Iktatószám: TF/RH/65 /2026

A Magyar Testnevelési és Sporttudományi Egyetem

rektorának

2026. évi 2. sz. rendelkezése

az elektronikus aláírások és elektronikus bélyegzők használatáról szóló szabályzatról

A Magyar Testnevelési és Sporttudományi Egyetem (a továbbiakban: Egyetem) Szervezeti és Működési Szabályzatának 1. rész (Szervezeti és Működési Rend) 15. § (6) bekezdése szerinti felhatalmazás alapján az alábbi rendelkezést adom ki:

1. §

Az Egyetem elektronikus aláírások és elektronikus bélyegzők használatáról szóló szabályzatát az 1. sz. melléklet tartalmazza.

2. §

Jelen rendelkezés az aláírását követő napon lép hatályba. A jelen rendelkezésben nem szabályozott kérdésekben a vonatkozó hatályos jogszabályok, különösen a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény (Dáp. tv.) és a végrehajtási rendeletei az irányadók.

3. §

Jelen rendelkezés közzétételre kerül az Egyetem honlapján.

Budapest, 2026. március 3.

Magyar Testnevelési és Sporttudományi Egyetem Rektor Budapest

Prof. Dr. Sterbenz Tamás
rektor

1. sz. melléklet

MAGYAR TESTNEVELÉSI ÉS SPORTTUDOMÁNYI EGYETEM

Elektronikus aláírások és elektronikus bélyegzők használatáról szóló szabályzat

Budapest, 2026.

TARTALOMJEGYZÉK

1. § A SZABÁLYZAT CÉLJA 4
2. § A SZABÁLYZAT HATÁLYA 4
3. § ELEKTRONIKUS ALÁÍRÁSBAN ÉRINTETT SZEMÉLYEK ÉS SZERVEZETEK KÖRE 4
4. § AZ ELEKTRONIKUS ALÁÍRÁS ÉS AZ ELEKTRONIKUS BÉLYEGZŐ ALKALMAZÁSA 5
5. § AZ ELEKTRONIKUS ALÁÍRÁS-LÉTREHOZÓ ESZKÖZ VAGY SZOFTVER HASZNÁLATÁNAK RENDJE 6
6. § AZ ELEKTRONIKUS ALÁÍRÁS ÉS ELEKTRONIKUS BÉLYEGZŐ ÉRVÉNYESSÉGÉRE VONATKOZÓ KÖZÖS SZABÁLYOK 7
7. § AZ EGYETEM KÉPVISELETÉBEN HASZNÁLT ALÁÍRÁSI TANÚSÍTVÁNYOK KEZELÉSÉNEK RENDJE 8
8. § AZ ELEKTRONIKUS ALÁÍRÁSSAL ÉS ELEKTRONIKUS BÉLYEGZŐVEL RENDELKEZŐ DOKUMENTUMOK HOSSZÚ TÁVÚ MEGŐRZÉSE (ARCHIVÁLÁSA) 9
9. § ÉRTELMEZŐ RENDELKEZÉSEK 10

1. § A SZABÁLYZAT CÉLJA

(1) Az elektronikus aláírások és elektronikus bélyegzők használatáról szóló szabályzat (a továbbiakban: Szabályzat) célja a Magyar Testnevelési és Sporttudományi Egyetem (a továbbiakban: Egyetem) elektronikus kiadmányozási szabályainak megállapítása, a dokumentumok hitelesítésére szolgáló elektronikus aláírások és elektronikus bélyegzők használatára, nyilvántartására, valamint az elektronikus aláírással, elektronikus bélyegzővel ellátott dokumentumok ellenőrzésére vonatkozóan, a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvénnyel (Dáp. tv.), valamint végrehajtási rendeleteivel összhangban.

(2) A Szabályzat meghatározza:

a) az Egyetem hatáskörébe tartozó ügyek során az Egyetem által alkalmazható elektronikus aláírási és elektronikus bélyegzési megoldásokat;

b) a hitelesítés-szolgáltatóval és időbélyegzéssel kapcsolatos megkötéseket;

c) az elektronikusan aláírt vagy elektronikusan bélyegzett dokumentumok elküldésének, értelmezésének, illetve ellenőrzésének szabályait.

2. § A SZABÁLYZAT HATÁLYA

(1) A szabályzat személyi hatálya kiterjed az Egyetem valamennyi szervezeti egységére – ideértve a fenntartásában működő köznevelési intézményt is – és munkavállalójára.

(2) A Szabályzat tárgyi hatálya kiterjed:

a) a kiadmányozásra vagy aláírásra jogosultak által az Egyetem hatáskörébe tartozó ügyek során az elektronikus formában létrehozott, elektronikus aláírással és időbélyeggel, vagy elektronikus bélyegzővel és időbélyeggel ellátott dokumentumok készítésére;

b) az Egyetem által elektronikus aláírással vagy elektronikus bélyegzővel ellátott küldemények hivatali kapun keresztül vagy egyéb elektronikus úton történő megküldésére;

c) az elektronikus aláírással, illetve időbélyegzővel ellátott dokumentumok hosszú távú megőrzési kötelezettsége miatt szükséges archiválásra.

