Országos Atomenergia Hivatal

Az Országos Atomenergia Hivatal adatvédelmi és adatbiztonsági szabályzata

Azonosító: SZ-11

6. kiadás

Jóváhagyta:

ORSZÁGOS ATOMENERGIA HIVATAL

Hollán Szabolcs
-3- főigazgató-helyettes

Budapest
2021

1. Az Adatvédelmi és Adatbiztonsági Szabályzat célja

Az Adatvédelmi és Adatbiztonsági Szabályzat (a továbbiakban: AASZ) célja, hogy biztosítsa az Országos Atomenergia Hivatal (OAH) által kezelt személyes adatok vonatkozásában az adatvédelem alkotmányos elveinek, az adatbiztonság követelményeinek érvényesülését, megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát, valamint meghatározza az OAH által vezetett, adatvédelemmel kapcsolatos nyilvántartások kezelésének rendjét.

Az AASZ a 3. pontban felsorolt jogszabályokban rögzített rendelkezésekkel együttesen értelmezendő és alkalmazandó.

2. Az AASZ hatálya

Az AASZ szervezeti hatálya kiterjed az OAH valamennyi szervezeti egységére – telephelytől függetlenül -, ahol személyes adatot kezelnek.

Az AASZ személyi hatálya kiterjed az OAH valamennyi szervezeti egységének munkatársára.

Az AASZ tárgyi hatálya kiterjed az OAH szervezeti egységeinél nyilvántartott valamennyi személyes adatra, a velük végzett adatkezelési műveletek teljes körére keletkezésük, felhasználásuk, feldolgozásuk helyétől, valamint megjelenési formájuktól függetlenül.

3. Az AASZ jogszabályi alapja, kapcsolata a belső szabályzatokkal

3.1. Az AASZ jogszabályi alapját többek között:

- az Európai Parlament és a Tanács 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 (GDPR);

- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény,

- az atomenergiáról szóló 1996. évi CXVI. törvény,

- a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. törvény,

- a kormányzati igazgatásról szóló 2018. évi CXXV. törvény (Kit.),

- a közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvény (Kttv.),

- a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről szóló 1995. évi LXVI. törvény,

- az államháztartásról szóló 2011. évi CXCV. törvény,

- a számvitelről szóló 2000. évi C. törvény,

- az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény,

- a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény (Szvtv.) rendelkezései biztosítják.

3.2. Az AASZ szorosan kapcsolódik az OAH alábbi belső szabályozó dokumentumaihoz:

SZ-02 Informatikai Biztonsági Szabályzat,

SZ-05 Egységes Közszolgálati Szabályzat,

SZ-06 Házirend,

ME-0-0-10 Iratkezelési Szabályzat,

ME-5-0-9 Szakmagyakorlási alkalmasság megállapítására irányuló eljárásrend.

3.3. Az AASZ alkalmazása során használatos alapfogalmak

Az AASZ alkalmazása során használatos alapfogalmak értelmezését az 1. Melléklet tartalmazza.

4. A személyes adatok kezelésére vonatkozó elvek

4.1. A személyes adatok:

a) kezelését jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni („jogszerűség, tisztességes eljárás és átláthatóság”);

b) gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés („célhoz kötöttség”);

c) az adatkezelés céljai szempontjából megfelelőek és relevánsak kell, hogy legyenek, és a szükségesre kell korlátozódniuk („adattakarékosság”);

d) pontosnak és szükség esetén naprakésznek kell lenniük; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék („pontosság”);

e) tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé; a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor, az érintettek jogainak és szabadságainak védelme érdekében előírt megfelelő technikai és szervezési intézkedések végrehajtására is figyelemmel („korlátozott tárolhatóság”);

f) kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („integritás és bizalmas jelleg”).

4.2. Az OAH adatkezeléseit úgy kell végezni, hogy azok megfeleljenek a 4.1. pontban foglaltaknak, továbbá az adatkezelőnek képesnek kell lennie e megfelelés igazolására („elszámoltathatóság”).

