártatlan és elfogulatlan érvényesítése, valamint a közélet tisztaságának biztosítása és a korrupció megelőzése
Érintettek kategóriái	a Hatóság vagyonnyilatkozat-tételi kötelezettséggel érintett köztisztviselői és azok hozzátartozói
Személyes adatok kategóriái	az egyes vagyonnyilatkozat-tételi kötelezettségekről 2007. évi CLII. törvény mellékletében meghatározott adatkör
A különböző adatkategóriák törlésére előirányzott határidők	a vagyonnyilatkozat-tételi kötelezettség megszűnésétől számított 8 nap
Címzettek kategóriái	áthelyezés esetén a fogadó közigazgatási szerv, állami adóhatóság
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

21. munkába járás költségnyilvántartása	
Adatkezelés célja	a munkába járás költségeinek elszámolása
Érintettek kategóriái	a Hatóság köztisztviselői és munkavállalói állománya
Személyes adatok kategóriái	a munkába járással kapcsolatos utazási költségtérítést igénybe vevő köztisztviselők és munkavállalók neve, állandó lakcíme és tartózkodási helye
A különböző adatkategóriák törlésére előirányzott határidők	a tárgyévet követő nyolcadik év december 31.
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

22. utazási kedvezmények nyilvántartása	
Adatkezelés célja	utazási kedvezmény biztosítása
Érintettek kategóriái	a Hatóság köztisztviselői, munkavállalói állománya
Személyes adatok kategóriái	a munkatárs neve
A különböző adatkategóriák törlésére előirányzott határidők	a tárgyévet követő év március 31.
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

23.	**béren kívüli juttatások nyilvántartása**
Adatkezelés célja	a béren kívüli juttatások biztosítása
Érintettek kategóriái	a Hatóság köztisztviselői, munkavállalói állománya
Személyes adatok kategóriái	a munkatárs neve, adószáma
A különböző adatkategóriák törlésére előirányzott határidők	a tárgyévet követő nyolcadik év december 31.
Címzettek kategóriái	áthelyezés esetén a fogadó közigazgatási szerv
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

	24. bélyegzők nyilvántartása
Adatkezelés célja	a Hatóság bélyegzői használatára jogosult munkatársak azonosítása
Érintettek kategóriái	a hatóság köztisztviselői és munkavállalói állománya
Személyes adatok kategóriái	a munkatárs neve
A különböző adatkategóriák törlésére előirányzott határidők	a bélyegző visszavétele évének december 31. napja
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

25.	kiküldetési rendelvények nyilvántartása
Adatkezelés célja	a Hatóság munkatársai külföldi kiküldetése teljesítésének elősegítése
Érintettek kategóriái	a hatóság köztisztviselői és munkavállalói állománya
Személyes adatok kategóriái	a munkatárs neve, állandó lakcíme vagy tartózkodási helye
A különböző adatkategóriák törlésére előirányzott határidők	a tárgyévet követő nyolcadik év december 31.
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

26. leltározás nyilvántartása	
Adatkezelés célja	az éves leltározás végrehajtása
Érintettek kategóriái	leltározási tevékenységben résztvevők
Személyes adatok kategóriái	a munkatárs neve
A különböző adatkategóriák törlésére előirányzott határidők	a leltári tárgy visszavétele évének december 31. napja
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

27. leltárfelelősök nyilvántartása	
Adatkezelés célja	tárolási hely alapú nyilatkozatok (személyi leltár) nyomon követhetősége
Érintettek kategóriái	személyes használatra kiadott eszközök használói
Személyes adatok kategóriái	a munkatárs neve
A különböző adatkategóriák törlésére előirányzott határidők	a tárgyévet követő nyolcadik év december 31.
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

28.	társadalombiztosítási nyilvántartások
Adatkezelés célja	társadalombiztosítással összefüggő nyilvántartás
Érintettek kategóriái	a Hatóság köztisztviselői, munkavállalói állománya
Személyes adatok kategóriái	a társadalombiztosítás ellátásaira és a magánnyugdíjra jogosultakról, valamint e szolgáltatások fedezetéről szóló 1997. évi LXXX. törvény 42. §-ában meghatározott adatkör
A különböző adatkategóriák törlésére előirányzott határidők	a tárgyévet követő nyolcadik év december 31.
Címzettek kategóriái	a társadalombiztosítás ellátásaira és a magánnyugdíjra jogosultakról, valamint e szolgáltatások fedezetéről szóló 1997. évi LXXX. törvény 43. §-ában meghatározott címzettek
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

