NIIF INTÉZET – HBONE+ PROGRAM
H–1132 Budapest, Victor Hugo utca 18–22. · postacím: H–1396 Budapest 62, Pf. 498.
telefon: (1) 450-3060 · fax: (1) 350-6750 · e-mail: info@hboneplus.hu · url: www.hboneplus.hu

KMOP-4.2.1/A_2-08/1-2009-0001 és TIOP-1.3.2-08/1-2009-0001

HBONE+

felsőoktatási információs infrastruktúra fejlesztése

ÁLLÁSFOGLALÁS A MAGYAR KUTATÁSI ÉS FELSŐOKTATÁSI FÖDERÁCIÓ (HREF) KERETÉBEN TÖRTÉNŐ ADATKEZELÉSRŐL

Dátum: 2009.09.30.	***Revizió***	1.0
Minősítése: nyilvános		

Befektetés a jövőbe
Új Magyarország FEJLESZTÉSI TERV

TARTALOMJEGYZÉK

1 Állásfoglalás célja

Az állásfoglalás célja az Magyar Kutatási és Felsőoktatási Föderáció (HREF) által létrehozni kívánt elosztott autentikációs és autorizációs infrastruktúra (NIIF AAI) adatvédelmi előírásoknak való megfelelőségének vizsgálata. A megfelelőségi vizsgálat során a 2009. szeptember 29-ig kialakított rendszertervek és elképzelések adatvédelmi szempontú értékelésére került sor. A 2009. szeptember 29-ig kialakított rendszertervek és elképzelések egy része a https://wiki.aai.niif.hu címen érhetők el, más részük pedig az NIIF és az OTY StarTel Kft. részvételével 2009 során tartott megbeszéléseken kerültek ismertetésre. A megbeszéléseken ismertetett elképzelések összefoglalása a jelen Állásfoglalás mellékletében található. Az Állásfoglalás bemutatja az NIIF AAI-ban tervezett adatkezelési folyamatokat és értékeli ezeket abból a szempontból, hogy azok megfelelnek-e a személyes adatok védelmére vonatkozó jogszabályi követelményeknek, egyben javaslatokat is megfogalmaz arra vonatkozóan, hogy a megfelelőség hogyan lenne teljesíthető azokban az esetekben, amikor a megfelelőség a rendszerterv vagy az elképzelések kidolgozottságának foka miatt még nem ítélhető meg.

2 NIIF AAI

A Magyar Kutatási és Felsőoktatási Föderáció (HREF) egy identitás föderáció (identity federation), amely azt biztosítja, hogy az identitás-információk a föderáció tagjainak egymástól független rendszerei között átadhatóak legyenek, vagyis egy olyan intézmények közötti együttműködés, amely lehetővé teszi az intézmények között az identitás-információk átadását. Identitás-információk olyan személyi azonosítók, amelyek alapján a felhasználók azonosítása megfelelően elvégezhető.

Az identitás föderációk működésének a feltétele, hogy a föderáció tagjai megbízzanak a föderáció egy másik tagja által nyújtott identitás-információkban. Az identitás föderáció létrehozásának éppen ennek a bizalomnak a megteremtése a lényege. A föderáció lehetővé teszi, hogy egy intézménynek ne kelljen minden más intézménnyel külön-külön megállapodásokat kötnie az identitás-információk kölcsönös elfogadása és megosztása érdekében. Az identitás föderációhoz történő csatlakozással automatikusan létrejöhet ez a kölcsönös bizalom. Egy indentitás föderáción belüli tagság nem zárja ki, hogy egy intézmény több föderációhoz is kapcsolódjon illetve, hogy külön kétoldalú megállapodásokat kössön identitás-információk megosztására.

Az identitás föderációk által létrehozott bizalmi viszonyt az ún. föderatív azonosító és jogosultság kezelő rendszerek (federated authentication and authorization systems) ültetik át a gyakorlatba. Az ilyen rendszerek föderáción belüli összessége alkotja egy föderáció autentikációs és autorizációs infrastruktúráját (Authentication and Authorization Infrastructure – AAI). Az AAI lehetővé teszi a felhasználók számára, hogy webes alkalmazások igénybe vételekor saját intézményük (Azonosítás Szolgáltató – Identity Provider, IdP) azonosítsa őket akkor is, ha éppen nem a saját intézményük által nyújtott szolgáltatásokat szeretnék igénybe venni. Az azonosító szervezetekkel azonos funkciót tölthetnek be egy AAI-ban az ún. Virtuális Azonosító Szervezetek (Virtual Home Organization, VHO).[1]

Az AAI-ban az egyes szolgáltatásokat nyújtó intézményeket Tartalomszolgáltató Szervezet-nek (Service Providers, SP) nevezik, a tartalom

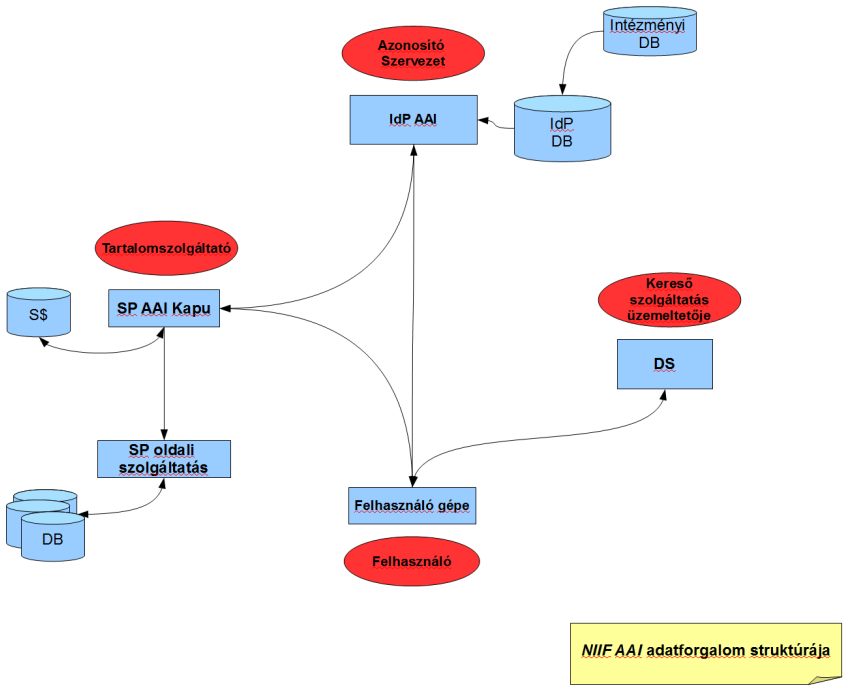
[1] Virtuális azonosító szervezet ugyanazokat a funkciókat látja el, mint egy IdP. Célja, hogy olyan személyek számára is lehetőséget biztosítson föderációban történő részvételre, elvégezve azok azonosítását, akik egyéni felhasználók vagy az anyaintézményük nem tagja a föderációnak, tehát nem IdP-k. Az NIIF a virtuális azonosító szervezet mint egyfajta központi IdP szervezet feladatait outsourcing szolgáltatásként kívánja nyújtani.

Szolgáltató Szervezetek által nyújtott szolgáltatások az SP AAI Kapun keresztül csatlakoznak az AAI-hoz.

A felhasználók azonosítása egy AAI-ban tehát minden esetben azon intézmény Azonosítás Szolgáltatójánál történik, amely intézménynél a felhasználó honos, és ahol a felhasználót korábban már megbízhatóan azonosították.

A föderatív szervezetekben az identitáshoz kapcsolódó adatok tehát csak egy helyen állnak rendelkezésre és egy felhasználó adataihoz csak a saját intézménye férhet hozzá, illetve csak a belső szabályzatban leírt elveknek megfelelően adja azokat ki más föderációs intézményeknek.

Az AAI-k használatának legnagyobb előnye, hogy nem kell "idegen", más föderációs intézmények felhasználóit a Tartalom Szolgáltató szervezeteknek külön-külön azonosítaniuk és nyilvántartásba venniük, mert az AAI lehetővé teszi, hogy azonosításukat vagy saját anyaintézményük, vagy a föderációban szintén tag Virtuális Azonosító Szervezet végezze el. További előnye az AAI-knak, hogy az azonosítás mellett lehetőséget nyújtanak arra is, hogy az Azonosító Szervezet (IdP) a felhasználói jogosultság kezeléshez szükséges információkat is átadja a Tartalomszolgáltató Szervezeteknek (SP).



A fenti ábra (1. ábra) a NIIF AAI-ben résztvevő intézménytípusok, valamint a felhasználók és más entitások között létrejövő adatforgalom struktúráját mutatja.