3. § ELEKTRONIKUS ALÁÍRÁSBAN ÉRINTETT SZEMÉLYEK ÉS SZERVEZETEK KÖRE

(1) Az Egyetemen az elektronikus aláírási tanúsítvány használatára jogosultak:

a) Az Egyetemen kiadmányozási jogot a Szervezeti és Működési Szabályzat 1. részében (Szervezeti és Működési Rend) meghatározott vezetők gyakorolnak az ott, valamint az adott szervezeti egység ügyrendjében és az egyéb vonatkozó egyetemi szabályzatokban meghatározottak szerint.

b) Az Egyetemen elektronikus aláírási tanúsítvány használatára a rektor és az általa meghatározott vezetők jogosultak.

c) Az elektronikus aláírás és elektronikus időbélyegző használatára jogosult jogosultságát kizárólag az SZMR-ben meghatározott feladat- és hatáskörébe tartozó ügyekben, az Egyetem képviseletében eljárva alkalmazhatja. Az elektronikus aláírás és elektronikus időbélyegző a jogosult feladat- és hatáskörébe nem tartozó ügyekben, illetve magáncélra nem használható fel.

(2) Az Egyetem külső partnerei:

Azon természetes és jogi személyek, illetve jogi személyiség nélküli szervezetek, amelyek részére az Egyetem a feladat- és hatáskörébe tartozó ügyviteli eljárások során elektronikus formában készített és elektronikusan aláírt vagy elektronikus bélyegzővel ellátott dokumentumot hivatali kapun vagy egyéb elektronikus csatornán továbbít vagy tőlük fogad.

(3) A bizalmi szolgáltató

a) A Dáp tv. szerinti olyan természetes vagy jogi személy, aki a hitelesítési szolgáltatás keretében azonosítja az igénylő személyét, tanúsítványt bocsát ki, nyilvántartásokat vezet, fogadja a tanúsítványokkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a tanúsítványhoz tartozó szabályokat, az aláírás-ellenőrző adatokat és a tanúsítvány aktuális állapotára (különösen esetleges visszavonására) vonatkozó információkat.

b) Az elektronikus kiadmányozásra vagy aláírásra jogosult vezető kiadmányozási vagy aláírási jogának igazolása a bizalmi szolgáltató által előírt formában tett jognyilatkozatban történik.

c) A bizalmi szolgáltató állítja elő és személyes beazonosítást követően bocsátja az arra jogosult vezető rendelkezésére az elektronikus aláírás létrehozásához szükséges tanúsítványt.

(4) A Jogi Igazgatóság

a) Az Egyetem szervezeti (intézményi) kapcsolattartója a bizalmi szolgáltató felé a jogi igazgató.

b) A jogi igazgató gondoskodik az Egyetem és a bizalmi szolgáltató közötti megállapodások előkészítéséről.

c) A jogi igazgató feladata az elektronikus aláírások, elektronikus bélyegzők, időbélyegekkel kapcsolatos igények felmérése, javaslattétel a rektor számára azok engedélyezésére, valamint a kapcsolódó operatív feladatok koordinálása (elektronikus aláíró és bélyegző tanúsítványok megrendelése, visszavonása, felfüggesztése, lejáratuk nyomon követése).

d) Az elektronikus aláírásra és az elektronikus bélyegző létrehozására használt, átadott tanúsítványok nyilvános adatait, a használatra jogosult átvevő személy nevét a Jogi Igazgatóság által vezetett, elektronikus aláírásokra vonatkozó nyilvántartás tartalmazza.

(5) Informatikai Iroda

a) Az Informatikai Iroda vezetője gondoskodik az elektronikus aláíró és bélyegző tanúsítványok biztosításához és használatához szükséges informatikai feltételek megteremtéséről, a szolgáltatás igénybevételéhez, használatához szükséges műszaki infrastruktúra biztosításáról, szükség esetén a bizalmi szolgáltatóval történő együttműködésben.

b) Az Informatikai Iroda feladata az elektronikus aláíró és bélyegző tanúsítványok használatához szükséges informatikai beállítások elvégzése és a jogosultak számára az egyéb szükséges informatikai szakmai támogatás biztosítása.

4. § AZ ELEKTRONIKUS ALÁÍRÁS ÉS AZ ELEKTRONIKUS BÉLYEGZŐ ALKALMAZÁSA

(1) Az Egyetem a feladat- és hatáskörébe tartozó ügyek ellátása során a vonatkozó jogszabályokban rögzítetteknek megfelelően elektronikus kapcsolattartást biztosíthat.