29.	Számfejtett illetmények nyilvántartása
Adatkezelés célja	a Hatóság munkatársai illetményének számfejtése a Központosított Illetmény-számfejtési Rendszeren (KIRA) keresztül
Érintettek kategóriái	a Hatóság köztisztviselői, munkavállalói állománya
Személyes adatok kategóriái	Kttv. 2. számú mellékletében felsorolt adat, az illetményszámfejtéshez szükséges adat
A különböző adatkategóriák törlésére előirányzott határidők	a jogviszony megszűnésétől számított ötven év
Címzettek kategóriái	áthelyezés esetén a fogadó közigazgatási szerv
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

30. Gazdálkodási rendszer nyilvántartása (Ecostat - integrált ügyviteli rendszer)	
Adatkezelés célja	a Hatóság gazdálkodásával összefüggő jogviszonyok nyomon követhetősége és elszámolása
Érintettek kategóriái	a hatóság gazdálkodásával kapcsolatos belső és külső szereplők, magánszemélyek, egyéni és társas vállalkozások, költségvetési szervek, egyéb szervezetek
Személyes adatok kategóriái	a Hatóság gazdálkodása során azzal jogviszonyt létesítő magánszemélyek, egyéni és társas vállalkozások, költségvetési szervek, egyéb szervezetek kapcsolattartói, képviselői személyazonosító adatai
A különböző adatkategóriák törlésére előirányzott határidők	a tárgyévet követő nyolcadik év december 31.
Címzettek kategóriái	Computrend Kft. (üzemeltető)
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

31. Kincstári átutalások nyilvántartása (Giro utalási rendszer)	
Adatkezelés célja	a Hatóság gazdálkodásával összefüggő jogviszonyok nyomon követhetősége és elszámolása
Érintettek kategóriái	a hatósági köztisztviselői és munkavállalói állománya, valamint a Hatósággal annak gazdálkodása körében jogviszonyt létesítő természetes személyek
Személyes adatok kategóriái	név, bankszámlaszám, lakcím
A különböző adatkategóriák törlésére előirányzott határidők	a tárgyévet követő nyolcadik év december 31.
Címzettek kategóriái	Magyar Államkincstár, az átutalási megbízást fogadó bankok
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

32. Munkaügyi nyilvántartások (Jdolber Humánügyi rendszer)	
Adatkezelés célja	a Hatóság által foglalkoztatottak közszolgálati, illetve munkaviszonnyal összefüggő adminisztráció elősegítése
Érintettek kategóriái	a Hatóság köztisztviselői, munkavállalói állománya
Személyes adatok kategóriái	Kttv. 2. számú mellékletében meghatározott adatkör, a munkajogviszony létesítéséhez, fenntartásához és megszüntetéséhez szükséges adatok
A különböző adatkategóriák törlésére előirányzott határidők	a jogviszony megszűnésétől számított ötven év
Címzettek kategóriái	Az OrgWare Kft. (üzemeltető), a köztisztviselők áthelyezése esetén a fogadó közigazgatási szerv
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

33. Kamerás őrzési védelmi rendszer	
Adatkezelés célja	Fizikai biztonság (adat- és vagyonvédelem) garantálása, illetve annak sérülése esetén a jogkövetkezmények megállapításának lehetővé tétele
Érintettek kategóriái	az egyes kamerák által megfigyelt területre belépők
Személyes adatok kategóriái	képmás, helyszín / CAM ID, időpont
A különböző adatkategóriák törlésére előirányzott határidők	3 nap (a megfigyelés kapcsán észlelt incidens esetén a szükséges eljárások lefolytatásáig)
Címzettek kategóriái	---
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

34. Épületfelügyeleti rendszer	
Adatkezelés célja	Épületüzemeltetéssel kapcsolatos elektronikus rendszerekhez hozzáférési jogosultságok nyilvántartása; fizikai biztonság (vagyonvédelem)
Érintettek kategóriái	hozzáférési jogosultsággal rendelkezők
Személyes adatok kategóriái	user id, név, jogosultság, kiadás, módosítás, visszavonás dátuma
A különböző adatkategóriák törlésére előirányzott határidők	a hozzáférési jogosultsággal rendelkező munkavállaló munkaviszonya megszűnése
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