3 Használt fogalmak

Az állásfoglalásban használt fogalmaknak az alábbi értelmezése tekintendő irányadónak.

a) Adatkezelés

Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így például gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása (Avtv. 2§ (1) 9. pont).

b) Adatkezelő

Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja. Teljes felelősséggel tartozik tehát az adatkezelés céljának meghatározásáért, döntések végrehajtásáért, adatfeldolgozói megbízás adásáért, illetve ezen megbízás jogszerűségéért (Avtv. 2.§ (1) 8. pont).

c) Adattörlés

Az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges (Avtv. 2§ (1) 12. pont).

d) Adattovábbítás

Az adattovábbítás alatt olyan adatkezelési folyamatot értünk, amikor az adatot meghatározott harmadik személy számára hozzáférhetővé teszik (Avtv. 2§ (1) 10. pont).

e) Attribútum

A felhasználóra vonatkozó tulajdonság. Az egyes attribútumok közös értelmezését az Attribútum Specifikáció határozza meg.

f) Attribútum Kiadás Szabályzat (Attribute Release Policy, ARP)

Az ARP határozza meg, hogy az attribútum feloldás után rendelkezésre álló attribútumok közül melyek adhatók ki az erőforrásokat kezelő SP-knek.

g) Attribútum Specifikáció (Attribute Specifications)

Az Attribútum Specifikáció meghatározza a föderáción belül használt attribútumok értelmezését az AAI elemek (IdP-k, SP-k) számára. Attribútum Specifikáció a föderáción belüli adatcseréhez nyújt segítséget.

h) Azonosítás (Autentikáció)

Egy korábban már regisztrált felhasználó azonosítása. Mind a regisztrálást, mind az azonosítást egy szervezet, a felhasználóhoz kötődő anyaintézmény, IdP végzi.

i) Azonosító Szervezet (Identitásszolgáltató, Identity Provider, IdP)

Az Azonosító Szervezet egy olyan AAI elem, amelynek a feladata a felhasználók adatainak kezelése és tárolása. Három fő funkciót lát el: (1) felhasználók azonosítását, (2) attribútumok kiadását az SP-k részére valamint (3) a felhasználók, illetve a felhasználói adatok menedzsmentjét.

j) Felhasználói hozzájárulás

Az érintett felhasználó kívánságának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok - teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez. (Avtv. 2§ (1) 6. pont)

k) Autorizáció (Hozzáférés Engedélyezés)

Egy már azonosított felhasználónak különböző erőforrásokhoz történő hozzáférésének szabályozása, amelyet a Tartalomszolgáltatók (SP-k) végeznek. Az SP-k az autorizációt az IdP-k által kiadott attribútumok alapján végzik.

l) Keresőszolgáltatás (korábban: WAYF, jelenleg: Discovery Service)

A WAYF szó a Where Are You From? mondat rövidítése és egy olyan szolgáltatást jelent, amely a föderációs metadata állomány(ok)ra épül és a felhasználó számára lehetőséget ad, hogy az Azonosítás Szolgáltatóját (IdP) kiválassza. A SAML2 szabvány a WAYF funkcionalitást megvalósító szolgáltatást Discovery Service-nek nevezi.

m) Resource Registry (Erőforrások Jegyzéke)

A Resource Registry egy olyan alkalmazás, amely az Azonosító Szervezetekre és a Tartalomszolgáltatókra vonatkozó információkat kezeli. A Resource Registry segítségével előállítható a föderációs metadata, valamint az ARP is.

n) Shibboleth

AAI megvalósításra alkalmas nyílt forrású alkalmazás.

o) Session (munkamenet)

Egy session állapotinformációt fejez ki a felhasználóról. A felhasználó IdP oldali sessionje biztosít(hat)ja azt, hogy ne legyen szükség az azonosító adatok többszöri megadására (Single Sign On). Az SP oldali munkamenet tartalmazza az azonosítás körülményeit (időpont, IdP) és az SP által értelmezett felhasználói attribútumokat. Amíg az SP oldali session érvényes, addig nem szükséges a felhasználót újra azonosítani.

A sessionöket technikailag a böngészőben tárolt sessionazonosító cookie-k segítségével rendelik a felhasználókhoz.

p) SAML

A SAML egy nyílt ipari szabvány, amely olyan XML-alapú protokollokat és adatstruktúrákat definiál, amelyekkel biztonságosan megoldható az adatok cseréje különböző szolgáltatások között. A föderációk esetében a felhasználói azonosítás és jogosultságkezelés a SAML XML üzenetek továbbításával történik, a HREF jelenleg a SAML 2.0 protokollt használja.

q) Tartalom vagy erőforrás-szolgáltató (Service Provider, SP)

A Tartalomszolgáltató egy olyan Shibboleth elem, amely a védett tartalmakat, erőforrásokat a felhasználók számára elérhetővé teszi.

r) Tiltakozás

Az érintett felhasználó nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri (Avtv. 2.§ (1) 7. pont), a tiltakozási jog gyakorlásának feltételeiről az Avtv. 16/A.§ rendelkezik (l. Felhasználói hozzájárulás).

4 Adatkezelési folyamatok

4.1 Adatkezelés szempontjából releváns AAI elemek és funkcióik

4.1.1 Föderáció valamennyi szereplője által használt AAI elemek

4.1.1.1 Felhasználói Föderációs Azonosító

Az egyes azonosító típusok közül a HREF nem a föderációs gyakorlatban egyébként elterjedt EduPersonPrincipalName-et vagy a EdupersonTargetedID-t, hanem az utóbbival szinte teljesen megegyező SAML 2 persisztens NameID-t kívánja használni. A SAML 2 persisztens NameID egy állandó, nem átlátszó (opaque)[2], célzott (targeted)[3] azonosító, amely elsősorban gép általi értelmezésre alkalmas (privacy preserving vagy adatvédelembarát azonosító).

A HREF-en belül az EduPersonPrincipalName használata csak az egyes intézményeken belüli alkalmazás esetén javasolt.

4.1.1.2 Attribútum specifikáció

A föderációs attribútum specifikáció célja, hogy a résztvevő felek között az információátadást megkönnyítse, illetőleg a személyes adatok védelmét garantálja közös attribútum definíciók révén. A közös attribútum definíciók tehát a föderációs rendszerelemek közötti kommunikációt segítik elő hiszen valamennyi fél ugyanazt érti az attribútum elnevezése és tartalma alatt. Az így meghatározott attribútumokon túl a felek egymás között tetszőlegesen meghatározhatnak további attribútumokat és ezeket szabadon használhatják. Az attribútum specifikáció elősegíti az AAI működését.

[2] Az ilyen nem átlátszó azonosítók nem jellemzők a felhasználóra, értékükből nem lehet következtetni a felhasználó személyére (pl. e-mail címére).

[3] Az ilyen, célzott azonosítók minden SP-nél különbözőek, s így az SP-k - az IdP közreműködése nélkül - nem képesek profilt készíteni egy felhasználóról, ami adatvédelmi szempontból kívánatos.

4.1.1.3 Resource Registry (metadata)

A Resource Registry tartalmazza a föderáció tagjaira, így az Azonosító Szervezetekre (IdP) és a Tartalom Szolgáltatókra (SP) vonatkozó valamennyi lényeges információt, vagyis tulajdonképpen a föderációs metadatát. A Resource Registry másodlagos szerepe, a metadata összeállításán túl, hogy az IdP-k itt adhatják meg, hogy milyen attribútumok használatát támogatják a föderáció működéséhez, továbbá az SP-k itt jelölhetik meg, hogy milyen - kötelező és opcionális felosztásban meghatározott - attribútumokra van szükségük ahhoz, hogy a felhasználók számára az általuk nyújtott szolgáltatást elérhetővé tegyék. Az így megadott attribútumok alapján generálható az attribútumok kiadására vonatkozó szabályok együttese, az Attribútum Kiadási Szabályzat is. A Resource Registry nyújt tehát segítséget az intézményi adminisztrátoroknak, hogy kivel, milyen feltételek mellett tudnak együttműködni. A HREF-ben jelenleg az eredetileg a SWITCH svájci föderáció által kifejlesztett Resource Registry jelentősen továbbfejlesztett és módosított változatát alkalmazzák.

A Resource Registry-ben a föderációs résztvevők maguk módosíthatnak az adatokon, amelyek a föderáció üzemeltetőjének jóváhagyása után lépnek életbe.

4.1.1.3.1 Metadata adminisztráció

Metadata egy központilag kialakított, automatikusan frissülő, aláírt publikus adatállomány, amely tartalmazza föderációban résztvevő valamennyi intézményre, így Azonosító Szervezetekre és Tartalom Szolgáltatókra vonatkozó lényeges információkat. A metadata adminisztrációja központilag történik, maga az állomány bárki számára hozzáférhető. Az egyes entitásokra vonatkozó háttér-információk egyrészt intézményi adatok (pl. tanúsítvány, név, scope[4], stb.), valamint az egyes intézményekhez tartozó technikai és adminisztratív kapcsolattartók elérhetőségéhez kötődő személyes adatok (a kapcsolattartók elérhetőségeként általában azok nevét és email címét jelölik meg). A metadata a kapcsolattartók elérhetőségeként megadott adatokon kívül más személyes adatot nem tartalmaz. A föderáció minden résztvevője egy központi helyről tölti le rendszeres időközönként a metadata fájlokat.[5]

[4] A metadata-ban szerepel, hogy egy intézmény milyen scope-ot használhat. Vannak olyan attribútumok, amelyek scope-t is tartalmaznak és az attribútum értéke mellé oda van írva, hogy milyen tartományra érvényes. Az SP ebben az esetben leellenőrzi, hogy a scope-ot valóban olyan IdP állította ki, amely jogosult az adott scope kiállítására (az ELTE nem állíthat ki bme.hu scope-os email címet), ennek azért van jelentősége, hogy az IdP működése is szabályozott keretek között történjen.