4.3. Az OAH adatkezelései során arra alkalmas műszaki vagy szervezési – így különösen az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisülésével

vagy károsodásával szembeni védelmet kialakító – intézkedések alkalmazásával biztosítani kell a személyes adatok megfelelő biztonságát.

4.4. Az OAH megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek.

5. Az adatkezelés jogalapja és általános feltételei

5.1. 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.

5.2. Különleges adat

a) az 5.1. pont bekezdés 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.

Az 5.1. pont a) alpontjában, az 5.2. pont b) alpontjában, valamint kötelező adatkezelés esetén a kezelendő adatok fajtáit, az adatkezelés célját és feltételeit, az adatok megismerhetőségét, az adatkezelő személyét, valamint az adatkezelés időtartamát vagy szükségessége időszakos felülvizsgálatát az adatkezelést elrendelő törvény, illetve önkormányzati rendelet határozza meg.

Különleges adatok kezelése esetén az OAH, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó megfelelő műszaki és szervezési intézkedésekkel biztosítja, hogy az adatkezelési műveletek végzése során a különleges adatokhoz kizárólag az rendelkezzen hozzáféréssel, akinek az adatkezelési művelettel összefüggő feladata ellátásához feltétlenül szükséges.

5.3. Az OAH jogosult az ügyfél és az eljárás egyéb résztvevője természetes személyazonosító adatainak és az ügyfajtát szabályozó törvényben meghatározott személyes adatok, továbbá - ha törvény másként nem rendelkezik - a tényállás tisztázásához elengedhetetlenül szükséges más személyes adatok megismerésére és kezelésére. A kérelemre induló eljárásban

vélelmezni kell, hogy a kérelmező ügyfél a tényállás tisztázásához szükséges személyes adatok - ideértve a különleges adatokat is - kezeléséhez hozzájárulást adott.

5.4.Ha az adatkezelést az OAH nevében más végzi, kizárólag olyan adatfeldolgozó vehető igénybe, aki vagy amely megfelelő garanciákat nyújt az adatkezelés GDPR-ban rögzített követelményeinek való megfelelését és az érintettek jogainak védelmét biztosító, megfelelő technikai és szervezési intézkedések végrehajtására. Az adatfeldolgozó által végzett adatkezelést az uniós jog vagy tagállami jog alapján létrejött olyan – az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó –szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az OAH-val szemben.

6. Az adattovábbítás feltételei

6.1. Az adattovábbítást megelőzően az OAH megvizsgálja a továbbítandó személyes adatok pontosságát, teljességét és naprakészségét; ha azt állapítja meg, hogy a továbbítandó adatok pontatlanok, hiányosak vagy már nem naprakészek, azokat kizárólag abban az esetben továbbíthatja, ha

a) az az adattovábbítás céljának megvalósulásához elengedhetetlenül szükséges, és

b) az adattovábbítással egyidejűleg tájékoztatja a címzettet az adatok pontosságával, teljességével és naprakészségével összefüggésben rendelkezésére álló információkról.

Ha az adattovábbítást követően jut az OAH tudomására, hogy az adattovábbítás törvényben, nemzetközi szerződésben vagy az Európai Unió kötelező jogi aktusában meghatározott feltételei nem teljesültek, arról a címzettet haladéktalanul értesíti.

6.2. Ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusának rendelkezése alapján az OAH személyes adatot akként vesz át, hogy az adattovábbító adatkezelő vagy adatfeldolgozó az adattovábbítással egyidejűleg jelzi a személyes adat kezelési feltételeit (például cél, időtartam, címzett) azokat e feltételeknek megfelelő terjedelemben és módon kezeli, az érintett jogait az adatkezelési feltételeknek megfelelően biztosítja. Az OAH adatátvevőként az adatkezelési feltételekre tekintet nélkül is kezelheti a személyes adatot és biztosíthatja az érintett jogait, ha ahhoz az adattovábbító adatkezelő előzetes jóváhagyását adta.

Ha törvény, nemzetközi szerződés vagy az Európai Unió kötelező jogi aktusának rendelkezése alapján az OAH adatkezelési feltételek alkalmazásának kötelezettségével kezel személyes adatot, annak továbbításával egyidejűleg tájékoztatja a címzettet az adatkezelési feltételekről és az azok alkalmazására vonatkozó jogi kötelezettségről.