(2) Az Egyetem az (1) bekezdés szerinti feladatellátása során törekszik arra, hogy a természetes és jogi személyek, illetve jogi személyiség nélküli szervezetek részére – amennyiben a körülmények

lehetővé teszik – elektronikus formában készített, legalább fokozott biztonságú elektronikus aláírással, vagy elektronikus bélyegzővel és időbélyegzővel ellátott dokumentumot továbbítson.

(3) Az elektronikus dokumentumok hitelesítése elektronikus bélyegzővel történik kivéve, ha jogszabály kifejezetten elektronikus aláírás alkalmazását írja elő, vagy ha a jogszabály a kiadmányozás vagy aláírás jogosultságát személyhez rendeli. Ebben az esetben az elektronikus aláírással rendelkező vezető a kiadmányozás során elektronikus aláírást alkalmaz.

(4) A döntést nem tartalmazó elektronikus dokumentumok és nagy tömegben előállított értesítések, igazolások, tájékoztatók hitelesítése elektronikus bélyegzővel és időbélyegzővel történik.

(5) Az Egyetem által elektronikus formában készített és elektronikusan hitelesített dokumentumok a címzett részére elektronikus úton kerülnek kézbesítésre (hivatali kapun vagy e-mailen).

(6) Az elektronikus aláírási tanúsítvánnyal rendelkező vezető a bizalmi szolgáltató által biztosított szoftver segítségével helyezheti el elektronikus aláírását a kiadmányozásra kerülő dokumentumon. Az aláírásra jogosult személy számára szükséges informatikai támogatásról az Informatikai Iroda gondoskodik.

(7) Az Egyetem kiadmányozási jogosultsággal rendelkező vezetői által használt elektronikus aláírás és annak grafikus megjelenítése tartalmazza legalább az elektronikus aláírás használatára jogosult vezető személyazonosító okmányában (és az aláírási tanúsítványában) szereplő teljes nevét.

(8) Az Egyetem elektronikus bélyegző használatára jogosult vezetői, munkatársai által használt elektronikus bélyegző és annak grafikus megjelenítése tartalmazza legalább az Egyetem hivatalos megnevezését.

5. § AZ ELEKTRONIKUS ALÁÍRÁS-LÉTREHOZÓ ESZKÖZ VAGY SZOFTVER HASZNÁLATÁNAK RENDJE

(1) Az elektronikus aláírásra vagy kiadmányozásra jogosult vezető kizárólag intelligens chipkártya vagy token birtokában, és a hozzá tartozó jelszó megadásával, vagy felhőszolgáltatáson alapuló, kétfaktoros azonosítást biztosító szolgáltatás keretében (távoli kulcsos aláírás) a jelszó (pin kód) megadásával, illetve a bizalmi szolgáltató által biztosított szoftverrel hozhat létre minősített elektronikus aláírást az elektronikus dokumentumon.

(2) Az adott ügyben hatáskörrel rendelkező szervezeti egység vezetőjének felhatalmazása alapján elektronikus szakrendszerben (pl. Neptun, Poszeidon) létrehozható legalább fokozott biztonságú elektronikus aláírással, elektronikus bélyegzővel és időbélyeggel hitelesített elektronikus dokumentum.

(3) Az elektronikus aláírás használatára jogosult vezető köteles a részére kiadott intelligens chipkártyát vagy tokent biztonságos, zárható helyen tárolni.

(4) Az intelligens chipkártya vagy token elvesztése, illetve kompromittálódása, valamint az ahhoz tartozó jelszó elvesztése, elfelejtése esetén a tanúsítvány felfüggesztése vagy visszavonása ügyében a vezető az Egyetem Informatikai Biztonsági Szabályzatában (a továbbiakban: IBSZ) foglaltakra is figyelemmel köteles soron kívül bejelentést tenni az Informatikai Iroda vezetőjének és a jogi igazgatónak. A tanúsítvány felfüggesztéséről vagy visszavonásáról a jogi igazgató köteles intézkedni a bizalmi szolgáltatónál.

(5) Az elektronikus aláírásra vagy kiadmányozásra jogosult vezető nem adhatja át és nem teheti elérhetővé – átmenetileg sem – más részére az elektronikus aláíró eszközt, illetve a szoftver használatához szükséges azonosítókat, kódokat.

(6) A fentiekkel kapcsolatos bármely egyéb informatikai biztonságot érintő ügyben a vonatkozó jogszabályok és az IBSZ rendelkezései az irányadók.