[5] A HREF metadata az alábbi címen érhető el: https://rr.aai.niif.hu/metadata/href-metadata.xml

4.1.1.3.2 Attribute Release Policy (Attribútum Kiadási Szabályzat , ARP)

Az Attribútum Kiadási Szabályzat egy olyan, a Resource Registry-be korábban bevitt adatok alapján generált szabálygyűjtemény, amely az Azonosító Szervezet számára rendelkezésre álló attribútumok közül megjelöli azokat, amelyek kiadhatóak az erőforrásokat kezelő SP-k részére. Az Azonosító Szervezetek maguk határozhatják meg azt, hogy a Resource Registry-ben az SP által korábban megjelölt attribútumok alapján a Resource Registry által összeállított ARP-t használják-e vagy kézileg konfigurált ARP-vel dolgoznak. Az ARP révén az Azonosító Szervezetek tehát, az adattovábbítás szabályozott rendjét határozzák meg. Az attribútumok így csak akkor kerülnek átadásra az SP részére, ha ezt az Attribute Release Policy-ban az IdP engedélyezte. Az Attribútum Kiadási Szabályzat vonatkozhat a teljes IdP-re, tehát az Azonosító Szervezetnél regisztrált és nyilvántartott valamennyi felhasználóra ("site" ARP), vagy alkalmazása leszűkíthető egy azonosított felhasználóra is.

A Resource Registry-ben a Tartalomszolgáltatók csak olyan – az Attribútum Specifikációban szereplő – attribútumokat jelölhetnek meg kötelező attribútumnak, amelyek a szolgáltatás igénybevételéhez feltétlenül szükségesek. Alapelv – és ezt a föderáció üzemeltetője a jóváhagyás előtt ellenőrzi – hogy a kötelező attribútumok köre a lehető legszűkebb legyen.

4.1.1.4 *Keresőszolgáltatás(ok) (DS)*

A Keresőszolgáltatás (Discovery Service)[6] alatt egy olyan alkalmazást értünk, amely a felhasználó számára nyújt segítséget az őt azonosítani hivatott identitásszolgáltató kiválasztásához. A Keresőszolgáltatás feladata tehát alapvetően technikai jellegű, strukturális szempontból lehet az IdP-nek és az SP-nek is része, illetőleg lehet különálló elem is, a működését ez nem befolyásolja. A Keresőszolgáltatás megpróbálhatja továbbá kitalálni (valós időben megtippelni) az IdP-t IP cím alapján. Legegyszerűbb esetben a Keresőszolgáltatás egy előválasztó felületen kilistázza az elérhető Azonosító Szervezeteket, amelyek közül a felhasználó választhat, majd a választást a DS bizonyos ideig (a böngésző bezárásáig, néhány napig, stb.), szintén a felhasználó hozzájárulásától függően megjegyezi és azt a felhasználó gépén egy cookie-ban eltárolja. A DS a felhasználót a választást követően közli az SP-vel, a felhasználónak ki az IdP-je vagyis, hogy melyik intézmény jogosult azonosítani. (Az üzenetátvitel a felhasználó böngészőjének átirányításával történik.)

[6] A DS, valamint a Shibboleth korábbi verziójában ugyanezt a funkciót betöltő WAYF alkalmazás között az az eltérés, hogy a WAYF nem az SP-nek mondja meg az információt, hanem megkapja az SP-től teljes autentikációs kérést és továbbítja az IdP-nek, mely esetben az autentikációs kérés nem megy át a DS-en, hanem a felhasználó választja ki egy felületen, hogy ki az IdP, aki azonosítani fogja.

A föderációban lehetőség van több DS használatára, továbbá lehetséges, hogy egyes intézmények saját maguk üzemeltessenek DS-t, illetve, hogy az intézményi DS mellett egy központi DS is működjön. A Keresőszolgáltatás által kezelendő adatok köre csakis azon szükséges adatokra korlátozódik, amelyek ahhoz szükségesek, hogy a felhasználó kiválassza az őt azonosító IdP-t, valamint a felhasználó választásától és hozzájárulásától függően a DS által használt cookie alkalmazásával összefüggésben megtörtént adatkezelésre, vagyis a cookie használata érdekében rögzített személyes adatok körére.

4.1.2 Azonosító szervezetek által üzemeltetett AAI elemek

4.1.2.1 *IdP AAI kapu*

Az Azonosító Szervezetek a föderációval az IdP AAI elemen keresztül lépnek kapcsolatba. Ezen IdP szolgáltatás funkciója az azonosítás, amely érdekében a felhasználó adatait az IdP adatbázis (IdP DB) tárolja, ennek alapján a hozzá érkező kérésnek megfelelően a felhasználót azonosítja és a felhasználói azonosítással kapcsolatos információkat átadja a Tartalomszolgáltatónak. Az IdP AAI elem adja ki a felhasználói attribútumokat az SP részére az Attribútum Kiadási Szabályzatnak megfelelően.

Az IdP adatbázist az Azonosító Szervezetek adminisztrálják, a felhasználók kezelése az Azonosító Szervezet belső előírásai szerint történik.

4.1.3 SP-k által üzemeltetett AAI elemek

4.1.3.1 SP AAI kapu

Az SP AAI kapu feladata az Azonosítás Szolgáltatótól kapott adatok értelmezése és ezek alapján az autorizáció elvégzése, lényegében annak eldöntése, hogy az Azonosító Szervezettől kapott adatok alapján, hogy a felhasználó jogosult-e az adott szolgáltatás igénybevételére. Az SP AAI kapu hozza létre az SP oldali sessiont, és ez az elem teszi elérhetővé az Azonosítás Szolgáltatótól kapott attribútumokat az SP szolgáltatás (az alkalmazás) számára.

A Tartalomszolgáltató által üzemeltetett SP AAI kapu általában nem rendelkezik, illetve nem kezeli közvetlenül a felhasználókhoz kapcsolódó személyes adatokat, és nem feladata a felhasználók adminisztrációja sem.

4.1.3.2 SP szolgáltatás

A Tartalomszolgáltató a föderáció részét képező SP AAI kapun kívül üzemelteti és elérhetővé teszi a föderáció felhasználói részére nyújtott szolgáltatásokat, alkalmazásokat és erőforrásokat. A szolgáltatások nem a föderáció részei, az SP szolgáltatásokat megvalósító rendszerelemek nem részei az AAI-nak. A szolgáltatások igénybevétele során kezelt adatok tipikusan lehetnek állandó azonosítók (pl. az IdP-től kapott azonosító) vagy ún. másodlagosan keletkező személyes adatok, mint például a szolgáltatás igénybevételének időpontja és helye vagy a szolgáltatás használatának időtartama. Bizonyos esetekben az SP szolgáltatás a felhasználóról további adatokat is tárolhat, ezt a saját adatkezelési szabályzata – és a felhasználó hozzájárulása – alapján teheti.

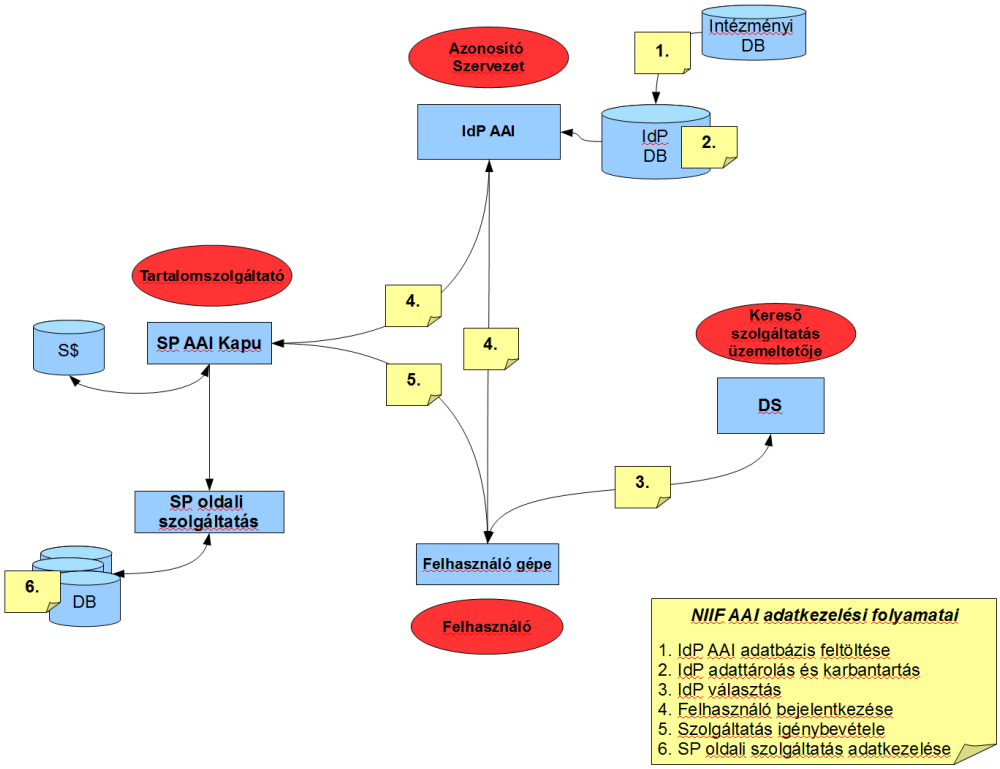
4.1.4 Naplózás

4.2 Az NIIF AAI működéséhez kapcsolódó adatkezelési folyamatok

Összesen 6 jól elkülöníthető adatkezelési folyamat található a tervezett NIIF AAI-ban:

1. IdP AAI kapu adatbázis feltöltés;
2. IdP AAI kapu adattárolás és karbantartás;
3. IdP AAI kapu választás;
4. Felhasználó bejelentkezés;
5. Szolgáltatás igénybevétele;
6. SP szolgáltatások adatkezelése;

A 6. adatkezelési folyamat az egyes SP szolgáltatások adatkezelése. Ezek a szolgáltatások az NIIF AAI működéséhez szorosan kapcsolódnak, különös tekintettel arra, hogy az NIIF AAI-hoz kapcsolódó SP szolgáltatások mind használják az NIIF AAI-ban képzett föderációs felhasználói azonosítókat. Mindazonáltal ezen szolgáltatásokhoz kapcsolódó adatkezelések a NIIF AAI adatkezelési folyamatok körén kívül esnek. Kizárólag azért foglalkozunk velük, mert az IdP-k által nyújtott adatok ezen szolgáltatásokban kerülnek végső soron felhasználásra, viszont az identitás föderáció működését az SP szolgáltatások belső adatkezelése nem érinti.



A fenti ábra (2. ábra) mutatja be a föderációban résztvevő intézménytípusok, valamint a felhasználók és más entitások között létrejövő, a NIIF AAI működéshez kapcsolódó adatforgalom alapvető struktúráját, külön jelezve az egyes szereplők közötti adatkezelési folyamatokat.

4.2.1 IdP AAI kapu adatbázis feltöltés

4.2.1.1 A folyamat rövid leírása

Felhasználó és az Azonosító Szervezet közötti adatkezelési folyamat a felhasználó személyes adatainak az átadását és az adatoknak az IdP adatbázisába történő rögzítését foglalja magába. Az adatok átadása több módon is történhet, de jellemzően az Azonosító Szervezet a saját címtárból vagy felhasználói adatbázisból veszi a felhasználó azonosításához és a föderáció működéséhez szükséges adatokat.

4.2.1.2 A folyamat szereplői

- Felhasználó
- Azonosító Szervezet (IdP)

4.2.1.2.1 Adatalanyok

- Felhasználó

4.2.1.2.2 Adatkezelők

- Azonosító Szervezet

4.2.1.3 Kezelt adatok

Felhasználó személyes adatai, amelyet az intézmény a saját adatvédelmi rendelkezéseinek megfelelően korábban már jogszerűen rögzített adatbázisába.

4.2.1.4 Adatkezelési cél

Felhasználó személyes adatainak átvétele és rögzítése az IdP AAI adatbázisában

4.2.1.5 Adatkezelés időtartama

Az adatkezelési folyamat a felhasználó személyes adatainak az átadását és rögzítését foglalja magába, így az adatkezelés időtartama az adatok rögzítésével véget ér.

4.2.2 IdP AAI kapu adattárolás és karbantartás

4.2.2.1 A folyamat rövid leírás

Az IdP a felhasználó személyes adatainak a rögzítését követően az adatokat tárolja és karbantartja. Az IdP AAI-t üzemeltető „anyaintézmény” rendszerint az alábbi típusú azonosításhoz szükséges adatokat tárolja a felhasználókról: a)

kötelezően megadandó adatok (pl. föderációs azonosító, jelszó, felhasználó név); b) felhasználó által önkéntesen megadott adatok (pl. felhasználóról készült fotók, mobil telefonszám).

4.2.2.2 A folyamat szereplői

- Felhasználó
- Azonosító Szervezet

4.2.2.2.1 Adatalanyok

- Felhasználó

4.2.2.2.2 Adatkezelők

- Azonosító Szervezet

4.2.2.3 Kezelt adatok

- Kezdetben a felhasználó azon személyes adatai, amelyeket az intézmény a saját adatvédelmi rendelkezéseinek megfelelően korábban már jogszerűen rögzített
- Mindazon adatok (attribútumok), amelyeknek a tárolását a felhasználó kérte

4.2.2.4 Adatkezelési cél

Az IdP autentikációs és autorizációs szolgáltatások nyújtása a felhasználó számára.

4.2.2.5 *Adatkezelés időtartama*

Mivel jelen esetben a szóban forgó adatkezelési folyamat a személyes adatok átvételét követőn azok tárolását és karbantartását foglalja magába, az

adatkezelés a felhasználó adatainak az IdP AAI kapu adatbázisból való törlésig tart.

4.2.3 IdP AAI kapu választás

4.2.3.1 A folyamat rövid leírás

A Keresőszolgáltatás adatkezelése technikai jellegű, segítséget nyújt a felhasználónak az őt azonosítani képes anyaintézmény kiválasztásához. Ennek érdekében a DS felsorolja például egy legördülő listában a felhasználó részére a választható IdP-ket (a DS olvasható IP cím alapján előválasztást is végezhet, valós időben megtippelve, hogy a felhasználó, milyen IdP-nél kívánja azonosítani magát), majd a megfelelő IdP kiválasztása után a választást egy cookie-ban eltárolja, amennyiben a felhasználó bejelölte, hogy a DS jegyezze meg a választást a munkamenet (session) végéig. Lehetőség van továbbá arra is, hogy a DS megmaradó cookie-ban rögzítse a felhasználó választását, a felhasználó gépén elhelyezve. A választás eredményeként a DS válaszol az SP-nek, az SP pedig átirányítja felhasználót az felhasználó által választott IdP-hez.

4.2.3.2 A folyamat szereplői

- Felhasználó
- Keresőszolgáltatás (DS)
- Tartalomszolgáltató (SP)

4.2.3.2.1 Adatalanyok

- Felhasználó

4.2.3.2.2 Adatkezelők

- Tartalomszolgáltató
- Keresőszolgáltatás

4.2.3.3 Kezelt adatok

- Felhasználó választása az őt azonosító IdP-jét illetően
- Felhasználó IP címe

4.2.3.4 Adatkezelési cél

A felhasználó segítése az IdP kiválasztásában.

4.2.3.5 Adatkezelés időtartama

A megfelelő IdP kiválasztása után, a DS a választást egy cookie-ban eltárolhatja, amennyiben a felhasználó bejelölte, hogy a DS jegyezze meg a választást a munkamenet (session) végéig. Ebben az esetben az adatkezelés időtartama az adott munkamenet végéig tart. Amennyiben, a felhasználó hozzájárul, hogy a DS egy maradandó cookie-ban tárolja el a kiválasztott Azonosító Szervezetet, az adatkezelés időtartama a cookie lejárati idejéig vagy addig az időpontig tart, amíg a felhasználó a DS által elhelyezett cookie-t ki nem törli.

4.2.4 Felhasználó bejelentkezés

4.2.4.1 *A folyamat rövid leírás*

A felhasználói bejelentkezés folyamata több adatkezelési lépésből tevődik össze. Elsőként a felhasználó megadja az azonosításához szükséges felhasználó nevet és a jelszót az Azonosító Szervezet részére. Az így megtörtént azonosítás alapján az IdP oldalán a felhasználónak munkamenete (session) jön létre, amely időtartam alatt a felhasználó újabb azonosítására nincsen szükség (1. lépés). Az azonosítás azzal válik befejezetté, hogy az IdP és az SP közötti üzenetváltások a felhasználó böngészőjén keresztül lezajlanak. Az SP autentikációs kérésére az IdP vagy egy Artifact[7] üzenetben válaszol vagy HTTP POST üzenetben, jellemzően titkosítva közvetlenül elküldi az autorizációhoz szükséges attribútumokat.[8] Az IdP - SP irányban az

[7] Az artifact használata esetén az IdP a válaszát nem közvetlenül küldi meg az SP részére, csupán egy hivatkozást küld, amely alapján az adatok elérhetőek.

[8] Részletes technikai leírás az Állásfoglalás mellékletét képező Emlékeztetőben található.

artifact nem titkosított és a Felhasználó böngészőjén keresztül megy. Az előző adatkezelési folyamat eredményeként az SP SOAP kapcsolatot nyit az IdP által megküldött artifact üzenethez és az artifact alapján megkapja az IdP teljes válaszát. Az IdP maga dönti el, hogy mi a kiadható attribútumok köre az adott SP felé - az attribútumok SP részére kiadható körének meghatározása az IdP Attribútum Kiadási Szabályban található.