35. Behatolásjelző rendszer	
Adatkezelés célja	a behatolásjelző rendszerhez hozzáférési jogosultságok nyilvántartása, fizikai biztonság (adat- és vagyonvédelem) garantálása, illetve annak sérülése esetén a jogkövetkezmények megállapításának lehetővé tétele
Érintettek kategóriái	hozzáférési jogosultsággal rendelkezők
Személyes adatok kategóriái	user id, név, jogosultság, kiadás, módosítás, visszavonás dátuma, belépés időpont, művelet
A különböző adatkategóriák törlésére előirányzott határidők	a hozzáférési jogosultsággal rendelkező munkavállaló munkaviszonya megszűnése
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

36. Tűzvédelmi rendszer	
Adatkezelés célja	a tűzvédelem elektronikus eszközeihez hozzáférési jogosultságok nyilvántartása, fizikai biztonság (személy- és vagyonvédelem), illetve annak sérülése esetén a jogkövetkezmények megállapításának lehetővé tétele
Érintettek kategóriái	hozzáférési jogosultsággal rendelkezők
Személyes adatok kategóriái	user id, név, jogosultság, kiadás, módosítás, visszavonás dátuma, belépés időpont, művelet
A különböző adatkategóriák törlésére előirányzott határidők	a hozzáférési jogosultsággal rendelkező munkavállaló munkaviszonya megszűnése
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

37. NAIH elektronikus belépőkártyák nyilvántartása	
Adatkezelés célja	NAIH foglalkoztatottak állandó belépőkártyáinak, és a vendégek rendszeres vagy eseti belépésre szolgáló belépőkártya-használatának nyilvántartása annak érdekében, hogy az épületbe csak az arra jogosultak tartózkodjanak; vagyon- és személyvédelem, minősített adatok és egyéb védett adatok, személyes adatok védelme, a munkavégzés zavartalanságának biztosítása, illetve a védelem sérülése esetén a jogkövetkezmények megállapításának lehetővé tétele
Érintettek kategóriái	köztisztviselők, munkavállalók, időszaki belépési engedélyt kapó egyéb személyek
Személyes adatok kategóriái	fizikai kártyaszám, név, szervezeti egység, jogosultság (belépési pontok), aláírás
A különböző adatkategóriák törlésére előirányzott határidők	jogviszony megszűnése, ill. belépési jogosultság megszűnése
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

38. parkolási engedélyek nyilvántartása	
Adatkezelés célja	a Hatóság parkolója használatának csak az arra jogosultak részére való megengedése
Érintettek kategóriái	a Hatóság székhelye parkolójának használatára jogosultak
Személyes adatok kategóriái	fizikai kártyaszám, név
A különböző adatkategóriák törlésére előirányzott határidők	a parkolási jogosultság megszűnése
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

39. Elektronikus beléptető rendszer	
Adatkezelés célja	NAIH foglalkoztatottak állandó belépőkártyáinak, és a vendégek rendszeres vagy eseti belépésre szolgáló belépőkártya-használatának nyilvántartása annak érdekében, hogy az épületbe csak az arra jogosultak tartózkodjanak; vagyon- és személyvédelem, minősített adatok és egyéb védett adatok, személyes adatok védelme, a munkavégzés zavartalanságának biztosítása, illetve a védelem sérülése esetén a jogkövetkezmények megállapításának lehetővé tétele
Érintettek kategóriái	köztisztviselők, munkavállalók, belépési engedélyt kapó egyéb személyek
Személyes adatok kategóriái	fizikai kártyaszám, név, helyszín, mozgásirány, idő
A különböző adatkategóriák törlésére előirányzott határidők	- állandó és időszakos kártya: 6 hónap, - vendég, ideiglenes kártya: 24 óra
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

40. parkolóhasználat nyilvántartása	
Adatkezelés célja	a Hatóság parkolója használatának csak az arra jogosultak részére való megengedése
Érintettek kategóriái	a Hatóság székhelye parkolójának használatára jogosultak
Személyes adatok kategóriái	fizikai kártyaszám, mozgásirány, idő
A különböző adatkategóriák törlésére előirányzott határidők	6 hónap
Címzettek kategóriái	
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