6. § AZ ELEKTRONIKUS ALÁÍRÁS ÉS ELEKTRONIKUS BÉLYEGZŐ ÉRVÉNYESSÉGÉRE VONATKOZÓ KÖZÖS SZABÁLYOK

(1) Az Egyetemen keletkezett elektronikus aláírás vagy elektronikus bélyegzővel, időbélyegzővel ellátott dokumentum érvényes az alábbi feltételek együttes teljesülése esetén:

a) azt jelen Szabályzatban meghatározott jogosult;
b) a Szervezeti és Működési Rendben (SZMR) meghatározott feladat-és hatáskörében eljárva;
c) a dokumentum hitelesítéséhez az eljárásra vonatkozó jogszabályi követelményeknek megfelelő szintű és fajtájú;
d) sértetlen tartalmú;
e) a dokumentum létrehozásakor visszavonás, vagy felfüggesztés hatálya alatt nem álló olyan elektronikus aláírási vagy elektronikus bélyegző és elektronikus időbélyegző tanúsítványt alkalmaz, amelynél nem áll fenn érvénytelenségi ok.

(2) Az Egyetemre érkező elektronikus aláírással, vagy elektronikus bélyegzővel ellátott dokumentum címzettjének a legnagyobb körültekintéssel kell eljárnia az elektronikus aláírás és az ahhoz tartozó tanúsítvány elfogadása során, ezért az elektronikusan átvett dokumentumon az érvényességi lánc vizsgálatával az elektronikus aláírás ellenőrzésének elvégzése a címzett felelősségi körébe tartozik.

(3) Az Egyetemre érkező elektronikusan aláírt dokumentum hitelességének ellenőrzése magában foglalja:

a) a dokumentum sértetlenségének (a dokumentum tartalma az aláírás óta nem változott);
b) a tanúsítványnak (az aláírást az a személy vagy szervezet készítette, aki vagy amely aláíróként meg van jelölve); valamint
c) az időbélyegnek (a dokumentumot az időbélyegben szereplő időpontban írta alá az aláíró és azóta annak tartalma nem változott meg) az ellenőrzését.

(4) Az elektronikus aláírás, valamint elektronikus bélyegző és az ahhoz tartozó tanúsítvány ellenőrzése az alábbiakra terjed ki:

a) az elektronikus aláíráshoz tartozó aláírási tanúsítvány segítségével azonosítani kell az aláírási tanúsítványt kibocsátó bizalmi szolgáltatót;

b) az aláírási tanúsítványt kibocsátó bizalmi szolgáltató tanúsítványának segítségével meg kell győződni az aláírási tanúsítvány integritásáról;
c) az aláírási tanúsítvány és az azt kibocsátó Bizalmi Szolgáltató tanúsítványának állapotát (érvényességét) ellenőrizni kell a tanúsítvány visszavonási listák alapján;
d) meg kell vizsgálni az aláírási tanúsítvány összes attribútumát, beleértve a hitelesítési rendet is.

(5) Az elektronikus aláírás, az elektronikus bélyegző, és az ezekhez tartozó tanúsítvány ellenőrzését a megfelelő aláírás ellenőrző szoftver (pl. e-szignó, Acrobat Reader) segítségével szükséges elvégezni.

a) Nem fogadható el az elektronikus aláírás, ha az elektronikus aláírás, az aláírási tanúsítvány vagy az érvényességi lánc valamely tanúsítványának valamely adata az aláírás érvénytelenségére utal, vagy a lefuttatott hitelességellenőrzés során az eredmény érvénytelenségre enged következtetni.

b) Nem fogadható el az időbélyeg, ha az időbélyegen elhelyezett elektronikus aláírás vagy elektronikus bélyegző tanúsítványa, vagy az érvényességi lánc tanúsítványának valamely adata annak érvénytelenségére utal.

c) Az elektronikus aláírással ellátott dokumentum ügyintézőjének felelősségi körébe tartozik az elektronikusan átvett dokumentumon az érvényességi lánc vizsgálatával az elektronikus aláírás ellenőrzésének elvégzése.

7. § AZ EGYETEM KÉPVISELETÉBEN HASZNÁLT ALÁÍRÁSI TANÚSÍTVÁNYOK KEZELÉSÉNEK RENDJE

(1) Ha az elektronikus aláírás használatára jogosult kiadmányozási, illetve aláírási jogosultsága megszűnik, a tanúsítvány visszavonása iránti igényt köteles ő vagy a közvetlen munkahelyi vezetője a jogi igazgató részére írásban, haladéktalanul megküldeni. A jogi igazgató köteles kezdeményezni a visszavonási eljárást a bizalmi szolgáltatónál.

(2) A tanúsítványt haladéktalanul vissza kell vonni továbbá:

a) a jogosult nevében történt változás esetén,

b) ha a tanúsítványban szereplő adatok nem felelnek meg a valóságnak,

c) a bizalmi szolgálató adataiban történt változás esetén.

(3) A visszavonással a tanúsítvány végérvényesen érvényét veszti, és a visszavont tanúsítvány alapján létrehozott elektronikus aláírás a továbbiakban dokumentumok hitelesítésére nem alkalmas.