4.2.4.2 A folyamat szereplői

- Felhasználó
- Tartalomszolgáltató (SP)
- Azonosító Szervezet (IdP)

4.2.4.2.1 Adatalanyok

- Felhasználó

4.2.4.2.2 Adatkezelők

- Tartalomszolgáltató
- Azonosító Szervezet

4.2.4.3 Kezelt adatok

- Felhasználó azonosításához szükséges adatok – felhasználó név és jelszó (autentikációs adatok)
- Az IdP AAI kapu által kiadott attribútumok.
- Másodlagosan keletkező adatok (igénybe vett szolgáltatás, szolgáltatás igénybevételének időpontja, szolgáltatás igénybevételének helye)

4.2.4.4 Adatkezelési cél

A felhasználó azonosítása érdekében történik az adatkezelés.

4.2.4.5 Adatkezelés időtartama

Felhasználó azonosítását követően a védett tartalom, szolgáltatás igénybevételéhez megadott IdP oldali munkamenet idejéig vagyis a felhasználó részére az azonosítás érvényességének idejéig tartó időtartam lejártáig.

4.2.5 Szolgáltatás igénybevétele

4.2.5.1 A folyamat rövid leírás

A felhasználói bejelentkezést követően az SP, az IdP által elküldött teljes választ ellenőrzi és amennyiben a Felhasználó jogosult az erőforrás igénybevételére az SP a Felhasználót tovább irányítja az alkalmazáshoz, vagyis az SP Szolgáltatáshoz. Ennek a folyamatnak nem része az SP oldali szolgáltatás által végzett, a felhasználó személyes adatait érintő szükségképpeni adatkezelés a szolgáltatás igénybevétele közben.

4.2.5.2 A folyamat szereplői

- Felhasználó
- Tartalomszolgáltató (SP)
- SP szolgáltatás

4.2.5.2.1 Adatalanyok

- Felhasználó

4.2.5.2.2 Adatkezelők

- Tartalomszolgáltató
- SP Szolgáltatás

4.2.5.3 Kezelt adatok

- Az IdP AAI kapu által kiadott attribútumok.
- Másodlagosan keletkező adatok (igénybe vett szolgáltatás, szolgáltatás igénybevételének időpontja, szolgáltatás igénybevételének helye stb.)

4.2.5.4 Adatkezelési cél

Felhasználó hozzáférésének engedélyezése a védett erőforráshoz.

4.2.5.5 Adatkezelés időtartama

Felhasználó azonosítását követően a védett tartalom igénybevételére megadott SP oldali munkamenet idejéig.

4.2.6 SP oldali szolgáltatás adatkezelése

4.2.6.1 A folyamat rövid leírás

Az adatkezelés a korábban már megfelelően azonosított és a szolgáltatás használatához, az ahhoz való hozzáféréshez engedélyt kapott felhasználóhoz kötődő adatkezelés, amely az SP Szolgáltatás saját belső adatvédelmi szabályainak és rendelkezéseinek megfelelően működik. Ez az adatkezelési folyamat már nem része a föderációs adatkezelésnek.

4.2.6.2 A folyamat szereplői

- Felhasználó
- SP Szolgáltatás

4.2.6.2.1 Adatalanyok

- Felhasználó

4.2.6.2.2 Adatkezelők

- SP Szolgáltatás

4.2.6.3 Kezelt adatok

- Az IdP AAI kapu által kiadott attribútumok.
- Másodlagosan keletkező adatok (igénybe vett szolgáltatás, szolgáltatás igénybevételének időpontja, szolgáltatás igénybevételének helye stb.)

4.2.6.4 Adatkezelési cél

Az SP Szolgáltatásnak az igénybevétele.

4.2.6.5 Adatkezelés időtartama

Felhasználó autorizációját követően a védett tartalom igénybevételére megadott SP oldali munkamenet idejéig, továbbá adott esetben a SP Szolgáltatás saját adatbázisában az így megadott adatokat, valamint további adatokat (leggyakrabban a szolgáltatás jellegétől függő másodlagosan keletkező adatokat) eltárolhatja hosszabb időre is.

5 Adatkezelési folyamatok értékelése

5.1 Alkalmazandó követelmények

Az adatkezelési folyamatok áttekintése során figyelembe veendő követelmények alatt mindazokat a jogszabályi rendelkezéseket érteni kell, amelyek a személyes adatok védelmére vonatkozóan általános vagy különös szabályokat állapítanak meg. Az alkalmazandó követelmények összefoglalása során ennek megfelelően az Adatvédelmi Törvény (a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény - a továbbiakban: Avtv.) rendelkezései mellett figyelemmel kell lenni az egyes speciális adatkezelőket érintő ágazati jogszabályokra, mint például a felsőoktatási intézmények esetében a Felsőoktatási törvény (a felsőoktatásról szóló 2005. évi CXXXIX. törvény - a továbbiakban Ftv.) vonatkozó rendelkezéseire, vagy a Ftv. végrehajtásáról rendelkező kormány rendelet (79/2006. (IV. 5.) Korm. rendelet a felsőoktatásról szóló 2005. évi CXXXIX. törvény egyes rendelkezéseinek végrehajtásáról) szabályaira. Megjegyzendő, hogy az egyes adatkezelői intézmények típusát tekintve az ágazati szabályok körét minden esetben szükséges tisztázni, mivel csak ezek ismeretében állapítható meg, hogy mely adatok kezeléséhez kell hozzájárulást kérni és mely adatok azok, amelyeket az intézmény – adott esetben – külön hozzájárulás nélkül is kezelhet, mert erre törvény lehetőséget ad.

Jelen állásfoglalás összeállítása során az Avtv. és a NIIF föderációban résztvevő, illetve várhatóan tagként csatlakozó intézményekre vonatkozó ágazati szabályokat, valamint nemzetközi föderatív szervezetek ajánlásait, gyakorlatát vettük figyelembe.

5.2 Föderációs adatkezelési folyamatok általános értékelése

A föderatív együttműködés körében felmerülő adatkezelési folyamatok általános értékelése során az alábbi három területet szükséges kiemelni az adatvédelmi megfelelőség szempontjából: (1) az adatalanyok, vagyis a felhasználók hozzájárulása személyes adataik kezeléséhez; továbbá (2) a személyes adatok védelme érdekében alkalmazott föderációs azonosítók használatával kapcsolatban felmerült kérdések valamint, (3) a metadata fájlokban szereplő személyes adatok kapcsán felmerülő adatvédelmi megfontolások.

5.2.1 Felhasználói hozzájárulás

A személyes adatok kezelése során minden esetben figyelemmel kell lenni arra, hogy a személyes adatok kezelése csak az adatvédelmi jogszabályokban előírt, megfelelő tájékoztatást követően megadott kifejezett felhasználói hozzájáruláson alapulhat.

Az Avtv. értelmező rendelkezései szerint a hozzájárulás az érintett kívánságának önkéntes és határozott kinyilvánítása, amely megfelelő tájékoztatáson alapul, és amellyel félreérthetetlen beleegyezését adja a rá vonatkozó személyes adatok - teljes körű vagy egyes műveletekre kiterjedő – kezeléséhez (Avtv 2.§ (1) 6. pont).

A megfelelő tájékoztatáson alapuló felhasználói hozzájárulás alapvető feltétele, az Avtv. 6.§-val összhangban[9] az, hogy az érintettel az adatok felvétele előtt megfelelően közöljék azt is, hogy adatszolgáltatása önkéntes vagy kötelező. Figyelemmel arra, hogy a föderatív együttműködés körében a felhasználók személyes adatainak kezelése nem tekinthető kötelező adatkezelésnek, a föderációban tag intézmények minden esetben kötelesek tájékoztatni a felhasználókat adatközlésük önkéntességéről. Az érintettet - egyértelműen és részletesen - tájékoztatni kell továbbá az adatai kezelésével kapcsolatos minden tényről, így különösen az adatkezelés céljáról és jogalapjáról, az adatkezelésre és az adatfeldolgozásra jogosult személyéről (magányszemély vagy szervezet), az adatkezelés időtartamáról, illetve arról, hogy kik ismerhetik meg az adatokat. A tájékoztatásnak ki kell terjednie az érintett adatkezeléssel kapcsolatos jogaira és jogorvoslati lehetőségeire is. A tájékoztatás elvéből következő ún. nyíltság elve tehát adatvédelmi szempontból azt jelenti, hogy a személyes adatokra vonatkozó fejleményeket, a velük folytatott gyakorlatot és politikát nyíltan kell kezelni, így a személyes adatok létezésének természetének és felhasználásuk fő céljának, valamint az adatkezelő személyének és állandó tartózkodási helyének megismerésére egyszerű módszereket kell kidolgozni.[10]

A hozzájárulás fogalma alapján egyértelműen megállapítható, hogy az adatkezelési hozzájárulást kiterjesztően nem lehet értelmezni, emiatt szükséges az adatalanyok lehető legszéleskörűbb tájékoztatása személyes adataik életútjáról, hogy a felhasználók egyértelműen be tudják azonosítani, hogy mely adatkezelési folyamat(ok)hoz nem kívánnak adott esetben hozzájárulni. A megadott hozzájárulásnak, amellett hogy megfelelő

[9] Az Avtv. 6.§-a rendelkezik a felhasználói hozzájárulás megadásához szükséges tájékoztatás törvény által előírt feltételeiről.