6.3. Személyes adatot az OAH harmadik országban, továbbá nemzetközi szervezet keretein belül adatkezelést folytató adatkezelő vagy adatfeldolgozó részére – a közvetett adattovábbítást is ideértve –akkor továbbíthat, ha

a) a nemzetközi adattovábbításhoz az érintett kifejezetten hozzájárult, vagy

b) a nemzetközi adattovábbítás az adatkezelés céljának eléréséhez szükséges, valamint

ba) annak során az adatkezelésnek az 5. pontban rögzített feltételei teljesülnek, és

bb) a harmadik országban, illetve a nemzetközi szervezet keretein belül adatkezelést folytató adatkezelő vagy adatfeldolgozó tekintetében a továbbított személyes adatok megfelelő szintű védelme biztosított, vagy

c) a nemzetközi adattovábbítás

ca) az érintett vagy más személy létfontosságú érdekeinek védelme érdekében szükséges,

cb) valamely EGT-állam vagy harmadik ország közbiztonságát közvetlenül és súlyosan fenyegető veszély elhárítása érdekében szükséges,

cc) egyedi ügyben, eseti jelleggel az OAH által végzett vizsgálatok vagy eljárások hatékony és eredményes lefolytatása érdekében szükséges, és az nem jár az érintett alapvető jogainak aránytalan korlátozásával,

cd) egyedi ügyben, eseti jelleggel az érintett vagy más jogi igényeinek előterjesztése, érvényesítése, illetve védelme érdekében szükséges, és az nem jár az érintett jogainak aránytalan korlátozásával.

6.4. Olyan adatkezelés esetén, amelynél számolni kell külföldre irányuló adattovábbítással, az érintettek figyelmét erre a körülményre már az adatok felvétele előtt fel kell hívni.

Az adattovábbítás papír alapon vagy elektronikus úton történhet. Abban az esetben, ha az adattovábbítás elektronikus adatfeldolgozással hatékonyabban teljesíthető, akkor az adattovábbításról az irattár részére kísérőlevelet kell készíteni, amely tartalmazza az adattovábbítást kérő megkeresésében felsorolt adatokat.

6.5. Az OAH szervezetén belül a kezelt személyes adat - a feladat elvégzéséhez szükséges mértékben és ideig - csak az üggyel érintett szervezeti egységhez továbbítható, feltéve, hogy a személyes adatok megismerése nélkül az ügyben érdemben eljárni nem lehet. Az OAH szervezetén belül a különböző célú adatkezelések csak törvényes cél érdekében, indokolt esetben, ideiglenesen kapcsolhatók össze.

7. Az érintett jogai

7.1. Az érintett jogosult az OAH és az annak megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által kezelt személyes adatai vonatkozásában a következőkre:

a) az adatkezeléssel összefüggő tényekről az adatkezelés megkezdését megelőzően tájékoztatást kapjon (előzetes tájékozódáshoz való jog),

b) kérelmére személyes adatai és az azok kezelésével összefüggő információk rendelkezésre bocsátására (hozzáféréshez való jog),

c) kérelmére személyes adatai helyesbítésére, illetve kiegészítésére (helyesbítéshez való jog),

d) kérelmére személyes adatai kezelése korlátozására (az adatkezelés korlátozásához való jog),

e) kérelmére személyes adatai törlésére (törléshez való jog).

7.2. Az OAH az érintett jogai érvényesülésének elősegítése érdekében megfelelő műszaki és szervezési intézkedéseket tesz, így különösen

a) az érintett részére törvényben meghatározott esetekben nyújtandó bármely értesítést és tájékoztatást könnyen hozzáférhető és olvasható formában, lényegre törő, világos és közérthetően megfogalmazott tartalommal teljesíti, és

b) az érintett által benyújtott, az őt megillető jogosultságok érvényesítésére irányuló kérelmet annak benyújtásától számított legrövidebb idő alatt, de legfeljebb huszonöt napon belül elbírálja és döntéséről az érintettet írásban, vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíti.