(4) Az elektronikus aláírási jogosultsággal rendelkező vezető visszavonási, illetve módosítási eljárást köteles kezdeményezni, ha a neve, munkaköre megváltozik, illetve a jogosultság meghosszabbítása érdekében 60 nappal azt megelőzően, hogy az aláírási tanúsítványának érvényességi ideje lejár.

(5) Az aláírási tanúsítvány visszavonása kapcsán a jogi igazgató gondoskodik a nyilvántartott adatok módosításáról.

8. § AZ ELEKTRONIKUS ALÁÍRÁSSAL ÉS ELEKTRONIKUS BÉLYEGZŐVEL RENDELKEZŐ DOKUMENTUMOK HOSSZÚ TÁVÚ MEGŐRZÉSE (ARCHIVÁLÁSA)

(1) Az Egyetem a feladat- és hatáskörébe tartozó ügyviteli eljárások során létrehozott és elektronikus aláírással vagy elektronikus bélyegzővel hitelesített dokumentumok tekintetében gondoskodik arról, hogy az Iratkezelési Szabályzat 2. sz. mellékletét képező Irattári Tervben meghatározott megőrzési idő lejártáig az aláírás ideje szerinti változatlan formában legyenek elérhetők, ezáltal a tartalmuk olvasható és visszakereshető maradjon.

(2) Az Egyetem a feladat- és hatáskörébe tartozó ügyviteli eljárások során létrehozott és elektronikus aláírással vagy elektronikus bélyegzővel hitelesített dokumentumok archiválása során a következők szerint jár el:

a) védi a dokumentumok bizalmasságát és integritását, gondoskodik a jogosulatlan hozzáférés megakadályozásáról;

b) kizárja az utólagos módosítás lehetőségét;

c) ha több dokumentumon egy elektronikus aláírás vagy bélyegző került elhelyezésre, akkor a megőrzési idő leteltéig ezeket a dokumentumokat együtt kezeli (archiválja).

(3) Az elektronikus iratok tárolása a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet 61. § (4) bekezdés b) pontja alapján a Poszeidon dokumentumkezelő rendszer irattári funkciójának, mint elektronikus irattárnak az igénybevételével történik.

Elektronikus aláírás: az elektronikus dokumentumhoz azonosítási célból logikailag hozzárendelt, vagy azzal elválaszthatatlanul összekapcsolt elektronikus adatsor, mely minden kétséget kizáróan bizonyítja a dokumentum eredetét, hitelességét, sértetlenségét, és azonosítja az alanyt, mint aláíró személyt, illetve bizonyítja az aláírás tényét. Az elektronikus aláírás az aláíró (alany) magánkulcsával készül és kizárólag annak párjával, a nyilvános kulccsal lehet ellenőrizni az aláírás eredetiségét, az aláírt elektronikus dokumentum sértetlenségét.

Elektronikus aláírási tanúsítvány: olyan tanúsítvány, amely természetes személy részére került kibocsátásra, és amellyel annak birtokosa elektronikus aláírásokat hozhat létre.

Elektronikus bélyegző tanúsítvány: olyan tanúsítvány, amely egy jogi személyhez kapcsolható és igazolja az érintett jogi személy nevét, és amellyel a jogi személy elektronikus bélyegzőt hozhat létre.

Elektronikus időbélyegző: olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét, sértetlenségét, valamint, hogy hitelesen igazolják az aláírás időpillanatát és azt, hogy az elektronikus dokumentum az időbélyegzés időpontjában változatlan formában már létezett.

Kompromittálódás: olyan esemény, amely során az aláírás-létrehozó adat (magánkulcs) vagy az aláírás-létrehozó eszköz illetéktelen személy által történő hozzáférését korlátozó jelszó illetéktelen személy birtokába jut vagy ismertté válik, azaz a védendő adat vagy kód bizalmassága sérül.

1. sz. melléklet

ÚTMUTATÓ AZ ELEKTRONIKUS ALÁÍRÁSOK HASZNÁLATÁHOZ ÉS AZ ELEKTRONIKUS ALÁÍRÁSOKNAK AZ IRATON TÖRTÉNŐ ELHELYEZÉSÉHEZ

Jelen útmutató célja, hogy gyakorlati segítséget nyújtson az Egyetem munkatársai számára az elektronikus aláírással ellátott iratok kezelésében, a web-Szignó és e-Szignó aláíró szoftver használatában és az aláírási munkafolyamat (workflow) menedzselésében.

Az elektronikusan aláírandó iratok előkészítésekor figyelemmel kell lenni arra, hogy egyedi vagy többes aláírás szükséges-e rá.

A) Önálló (egyedi) aláírás: Amikor az iratra csak egyetlen elektronikus aláírás kerül (pl. egyoldalú jognyilatkozatok, határozatok, igazolások).

B) Többes aláírás (szerződések, megállapodások): Amikor az irat érvényességéhez több résztvevő jóváhagyása és elektronikus aláírása szükséges (pl. jogi és pénzügyi ellenjegyzés, végül rektori aláírás).