[10] OECD Irányelvek a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról (OECD Adatvédelmi irányelvek, OECD, Guidelines Governing the Protection of Privacy and Transborder Date Flows of Personal Data, 1980.) http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

Az OECD alapelvek a következők: adatgyűjtés korlátozásának elve, adatminőség elve, célhoz kötöttség elve, korlátozott felhasználás elve, biztonság elve, nyíltság elve, személyes részvétel elve, illetőleg a felelősség elve.

tájékoztatáson kell alapulni, bármikor visszavonhatónak is kell lennie, hiszen a személyes adatok feletti aktív önrendelkezési jog, a hozzájárulás visszavonásának jogával együtt értelmezhető.

Az Adatvédelmi törvény 16/A. §(1) bekezdése rendelkezik a felhasználót megillető tiltakozási jogról, amely az érintett azon nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri. A tiltakozási jog akkor gyakorolható, ha a személyes adatok kezelése (továbbítása) kizárólag az adatkezelő vagy az adatátvevő jogának vagy jogos érdekének érvényesítéséhez szükséges, kivéve, ha az adatkezelést törvény rendelte el. Gyakorolható továbbá a tiltakozási jog akkor is, ha a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik, illetve ha a tiltakozás jogának gyakorlását egyébként törvény lehetővé teszi.

Itt fontos megemlíteni az adatkezelőkre vonatkozó ágazati szabályozás körében a Felsőoktatási törvényben foglalt, törvényi felhatalmazáson alapuló adatkezelési engedélyt, illetve a nem törvényi felhatalmazáson alapuló adatkezelési hozzájárulást tartalmazó nyilatkozatot. Az egyes anyaintézmények ugyanis nem tehetik kötelezővé a föderációban való részvételt olyan szolgáltatások igénybevételéhez, amelyek esetében azzal, hogy a felhasználó a személyes adatainak kezeléséhez nem adja a hozzájárulását, illetőleg az hozzájárulást utólag visszavonja, tulajdonképpen a felsőoktatási törvény alapján őt megillető jogok gyakorlásában van akadályozva.

Külön esetként kezelendő, ha a Tartalomszolgáltató, az Azonosító Szervezettől megkapott attribútumokon túl további adatokat kér a felhasználótól. Az ilyen adatok kezeléséhez történő felhasználói hozzájárulás beszerzése már nem a föderatív együttműködés körébe tartozik, így a Tartalomszolgáltatónak kell gondoskodnia az adatvédelmi szabályok betartásáról.

Amennyiben a személyes adatok kezelése során az adatkezelő figyelmen kívül hagyja az Avtv.-nek a felhasználói hozzájárulásra vonatkozó rendelkezéseit, az adatkezelés jogszerűsége kétségbe vonható. Jogellenes adatkezelés esetén a felhasználó több, akár párhuzamosan is megindítható eljárást kezdeményezhet személyes adatainak védelme érdekében. A felhasználó így többek között az adatvédelmi biztos eljárását kérheti az Avtv. 25.§-a alapján[11], továbbá az Avtv. 17.§-a alapján az érintett jogainak megsértése esetén bírósághoz fordulhat, valamint a megfelelő törvényi feltételek megléte esetén

[11] Avtv. 25.§ alapján az adatvédelmi biztos felszólíthatja az adatkezelőt a jogellenes adatkezelés megszüntetésére, melynek eredménytelensége esetén elrendelheti a jogosulatlanul kezelt adatok zárolását, törlését, megsemmisítését, megtilthatja az adatkezelést vagy adatfeldolgozást, továbbá tájékoztathatja a nyilvánosságot eljárásáról.

büntetőeljárás, illetőleg szabálysértési eljárás is kezdeményezhető a jogsértő féllel szemben[12].

5.2.2 Felhasználói föderációs azonosító használata

Alapvető követelményként fogalmazható meg a föderáción belüli adattovábbítást illetően, hogy a felhasználóhoz kapcsolódó felhasználói föderációs azonosító („kulcs") ne egy olyan személyes azonosító legyen, amely alapján a felhasználó azonosítása az Azonosító Szervezeten kívül más személy vagy intézmény számára könnyen elvégezhető. A Felhasználói hozzájárulás kapcsán kifejtett tájékoztatási kötelezettség alapján az adatkezelőnek megfelelően tájékoztatni kell a felhasználót arról, hogy személyes adataival mi történik az adatkezelés során. Az olyan azonosító esetében, amely elsősorban gép általi értelmezésre alkalmasak a felhasználó számára nem az adat értelmezhetősége a lényeges, hanem az, hogy az adatkezelés folyamata, az adat életútja legyen előzetesen röviden és érthetően feltárva a felhasználó számára, hogy az így felvázolt adatkezeléshez egyértelműen hozzá tudjon járulni, illetőleg hozzájárulását megfelelően vissza tudja vonni (l. részletesen Felhasználói hozzájárulás).

Általában elmondható, hogy ha a Tartalomszolgáltató nem kapja meg az autorizációhoz vagyis az erőforrásokhoz való hozzáférés engedélyezéshez szükséges valamennyi adatot, akkor azokat közvetlenül kéri el a felhasználótól. Az adatok kezeléséhez való hozzájárulás beszerzése, az adatkezelésnek az Avtv.-ben előírt feltételeknek való megfelelése ebben az esetben is az adatot kérő tartalomszolgáltató feladata és felelőssége. A Tartalomszolgáltató által elkért további adatokhoz való hozzájárulás esetében NIIF AAI számára ajánlatos lehet előírni az Azonosító Szervezetek védelmében, hogy csak olyan Tartalomszolgáltatók lehetnek tagjai a föderációnak, akik a felhasználó hozzájárulását az így elkért adatok tekintetében is az Adatvédelmi törvény rendelkezéseinek megfelelően szerzik be és az adatokat is ennek megfelelően kezelik[13].

Noha a NIIF AAI nem kívánja szigorú keretek közé szorítani, a szervezetek választását az azonosítókat illetően, azonban célszerű lehet, hogy a NIIF AAI

[12] Büntető Törvénykönyv (1978. évi IV. törvény) 177/A.§-a alapján, aki a személyes adatok védelméről vagy kezeléséről szóló törvényi rendelkezések megszegésével jogtalan haszonszerzési célból vagy jelentős érdeksérelmet okozva a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel, b) az adatok biztonságát szolgáló intézkedést elmulasztja, vétséget követ el, és egy évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő. A Szabálysértésekről 218/1999. (XII. 28.) Korm. Rendelet 26. §.-a alapján aki a) a technikai adatvédelem követelményeinek nem tesz eleget, b) az érintettet a személyes adatok védelméhez, illetőleg a közérdekű adatok nyilvánosságához való jogának gyakorlásában akadályozza, hatvanezer forintig terjedő pénzbírsággal sújtható. Ez utóbbi esetben a kerületi, települési jegyző jogosult eljárni az adatvédelmi szabálysértés ügyében.

[13] A konkrét javaslatok megfogalmazása a későbbiekben elkészítendő föderációs adatkezelési és adatvédelmi szabályzat, valamint a Tartalomszolgáltatók adatkezelését átfogó adatvédelmi ajánlás részét fogja képezni.

ajánlás formájában fogalmazza meg, mely azonosítók használata tekinthető célszerűnek, illetve, hogy az egyes azonosítók használata esetén mik az előnyök és hátrányok, adatvédelmi, illetve adatbiztonsági szempontokat figyelembe véve. Fontos eszköze lehet a föderatív szervezet működőképességének és az egyes entitások által követett gyakorlatok nyomon követése során egy központi föderációs nyilvántartás vezetése arról, hogy az egyes SP-k milyen azonosítót használnak.

5.2.3 Metadata

Figyelemmel arra, hogy a metadata fájl publikus és így mindenki számára nyilvánosan hozzáférhető és letölthető, ezért az aláírt metadata fájlok felhasználási feltételeit a föderációnak egyértelműen meg kellene határoznia. A föderáció tagjai közötti együttműködés során nem kerülhet sor tehát a metadata fájlban szereplő információknak azok eredeti céljával ellentétes használatára. A felhasználási feltételeknek és a használathoz szükséges ajánlások és szabályok megfogalmazására a föderáció központi szervezeti szintjén van szükség.

Figyelemmel arra, hogy a metadata fájlok tartalmaznak személyes adatokat is, így a technikai és adminisztratív kapcsolattartó személyek elérhetőségére vonatkozó adatokat, az ezen adatok kezeléséhez történő hozzájárulás az adatalanyok részéről elengedhetetlen.[14] A hozzájárulás megadásával egy időben az érintett személyeket tájékoztatni kell arról is, hogy személyes adataik kezelésének célja az egyes intézmények közötti kommunikáció és bizalom kiépítésével összhangban az elérhetőség biztosítsa, továbbá tájékoztatni kell őket arról is, hogy személyes adataikkal mi fog történnie és mi történhet a föderatív együttműködés keretében. Az adatalanyok hozzájárulásának beszerzése és a hozzájárulással kapcsolatos dokumentumok adminisztrációja minden esetben az adott intézmény feladata.