41. NAIH hatósági intézkedésre jogosító szolgálati igazolvány, munkáltatói igazolványok nyilvántartása	
Adatkezelés célja	köztisztviselői és munkavállalói hatósági igazolványok tekintetében a biztonsági okmányokra vonatkozó követelmények érvényesítése
Érintettek kategóriái	köztisztviselők, munkavállalók
Személyes adatok kategóriái	Név, fénykép, beosztás, igazolvány szám, kiadás dátuma, visszavonás dátuma
A különböző adatkategóriák törlésére előirányzott határidők	visszavonás / jogviszony megszűnése után megsemmisítésig
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

42. IT rendszer jogosultságok kezelésével összefüggő adatkezelések	
Adatkezelés célja	az egyes informatikai rendszerekhez való hozzáférési jogosultságok adminisztrálása az informatikai biztonság garantálása, illetve annak sérülése esetén a jogkövetkezmények megállapításának lehetővé tétele érdekében: - e-mail fiókok, - NAS hozzáférés, - iratkezelő rendszerbeli jogosultságok, - privilegizált felhasználói jogosultságok
Érintettek kategóriái	köztisztviselők, munkavállalók, egyes szakrendszerekhez egyedi engedéllyel hozzáférő külső személyek.
Személyes adatok kategóriái	- e-mail fiókok: név, user id, password, szervezeti egység, e-mail cím, kiadás, módosítás, visszavonás dátuma, - NAS hozzáférés: név, user id, password, szervezeti egység, SAMBA user ID, felh. Jog, kiadás, módosítás, visszavonás dátuma, - iratkezelő rendszerbeli jogosultságok: név, user id, password, szervezeti egység, jogosultsági szint, kiadás, módosítás, visszavonás dátuma, - privilegizált felhasználói jogosultságok: név, user id, password, server ID, jogosultsági szint, kiadás, módosítás, visszavonás dátuma,
A különböző adatkategóriák törlésére előirányzott határidők	hozzáférési jogosultság visszavonásáig / jogviszony fennállása alatt
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás

43. IT szakrendszeri jogosultságok kezelésével összefüggő adatkezelések	
Adatkezelés célja	A Hatóság által igénybevett szolgáltatásokkal összefüggő szerződéses kötelezettségek teljesítése (licenszek kiosztása): - Complex jogtár jogosultságok, - egyéb szakrendszeri jogosultság,
Érintettek kategóriái	köztisztviselők, munkavállalók, egyes szakrendszerekhez egyedi engedéllyel hozzáférő külső személyek.
Személyes adatok kategóriái	- szakrendszeri jogosultság: név, user id, password, szervezeti egység, szakrendszer, jogosultsági szint, kiadás, módosítás, visszavonás dátuma, - Complex jogtár jogosultságok: név, user id, password, szervezeti egység, jogosultsági szint, szolgáltatások, e-book, kiadás, módosítás, visszavonás dátuma
A különböző adatkategóriák törlésére előirányzott határidők	hozzáférési jogosultság visszavonásáig / jogviszony fennállása alatt
Címzettek kategóriái	–
A személyes adatok harmadik országba vagy nemzetközi szervezet részére történő továbbítására vonatkozó információk	–
Az adatbiztonság garantálása érdekében alkalmazott technikai és szervezési intézkedések leírása	A szükséges és megfelelő, komplex információbiztonsági szintet a következő intézkedések / szabályozó eszközök biztosítják, bizalmasság, sértetlenség és rendelkezésre állás tekintetében: • komplex fizikai védelmi intézkedések (kamerás megfigyelés, belépések elektronikus rendszerben való regisztrálása, behatolásjelző rendszer alkalmazása), • komplex adminisztratív és technikai védelmi intézkedések és szabályzók (informatikai biztonsági stratégia és politika, informatikai biztonsági szabályzat, a minősített adatok védelmére vonatkozó biztonsági szabályzat, illetve a belső adatvédelmi szabályzat), • A folyamatos kockázat feltárás és elemzés eredménye alapján a mindenkori védelmi intézkedések zárt, teljes körű, folytonos és a kockázattal arányos beavatkozási rendszere, • megfelelő erőforrás biztosítása, • személyi biztonsági intézkedések, • Képzés, tudatosítás