Közös szabály mindkét esetben, hogy az elektronikus aláírási folyamat során biztosítani kell, hogy az irat már az aláírás előtt rendelkezzen minden formai kellékkel, beleértve az iktatószámot is.

I. Előkészítés és iktatás

1. Irat előkészítése: Az ügyintéző elkészíti az irat tervezetét (pl. Word formátumban).

2. Előzetes iktatás: Mielőtt az elektronikus aláírás rákerülne, az iratot az ügy indítójának a Poszeidon iratkezelő rendszerben iktatnia kell. Az így kapott iktatószámot, továbbá a vonalkódot fel kell tüntetni a word dokumentumon (a fejlécben vagy az erre rendszeresített helyen).

3. Főszabály szerint az elektronikus szerződés aláírását az egyetemen kell indítani iktatott pdf dokumentum formájában. Amennyiben elektronikus szerződés esetében az elektronikus aláírást előbb végezte el a partner, az egyetem általi aláírás során az elektronikus iratot az Iratkezelési Szabályzat szerint iktatni szükséges az elektronikus iratkezelő rendszerben (Poszeidon). Az iktatószámot ekkor már nem lehetséges magára az elektronikus iratra rávezetni, így az a Poszeidon rendszerben, illetve a papíralapú hiteles másolatot tartalmazó előadói íven lesz kézzelfoghatóan is nyomonkövethető.

4. PDF konvertálás: A végleges, iktatószámmal ellátott iratot PDF formátumba kell menteni (vagy szükség esetén e-akta/ASiC konténerbe).

II. Feltöltés és az elektronikus aláírási folyamat (workflow) beállítása a web-Szignó felületen

1. Belépés: Az aláírási folyamatot az első aláíró indítja. Belép az aláíró szoftverbe (ez történhet kliens, web-szigno.com felületen vagy e-Szignó mobil alkalmazás segítségével is). A belépés történhet felhasználónév/jelszó párossal vagy a mobilalkalmazás (e-Szignó) QR-kód olvasójával.

2. Irat feltöltése: a „Fájl feltöltése" gombbal történik.

3. Aláíró(k) és jóváhagyó(k) megadása:

3.1. Egy vagy több aláíró: Kattintson az „Aláírás" gombra. Itt a dokumentum típusától függően az önálló aláírás („Egyedül én" írom alá) vagy a többes aláírás („Más is" aláírja) opció választható ki.

A) Önálló aláírás: a folyamatban csak egyetlen aláíró (pl. a rektor vagy a meghatalmazott vezető) szerepel.

B) Többes aláírás: szerződések esetén az aláírási folyamatban (workflow) több résztvevő követi egymást. Az aláíró láncba fel kell venni az összes szükséges jóváhagyót és aláírót.

3.2. Szerepkörök: Az aláírás menetében és az aláíró szoftverben logikailag kétféle szerepkör van.

A) Aláíró: Az a személy (pl. rektor, szervezeti egység vezetője), aki minősített személyes távoli kulcsos aláíró tanúsítvánnyal rendelkezik, és elektronikusan aláírja az iratot.

B) Jóváhagyó: Olyan munkatárs (pl. szakmai ellenjegyző), akinek nincs elektronikus aláírása vagy nem szükséges elhelyeznie azt, de a folyamatban a jóváhagyása szükséges a továbbításhoz, és rendelkezik e-Szignó regisztrációval aláíró tanúsítvány nélkül is. A jóváhagyás tényét a rendszer átmeneti időre naplózza, de az elektronikusan aláírt PDF-en ez vizuálisan nem jelenik meg.

4. Sorrendiség: Többes aláírás, azaz jellemzően szerződések esetén a résztvevők egymás után, lineáris láncban kapják meg az iratot. A rendszer addig nem küldi tovább a következő szereplőnek, amíg az előző aláíró vagy jóváhagyó nem végezte el a feladatát. A rektor számára elektronikusan aláírandó irat csak úgy küldhető, hogy a jogi és gazdasági vezető már elektronikusan aláírta (ellenjegyezte).

5. Sablonok: Gyakori aláírási láncok esetén (pl. szerződésaláírás) a résztvevők listáját „Sablonként" is el lehet menteni a gyorsabb ügyintézés érdekében. Az aláíró szoftverek sablonjainak kezelése nem központi módon történik, az személyhez kötött, azaz a sablonok minden esetben az adott felhasználó profiljában jönnek létre és ahhoz kötődnek, így minden felhasználó csak a saját sablonjait és aláírói láncait látja.