5.2.4 Naplózás

Az NIIF AAI-ban minden adatkezelési folyamathoz kapcsolódóan történik naplózás.

5.3 Egyes adatkezelési folyamatok értékelése

5.3.1 IdP AAI kapu adatbázis feltöltés

[14] l. részletesen Felhasználói hozzájárulás.

Az intézményi adatbázisban, címtárban szereplő adatoknak az IdP AAI adatbázisába történő átadása, olyan adatmozgás, amely intézményen belüli, belső adattovábbításnak tekintendő, így nem okoz adatvédelmi szempontból problémát az IdP adatbázis feltöltése, ha az anyaintézmény által korábban, a felhasználónak személyes adatai kezeléséhez való hozzájárulása erre az adatkezelésre is kiterjedt.

5.3.2 IdP AAI kapu adattárolás és karbantartás

Az adatok tárolása és karbantartása során figyelemmel kell lenni az Avtv. szerinti adatminőség biztosítására vonatkozó követelményekre. Az Adatvédelmi törvény rendelkezései alapján, az adatkezelés során a személyes adat felvételének és kezelésének nemcsak tisztességesnek és törvényesnek kell lennie[15], de az így rögzített adatnak pontosnak, teljesnek és ha szükséges időszerűnek is kell lennie. A személyes adat tárolási módjának alkalmasnak kell lennie arra, hogy az érintettet felhasználót csak a tárolás céljához szükséges ideig lehessen azonosítani.[16]

Amennyiben a rögzített adatok egy ún. authoritatív adatbázisban rögzített adatok alapján folyamatosan frissülnek, és ezért az adatok időszerűsége, pontossága nem vitatott, akkor az adatminőséggel kapcsolatos adatvédelmi követelmények teljesítése kevesebb problémát jelent, azonban ha az adatok egy nem autoritatív, vagyis nem megbízható és a változásokat folyamatosan nem követő rendszerből származnak, akkor külön gondot kell fordítani az IdP üzemeltetése során arra, hogy az adatminőséggel kapcsolatos követelményeknek az IdP adatkezelése megfeleljen..

5.3.3 IdP AAI kapu választás

A Keresőszolgáltatás esetében az adatkezeléshez való hozzájárulásnak az IP cím, valamint a felhasználó választására kell kiterjednie, tehát a felhasználónak tisztában kell lennie azzal, hogy a DS alkalmazás használata során mind az IP címe, mind az őt azonosítani képes IdP-re vonatkozó választása tárgya az adatkezelésnek. Az előválasztó felületen megjelenített tájékoztató, illetve a tartós cookie elfogadására vonatkozó hozzájárulás megadása mindenképpen szükséges. A Keresőszolgáltatás rendelkezésére áll egyrészt a felhasználó IP címe, a felhasználó választásától függően pedig az az adat is, hogy a felhasználót melyik IdP azonosítja. Amennyiben a felhasználó külön hozzájárul ahhoz, hogy a Keresőszolgáltatás megjegyezze a választását, a DS a cookie elhelyezésével adatokat rögzít, és így adatkezelést

[15] Az adatkezelés során a korábban ismertetett adatkezelési és felhasználói hozzájárulással kapcsolatos feltételeknek eleget kell tenni.

[16] Avtv. 7.§

végez, amely adatkezeléshez szükség van a felhasználó hozzájárulására. Hozzájárulás megadható oly módon, hogy a felhasználó az elővalasztó felületen ad engedélyt az adatok rögzítéséhez, azonban megfelelően tájékoztatni kell a felhasználót arról is, hogy mennyi ideig tárolódik a cookie, továbbá, hogy az adatkezeléssel kapcsolatos tiltakozási jogával úgy élhet, hogy a cookiet kitörli a browseréből. Szintén tájékoztatni kell a felhasználót arról, hogy egyébként az adatkezelés időtartama a cookie lejárati idejének vége.

5.3.4 Felhasználó bejelentkezés

A felhasználó bejelentkezése a korábban említetteknek megfelelően két lépésből álló adatkezelési folyamat első lépése a felhasználó azonosításának folyamata, míg a második adatkezelési lépés a felhasználóra vonatkozó attribútumok továbbításának folyamata, amely tulajdonképpen az Azonosító Szervezet és a Tartalomszolgáltató közötti üzenetváltásokon alapul.

A megbeszélések során egyértelműen megfogalmazódott az a föderációs alapelv, hogy az egyes entitások autonóm módon dönthessék el, hogy milyen attribútumokat kérnek és milyen attribútumokat adnak ki a föderatív együttműködés keretei között. Ennek megfelelően mind az Attribútum kiadása, mind a kiadás rendjét alapvetően meghatározó Attribútum specifikáció meghatározása során figyelemmel kell lenni arra, hogy az egyes entitások csak a működésükhöz feltétlenül szükséges adatok kiadását követeljék meg, illetőleg a föderáció ezt a gyakorlatot támogassa.

Szükséges lehet, egy olyan belső eljárási rend kialakítása is, amely az újonnan csatlakozó SP-k által kért adatokat illetően tartalmaz ajánlásokat, így például arról, hogy milyen adatok igényelhetőek egyáltalán az SP-k által.

A Tartalomszolgáltatók által kért attribútumokra vonatkozóan fontos megemlíteni azt, hogy az Adatvédelmi törvény alapján a különböző adatkezelési folyamatoknak minden esetben meg kell felelniük a célhoz kötöttség elvének. Az Avtv. 5. § alapján személyes adatot kezelni csak meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében lehet. Az adatkezelésnek minden szakaszában meg kell felelnie e célnak. Továbbá, csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, csak a cél megvalósulásához szükséges mértékben és ideig. A föderáció tagjaiként résztvevő Tartalomszolgáltatók a személyes adatok kérése és kezelése során ezen alapelvnek megfelelően kötelesek eljárni.

A Felhasználó által az azonosítás céljából megadott felhasználó név és jelszó átadásához, valamint a föderatív együttműködéshez szükséges attribútumok entitások közötti cseréjéhez a felhasználónak vagy itt, az adatok megadásakor vagy a Felhasználó személyes adatainak az anyaintézmény adatbázisába történő adatbevitel idején hozzá kell járulnia. Fontos megjegyezni, hogy minden esetben a felhasználó hozzájárulásának határozottnak és megfelelő

tájékoztatáson alapulónak kell lennie, továbbá ez a hozzájárulás bármikor visszavonható kell, hogy legyen az Adatvédelmi törvényben biztosított tiltakozási jognak megfelelően. A megfelelő tájékoztatáson alapuló hozzájárulás további feltétele az érintett tisztában legyen az adatfelvétel önkéntességéről.[17]

5.3.5 Szolgáltatás igénybevétele

A Szolgáltatás igénybevétele azt a köztes folyamatot jelöli, amikor a felhasználó azonosítása az IdP oldalán megtörtént és így az SP számára szükséges autorizációhoz az adatokat az Azonosító Szervezet eljuttatja a Tartalomszolgáltató részére. Ez a folyamat az Avtv. szerinti adattovábbítás, vagyis a törvény által külön nevesített adatkezelési mód[18]. Ennek az adatkezelési folyamatnak nem része az az adatkezelés, amelyet az SP oldali szolgáltatás végez, a szolgáltatás használata közben. Az Azonosító Szervezet által a Tartalomszolgáltató részére átadott attribútumok körét az Attribútum kiadási Szabályzatban egyrészt a lehető legszűkebb körben kell meghatározni, illetőleg az így átadott attribútumok, tehát személyes adatok sorsáról a Felhasználót megfelelően tájékoztatni kell. Fontos, hogy ennek a tájékoztatásnak, még a szolgáltatás igénybevétele előtt, tehát az attribútumoknak az SP részére történő kiadása előtt meg kell történnie. Az IdP AAI elem általi azonosítás megtörténtekor, még az SP AAI Kapu részére az attribútumok átadását megelőzően célszerű a felhasználó egyedi, az adott adattovábbításra vonatkozó hozzájárulásának a beszerzésére. Az egyedi, az adott adatkezelési folyamatra vonatkozó eseti felhasználói hozzájárulás adatvédelmi szempontból kedvezőbb, mint egy általános felhasználói hozzájárulás, amelyet a felhasználó az adatainak az Azonosító Szervezet saját intézményi vagy az IdP AAI föderációs adatbázisába való bekerülésekor ad. Az így egyedileg megadott felhasználói hozzájárulás alkalmazása révén a felhasználók az Avtv. által biztosított jogaikkal úgy tudnak élni, hogy az egyedi adatkezelés esetében, egy-egy tartalomszolgáltatás igénybevétele során külön-külön is eldönthetik, hogy adataik kezeléséhez valóban hozzá kívánnak-e járulni. Az egyedileg megadott felhasználói hozzájárulás megadásához szolgálhat eszközként például a uApprove alkalmazás.[19]

5.3.6 SP oldali szolgáltatás adatkezelése

Az SP által üzemeltetett alkalmazás esetében, maga a Tartalomszolgáltató felel az alkalmazás részére átadott személyes adatok biztonságáért,

[17] Részletes szabályokat l. Felhasználó hozzájárulás cím alatt.