7.3. Az OAH a 7.1. pontban meghatározott jogok érvényesülésével kapcsolatban meghatározott feladatait – törvényben rögzített kivétellel - ingyenesen látja el.

7.4. Ha megalapozottan feltehető, hogy a 7.1. b) - e) pontjában meghatározott jogok érvényesítése iránt kérelmet benyújtó személy az érintettel nem azonos személy, az OAH a kérelmet az azt benyújtó személy személyazonosságának hitelt érdemlő igazolását követően teljesíti.

7.5. A 7.1. a) pont szerinti előzetes tájékoztatás az OAH-ban – az Szvtv. szabályai alapján - működő elektronikus megfigyelőrendszerrel kapcsolatban ki kell, hogy terjedjen:

a) az elektronikus megfigyelő rendszer kamerái helyeire, illetőleg arra, hogy a kamerák mit rögzítenek;

b) az adatkezelő és az adatfeldolgozó személyére, illetőleg azon természetes személyek nevére, beosztására, akik a kamerák felvételeihez hozzáférhetnek.

8. Az adatvédelemért felelősök feladatai

8.1. Az OAH főigazgatója

a) kijelöli az adatvédelmi tisztviselőt, nevét és elérhetőségét közli a felügyeleti hatósággal, biztosítja a feladata elvégzéséhez szükséges feltételeket,

b) kiadja az AASZ-t,

c) felügyeli az adatvédelmi feladatok ellátását.

8.2. Az adatvédelmi tisztviselő jogállása és feladatai

Az adatvédelmi tisztviselő közvetlenül az OAH főigazgatójának tartozik felelősséggel.

Az adatvédelmi tisztviselő más feladatokat is elláthat, de csak akkor, ha e feladatokból nem fakad összeférhetetlenség.

Az adatvédelmi tisztviselő feladatai:

a) közreműködik, illetőleg segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;

b) ellenőrzi a jogszabályok, valamint az AASZ rendelkezéseinek a megtartását;

c) kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés esetén annak megszüntetésére hívja fel az adatkezelőt;

d) elkészíti és aktualizálja az AASZ-t;

e) együttműködik a felügyeleti hatósággal; az adatkezeléssel összefüggő ügyekben kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele.

8.3. Az önálló szervezeti egységek vezetői

a) felelősek azért, hogy az általuk vezetett szervezeti egységnél az adatkezelés a jogszabályokban és az AASZ-ben meghatározottak szerint történjék;

b) gondoskodnak a szervezeti egység által kezelt személyes adatoknak a belső adatvédelmi nyilvántartásba történő bejelentéséről, a változások folyamatos jelentéséről;

c) felelősek azért, hogy a szervezeti egység által végzett adatkezelések során az adatbiztonságról szóló 10. pontban leírt biztonsági előírások maradéktalanul teljesüljenek;

d) a szervezeti egységükbe érkező új munkatársakról, valamint a szervezeti egységükből távozó munkatársakról azonnal kötelesek az Informatikai Osztályt írásban (pl. Help Desk segítségével) értesíteni a jogosultságok aktualizálása céljából, akkor is, ha a személyi változás belső áthelyezésből ered. Ez a kötelezettség a munka jogviszonyban álló munkatársakra vonatkozóan is fennáll;

e) gondoskodnak arról, hogy a szervezeti egységüktől tartósan távollévők (például gyermekgondozási díjban részesülő kismama) jogosultságát az Informatikai Osztály a távollét idejére korlátozza.