III. Az elektronikus aláírás elhelyezése és az elektronikus aláírási folyamat indítása

1. Pozicionálás: Az aláíró szoftver felületén az irat előnézeti képén dupla kattintással – mobileszközön érintéssel és húzással – kijelölhető, hogy az elektronikus aláírás vizuális képe (a „bélyegzőkép") hova kerüljön a PDF-en (pl. az aláíró neve fölé/alá). Többes aláírást tartalmazó iratok (szerződések) esetén az aláíróknak ügyelniük kell arra, hogy a saját elektronikus aláírásuk vizuális képét az iraton a számukra megjelölt helyre (pl. a saját ellenjegyzői vagy aláírói rubrikájukhoz) pozicionálják, úgy, hogy az ne takarja el mások aláírását vagy a szöveges tartalmat.

2. Tömeges aláírás: Több irat egyidejű feltöltése esetén lehetőség van az aláírás pozíciójának rögzítésére az összes iraton, így azokat egyetlen hitelesítési művelettel lehet aláírni.

3. Küldés: A „Kérés elküldése" gombbal a rendszer értesítést küld az első résztvevőnek. Az elindított aláírási folyamat résztvevőinek listája utólag új személlyel nem bővíthető. A folyamat indítója azonban visszavonhatja a teljes kérést, illetve törölheti a láncból azt a résztvevőt, akihez még nem ért el az irat (pl. hirtelen távollét vagy helyettesítés miatt, hogy a folyamat ne akadjon meg). Ha a láncban valaki elutasítja az aláírást vagy jóváhagyást, a folyamat azon a ponton megszakad, és az irat visszatér az indítóhoz. A folyamat indítója az aláírások státuszáról (kinél van az irat aláíráson, ki nem írta még alá, stb.) az aláíró szoftverekben tájékozódhat.

IV. Az irat elektronikus aláírással való ellátása

1. Az aláíró beállítása szerint e-mailben és/vagy mobil push üzenetben értesítést kap, hogy aláírandó irata érkezett.

2. Az aláírásra jogosult vezető két módon írhatja alá az iratokat: vagy közvetlenül a mobiltelefonján, vagy számítógépen a web-Szignó felületén keresztül (irodai környezetben), a mobilját hitelesítő eszközként használva.

A) Aláírás számítógépen, web-Szignó felületen. (Ez a javasolt módszer irodai munkavégzés során, mivel az irat áttekintése és az aláírás pozicionálása nagy képernyőn egyszerűbb.)

1. Belépés az aláíró szoftverbe: A vezető belép a számítógép böngészőjében a www.web-szigno.com oldalra.

2. Irat megnyitása: A listából kiválasztja az aláírandó irato(ka)t.

3. Az aláírás vizuális pozicionálása: Az aláíró szoftver alapbeállítása szerint az elektronikus aláírás látható képét az irat első oldalának bal felső sarkában helyezi el. Az aláíró személy az irat előnézeti képén dupla kattintással elhelyezheti az aláírás képét más, általa kívánt helyre (pl. a szövegben jelölt aláírási helynél a neve fölé). Tömeges aláírás esetén rögzítheti az általa használni kívánt pozíciót az összes kijelölt fájlra vonatkozóan.

4. Hitelesítés indítása (az aláírás jóváhagyása): Az „Aláírás" gombra kattintva a rendszer kéri a hitelesítést. Ez kétféleképpen végezhető el a telefon segítségével:

a) QR-kódos módszer: A számítógép képernyőjén megjelenik egy egyedi QR-kód. A vezető megnyitja mobilján az e-Szignó alkalmazást, a „QR-kód olvasása" funkcióval leolvassa a képernyőt, majd a telefonon megadja a PIN kódját vagy használja a biometrikus azonosítást (ujjlenyomat/arcfelismerés).
b) Push üzenet (Azonnali üzenet): Ha be van állítva, a szoftver nem QR-kódot ad, hanem értesítést küld a telefonra. A vezető rákattint a telefonjára érkező értesítésre, és PIN kóddal/biometriával jóváhagyja a műveletet.

Ezzel a tanúsítvány hitelesíti az iratot, és automatikusan elhelyezésre kerül az időbélyeg is, amely biztosítja az irat hosszú távú érvényességét. E jóváhagyást követően az elektronikus aláírás technikailag létrejön és az irathoz rögzítésre kerül.

5. Befejezés: A számítógép képernyőjén az irat státusza „Aláírt"-ra változik.

B) Aláírás közvetlenül mobilalkalmazásban.

1. Értesítés: Többes aláírás esetén az aláírási folyamat elindítását követően az aláíró e-mailben vagy mobil értesítésben jelzést kap, hogy aláírandó feladata érkezett.

2. Az irat megnyitása: Az aláíró az e-Szignó mobilalkalmazás elindítását követően a dokumentumkezelési funkciók segítségével megnyitja az aláírni kívánt PDF iratot. Az irat az alkalmazásba betölthető közvetlen tallózással, illetve külső alkalmazásból (például elektronikus levelezőrendszerből) történő megosztással is.

3. Az aláírási folyamat elindítása: Az irat megnyitását követően a felhasználó az „Aláírás" funkció kiválasztásával kezdeményezi az elektronikus aláírás elhelyezését. E lépés kizárólag az aláírás előkészítését szolgálja, joghatással még nem jár.