[18] l. Definíciók d) pont.

[19] l. Emlékeztető VIII. Felhasználói hozzájárulás

védelméért. A Felhasználó hozzájárulásának megfelelő tájékoztatáson kell alapulnia, továbbá ki kell terjedni személyes adatainak kezelésével járó teljes folyamatra. Ez az adatkezelési folyamat az SP Szolgáltatás saját belső adatvédelmi szabályainak és rendelkezéseinek megfelelően kell, hogy működjön, mivel a föderációs adatkezelésnek ez a folyamat már nem része, ezért az erre vonatkozó adatvédelmi rendelkezések és előírások összefoglalása és betartatása nem a föderáció hatáskörébe tartozik.

Mellékletek

Attribútum specifikáció és Felsőoktatási törvényen alapuló adatkezelés

A felsőoktatásról szóló 2005. évi CXXXIX. törvény 34.§-a tartalmazza a felsőoktatási intézményekben történő adatkezelés alapvető szabályait, valamint a felsőoktatás információs rendszerre vonatkozó előírásokat.

A hivatkozott rendelkezés alapján a felsőoktatási „intézmény kezelheti a hallgató személyének azonosítására és elérhetőségére szolgáló adatokat (név, születési hely, idő, állampolgárság, állandó lakóhely és tartózkodási hely, telefonszám), valamint a hallgatói jogviszonnyal összefüggő adatokat. Ez utóbbi körben különösen a felvételeivel kapcsolatos adatokat, hallgató tanulmányainak értékelését és minősítését, a vizsgaadatokat, a hallgatói fegyelmi és kártérítési ügyekkel kapcsolatos adatokat.” Más törvények az intézmény számára kötelezően előírják bizonyos személyes adatok kezelését, bizonyos esetekben köteles például nyilvántartani a hallgató adóazonosító jelét, társadalombiztosítási azonosító számát, mivel bevallási, illetve a különböző fizetési kötelezettségének csak így tud eleget tenni.

Minden más adatot csak akkor kezelhet az intézmény, ha ahhoz az érintett előzetesen hozzájárult. A kezelt adatokat csak akkor lehet az intézményen kívülre továbbítani, ha az érintett ehhez előzetesen hozzájárult, illetve ha az adattovábbítást törvény előírja.

A felsőoktatási törvény 34.§ alapján a felsőoktatási intézmény rendeltetésszerű működéséhez, munkáltatói jogok gyakorlásához, alkalmazottak kedvezményekre való jogosultság elbírálásához és igazolásához szükséges adatok, valamint a beiratkozott hallgatók törzslapja. Az adatkezelés és továbbítás rendjét az intézményi Szervezeti és Működési Szabályzat írja le, vagyis ebből a szempontból az egyes intézmények (IdP-k) SZMSZ az irányadó.

A felsőoktatás törvény 2. sz. melléklete rendelkezik a felsőoktatási intézményekben nyilvántartott és kezelt személyes és különleges adatokról. A melléklet alapján a felsőoktatási intézmény a hallgatók adatait illetően a törvény alapján a következő adatokat tarthatja nyilván:

a) felvétellel összefüggő adatok:

[...]

b) a hallgatói (kollégiumi tagsági, doktorjelölt) jogviszonnyal összefüggő adatok:

ba) a hallgató neve, születési neve, anyja neve, születési helye és ideje, állampolgársága, bejelentett lakóhelyének, tartózkodási helyének címe, értesítési címe és telefonszáma, elektronikus levélcíme, nem magyar állampolgár esetén a Magyar Köztársaság területén való tartózkodás jogcíme és a tartózkodásra jogosító okirat - külön törvény szerint a szabad mozgás és tartózkodás jogával rendelkező személyek esetén a tartózkodási jogot igazoló okmány - megnevezése, száma,

bb) a hallgatói (kollégiumi tagsági, doktorjelölti, vendéghallgatói) jogviszonya keletkezésének és megszűnésének időpontja és módja, a hallgató által folytatott képzés megnevezése, állami támogatottsága és munkarendje, a hallgató tanulmányainak értékelése, vizsgaadatok, megkezdett félévek, igénybe vett támogatási idő, a hallgatói jogviszony szünetelésének ideje,

be) a hallgatói juttatások, kollégiumi elhelyezés adatai, a juttatásokra való jogosultság elbírálásához szükséges adatok (szociális helyzet, szülők adatai, tartásra vonatkozó adatok),

bf) a hallgatói munkavégzés adatai,

bg) a hallgatói fegyelmi és kártérítési ügyekkel kapcsolatos adatok,

bh) a fogyatékossággal élőket megillető különleges bánásmód elbírálásához szükséges adatok,

bi) a hallgatói balesetre vonatkozó adatok,

bj) a hallgató diákigazolványának sorszáma, a törzslap azonosító száma,

bk) a hallgató azonosító száma, társadalombiztosítási azonosító jele,

bl) a záróvizsgára (szakmai vizsgára, doktori védésre) vonatkozó adatok,

bm) a hallgatói jogviszonyból adódó jogok és kötelezettségek teljesítéséhez szükséges adatok;

c) a hallgatói pályakövetéssel kapcsolatos adatok;

d) a hallgató adóazonosító jele;

e) az adatokat igazoló okiratok azonosítására szolgáló adatok.

A fentiekben felsorolt adatokon kívüli adat kizárólag az érintett hozzájárulásával tartható nyilván, kezelhető.

Megjegyzendő, hogy az egyes, intézményi azonosítók, mint a Neptun-kód, ETR-kód stb., a felsőoktatási törvényben külön nem nevesített hallgatói azonosító kódoknak tekinthetőek. Ezek az azonosítók valójában olyan kapcsolati kódok, amelyek a felsőoktatási intézmény hallgatóinak az intézményen belüli azonosítására szolgál, vagyis felsőoktatási intézmény a belső, elektronikus ügyintézési rendszerében történő azonosításra szolgál. Az adatalanyokat kóddal azonosítjuk, egy másik adatkezelésben

pedig a kódot a kívánt információval kapcsoljuk össze, így két különböző adatkezelésen keresztül hozzuk kapcsolatba az adatalanyt és az információ. Az így kialakított és az intézmény belső használatában alkalmazott azonosító kódokra a felsőoktatási törvény adatkezelési engedélye nem terjed ki, tehát ezek csak az érintett hozzájárulásával tartható nyilván, kezelhető.

A hivatkozott melléklet kimondja továbbá, az adatok továbbíthatóságával kapcsolatban, hogy a felsőoktatási intézmény (1) fenntartója részére valamennyi adat, amely a fenntartói irányítással összefüggő feladatok ellátásához szükséges; (2) a bíróságnak, (3) rendőrségnek, (4) ügyészségnek, a (5) bírósági végrehajtónak, (6) államigazgatási szervnek a konkrét ügy eldöntéséhez szükséges adat; a (7) nemzetbiztonsági szolgálat részére valamennyi adat; a (7) felsőoktatási információs rendszer működéséért felelős szerv (Oktatási Hivatal) részére valamennyi adat; a (8) Diákhitel Központnak a tanulmányok folytatásával összefüggő adatok.

A fenti törvényhely alapján a föderatív együttműködés keretében átadott adatok tekintetében a felsőoktatási törvény által biztosított törvényen alapuló adatkezelés nem alkalmazható. Ennek megfelelően a felhasználók hozzájárulásának beszerzése minden esetben szükséges.

A felsőoktatásról szóló 2005. évi CXXXIX. törvény egyes rendelkezéseinek végrehajtásáról szóló 79/2006. (IV. 5.) Korm. rendelet 15/B-C.§-a rendelkezik a hallgató (doktorjelölt) személyes és tanulmányi adatainak nyilvántartására szolgáló törzslapról, amelyet a felsőoktatási intézmények kötelesek vezetni. A Kormány rendelet 15/E és F.§-a rendelkezik a hallgató beiratkozási, valamint a doktorjelölt regisztrációs lapjáról, illetve az azokon nyilvántartott adatok köréről és a nyilvántartásra vonatkozó szabályokról.

A fentebb hivatkozott törvényhelyek szolgálnak iránymutatásul az egyes „anyaintézmények” által nyilvántartott, a föderációban használt személyes adatok kezelésekor. Így különösen fontos kiemelni, hogy a felsőoktatási intézmény hallgatójának a 15/E.§ (3) bekezdésben foglaltak szerinti a hallgatói adatkezelési nyilatkozatáról, amely a beiratkozási lap mellékletét képezi. A Kormány rendelet 15./N.§-a alapján a hallgatói adatkezelési nyilatkozat a nem kötelezően kezelt adatok kezeléséhez való hozzájárulásra szolgál, és mint kötelező formanyomtatvány a felsőoktatási intézmény alkalmazni köteles.[20]

Emlékeztető

ld. külön dokumentum

[20] A hallgató adatkezelési nyilatkozat formanyomtatvány mintaszövege a 79/2006. (IV. 5.) Korm. rendelet 10. sz. mellékletének részét képezi (l. IX. pont)