8.4. Az adatkezelést végző személy

a) tevékenységi körén belül felelős az adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért, valamint az adatok pontos, követhető dokumentálásáért;

b) kezeli és megőrzi a feladata ellátása során birtokába került adatokat;

c) ügyel a nyilvántartások biztonságos kezelésére és tárolására;

d) gondoskodik arról, hogy az általa vezetett nyilvántartások adataihoz illetéktelen személy ne férhessen hozzá;

e) betartja az adatkezelésre vonatkozó jogszabályokat és belső utasításokat;

f) részt vesz az adatkezeléssel, adatvédelemmel összefüggő szakmai képzéseken;

g) a Kit. 94. §-ában foglaltak szerint köteles megtagadni minden olyan utasítás végrehajtását, amelynek teljesítésével bűncselekményt vagy szabálysértést valósítana meg, vagy más személy életét, testi épségét, egészségét, vagy a környezetét közvetlenül és súlyosan veszélyeztetné;

h) az utasítás végrehajtását megtagadhatja, ha annak teljesítése az életét, egészségét vagy testi épségét közvetlenül és súlyosan veszélyeztetné, vagy jogszabályba, kormányzati igazgatási szerv által kiadott normatív utasításba ütközne;

i) köteles az utasítást adó figyelmét felhívni, és egyben kérheti az utasítás írásba foglalását, ha az utasítás végrehajtása jogszabályba vagy a kormányzati igazgatási szerv által kiadott normatív utasításba ütközne, teljesítése kárt idézhet elő és az érintettek jogos érdekeit sérti.

9. Belső adatvédelmi nyilvántartás

A belső adatvédelmi nyilvántartás az OAH szervezeti egységeinél történő, a személyes adat kezelésekkel kapcsolatban tartalmazza legalább

a) az adatkezelés célját;

b) az adatok fajtáját és kezelésük jogalapját;

c) az érintettek körét;

d) az adat forrását;

e) az esetleges adattovábbítások fajtáját, címzettjét és a továbbítás jogalapját;

f) az egyes adatfajták törlésének határidejét;

g) az adatkezelő, valamint az adatfeldolgozó nevét és címét (székhelyét), a tényleges adatkezelés, illetve az adatfeldolgozás helyét és az adatfeldolgozónak az adatkezeléssel összefüggő tevékenységét.

A belső adatvédelmi nyilvántartást a 2. Melléklet tartalmazza.

10. Adatbiztonság

10.1. Az adatkezelés biztonsága

Az OAH a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:

a) a személyes adatok álnevesítését és titkosítását;

b) a személyes adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét;

c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen állítani;

d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást.

A biztonság megfelelő szintjének meghatározásakor kifejezetten figyelembe kell venni az adatkezelésből eredő olyan kockázatokat, amelyek különösen a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan nyilvánosságra hozatalából vagy az azokhoz való jogosulatlan hozzáférésből erednek.

Adatkarbantartást csak az erre felhatalmazott munkatárs végezhet.

A számítástechnikai rendszerek üzemeltetését ellátó munkatársak a feladataik ellátásához szükséges mértékig az adatállományokhoz hozzáférhetnek, az adatokat azonban más célra nem használhatják fel, és mások tudomására nem hozhatják.

Az adatbiztonság érdekében megfogalmazott előírások betartásáért a központi informatikai rendszer vonatkozásában az Informatikai Osztály vezetője, a lokális adatfeldolgozási rendszerek vonatkozásában az adatfeldolgozást végző szervezeti egység vezetője a felelős.

10.2. Az adatokhoz való hozzáférés szabályozása

Az adatokhoz való hozzáférést jelszavas védelemmel és jogosultsági rendszer működtetésével történik.

A központi rendszerhez, illetve a szerver központi tárterületeihez való hozzáférés jelszavát és jogosultsági rendszerét az Informatikai Osztály vezetője állítja be és kezeli.

Az egyedi alkalmazások lokális gépein a speciális adatfeldolgozó szoftver saját jelszó és jogosultsági rendszerét kell alkalmazni. A jelszavak használatáért, azok rendszeres változtatásáért és dokumentálásáért az Informatikai Osztály vezetője felelős.

A központi rendszer és az egyedi rendszerek hozzáférési jogosultságának működtetésére egyaránt érvényesek az Informatikai Biztonsági Szabályzatban rögzített előírások.

10.3. Az adatok mentése, az adathordozók biztonsága

Az adatok mentésének és az adathordozók biztonságának általános szempontjait az Informatikai Biztonsági Szabályzat rögzíti.

A központi szervereken tárolt adatok rendszeres mentését az Informatikai Osztály munkatársa végzi az Informatikai Biztonsági Szabályzatban foglaltak szerint.

A lokális adatfeldolgozási rendszerek adatainak mentéséről, a mentések naplózásáról az adathordozók nyilvántartásáról, biztonságos tárolásáról a konkrét adatkezelést végző munkatárs gondoskodik.

11. Egyéb rendelkezések

11.1. Adatvédelmi incidens

Az adatvédelmi incidenst az OAH indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti a felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is.

A bejelentésben legalább:

a) ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;

b) közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;

c) ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;

d) ismertetni kell az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

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

Az adatvédelmi tisztviselő nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket. E nyilvántartás lehetővé teszi, hogy a felügyeleti hatóság ellenőrizze az e cikk követelményeinek való megfelelést

11.2. Adatvédelmi hatásvizsgálat

Ha az adatkezelés valamely, különösen új technológiákat alkalmazó típusa – figyelemmel annak jellegére, hatókörére, körülményére és céljaira – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, akkor az adatkezelő az adatkezelést megelőzően hatásvizsgálatot végez arra vonatkozóan, hogy a tervezett adatkezelési műveletek a személyes adatok védelmét hogyan érintik.

Az adatvédelmi hatásvizsgálat elvégzésekor az adatvédelmi tisztviselő szakmai tanácsát ki kell kérni.

Az OAH - az adatvédelmi tisztviselő bevonásával - szükség szerint, de legalább az adatkezelési műveletek által jelentett kockázat változása esetén ellenőrzést folytat le annak értékelése céljából, hogy a személyes adatok kezelése az adatvédelmi hatásvizsgálatnak megfelelően történik-e.

11.3. Előzetes konzultáció

Ha a 11.2. pont szerinti adatvédelmi hatásvizsgálat megállapítja, hogy az adatkezelés az OAH által a kockázat mérséklése céljából tett intézkedések hiányában valószínűsíthetően magas kockázattal jár, a személyes adatok kezelését megelőzően az OAH konzultál a felügyeleti hatósággal.

Az OAH a felügyeleti hatósággal folytatott konzultáció során a felügyeleti hatóságot tájékoztatja:

a) adott esetben az adatkezelésben részt vevő adatkezelő, közös adatkezelők és adatfeldolgozók feladatköreiről, különösen vállalkozáscsoporton belüli adatkezelés esetén;

b) a tervezett adatkezelés céljairól és módjairól;

c) az érintettek fennálló jogainak és szabadságainak védelmében hozott intézkedésekről és garanciákról;

d) adott esetben, az adatvédelmi tisztviselő elérhetőségeiről;

e) a lefolytatott adatvédelmi hatásvizsgálatról; és

f) a felügyeleti hatóság által kért minden egyéb információról.

11.4. Az iratkezelésre vonatkozó adatvédelmi szabályok

Az iratokhoz való hozzáférési jogosultságokat a szervezeti egységek vezetőinek kérése alapján az Informatikai Osztály munkatársa állítja be és tartja nyilván.

Az OAH ügyiratkezelése során az iratokat csak az arra jogosultsággal rendelkező munkatársak kezelhetik.

Az iratokat különálló, zárható helyiségben, zárható iratszekrényekben kell védeni az illetéktelen hozzáféréstől.

A passzív kezelésben lévő iratok archiválását évente el kell végezni. Az iratokat jól zárható, száraz, tűzvédelmi és vagyonvédelmi berendezéssel ellátott helyiségben kell tárolni.

Mindazon iratot, amelyet a Magyar Nemzeti Levéltár történeti értékűnek minősít, őrzésre át kell adni a Levéltár részére. A levéltári átadás legkorábban az irat keletkezésétől számított 15 év eltelte után történhet. A levéltári kezelésbe átadott iratok adatvédelméért, a beszállítást követően, a Magyar Nemzeti Levéltár tartozik felelősséggel.

Mellékletek:

1. melléklet Az adatkezeléssel kapcsolatos alapfogalmak értelmezése
2. melléklet Belső adatvédelmi nyilvántartás