4. Az aláírás vizuális pozícionálása: Az alkalmazás az irat előnézeti képén megjelenít egy aláírási keretet, amely az elektronikus aláírás vizuális megjelenésének helyét jelöli. A felhasználó ezt a keretet érintéssel, húzással a kívánt pozícióba helyezheti el az adott oldalon. Többoldalas irat esetén az aláírás kizárólag azon az oldalon jelenik meg, amelyen a keret elhelyezésre kerül.
A pontos elhelyezés érdekében az aláírás nagyítható és kicsinyíthető. A felhasználónak ügyelnie kell arra, hogy az aláírás ne takarjon ki szöveges tartalmat, és ne kerüljön túl közel az oldal széléhez.

5. Hitelesítés indítása (az aláírás jóváhagyása): Az aláírási pozíció ellenőrzését és elfogadását követően a felhasználó megerősíti az aláírási szándékát. Az alkalmazás biztonsági azonosítást kérhet (például PIN-kód vagy biometrikus azonosítás formájában). Ezzel a tanúsítvány hitelesíti az iratot, és automatikusan elhelyezésre kerül az időbélyeg is, amely biztosítja az irat hosszú távú érvényességét. E jóváhagyást követően az elektronikus aláírás technikailag létrejön és az irathoz rögzítésre kerül.

V. Bejövő, a partner által elektronikusan már aláírt iratok kezelése

Az Egyetemre érkező (pl. Hivatali Kapun vagy e-mailben kapott) elektronikusan aláírt iratok esetében a legfontosabb lépés a hitelesség ellenőrzése az iktatás előtt.

Érvényesség ellenőrzése: Amennyiben elektronikusan hiteles (elektronikusan aláírt) irat érkezik az Egyetemre, a címzett vagy az érintett iratkezelési ügyintéző – a szabályzat 6. §-ában foglaltaknak megfelelően – köteles meggyőződni arról, hogy:

a) az irat sértetlen (nem módosult az aláírás óta),
b) az aláíró tanúsítványa érvényes és a megfelelő személyhez tartozik,
c) az aláíráshoz időbélyeg is tartozik.

Az ellenőrzéshez az ingyenes e-Szignó program vagy az Adobe Acrobat Reader használható.

Egyebekben a bejövő, partner által elektronikusan aláírt iratnak az Egyetem oldaláról történő aláírása megegyezik az előző pontban leírtakkal azzal, hogy az indító irat a partner által már aláírt pdf dokumentum lesz.

VI. Az elektronikusan minden érintett által aláírt iratok kezelése

1. Az aláírási folyamat befejezését követően az irat elektronikusan hitelesnek minősül. Az irat tartalma az aláírás létrejötte után nem módosítható; bármely további változtatás az aláírás érvénytelenségét eredményezné.

2. Az elektronikus hiteles irat aláírását követően, illetve az elektronikus hiteles szerződés esetén a mindkét fél általi aláírást követően az elektronikus példánynak az iratkezelő rendszerbe történő feltöltését az iratkezelési szabályzatnak megfelelően kötelező elvégezni. Az ügyintéző ezt követően az aláírt, érvényes szerződést tartalmazó ügyiratot köteles eljuttatni a Jogi Igazgatóságra (kivéve, ha az ügy indítója a Jogi Igazgatóság volt).

3. Az elektronikus hiteles példányról készített papíralapú aktapéldányt a Jogi Igazgatóság hitelesíti, annak érdekében, hogy az fizikailag is irattárba helyezhető legyen.

4. Az elektronikus aláírással ellátott szerződések nyilvántartását a Jogi igazgatóság végzi a Poszeidon iratkezelő rendszer szerződéstárában.

VII. Egyéb technikai információk

1. Eszközcsere: Amennyiben az egyetemi tanúsítvánnyal rendelkező munkatársnál telefoncsere következik be, új telefonra váltáskor az e-Szignó alkalmazást újra kell aktiválni az web-Szignó portálon igényelt „Helyreállító adatlappal" (QR-kód).

2. Két mobileszköz: Amennyiben az aláíró két mobiltelefonon is szeretné párhuzamosan használni az e-aláírás szolgáltatást, az ügyféltéren (portal.e-szigno.hu) az ún. „másolós adatlap" kikérésével van lehetősége az új eszközt a meglévővel szinkronba hozni.

3. Időbélyeg: A bizalmi szolgáltató a web-Szignó/e-Szignó szoftver használatakor automatikusan időbélyeggel látja el az aláírásokat, így azok a tanúsítvány esetleges későbbi lejárta vagy visszavonása után is érvényesek maradnak. Így külön időbélyeg elhelyezése nem szükséges, automatikusan megtörténik.

4. Jelszó/PIN védelem: Az aláíráshoz szükséges PIN kódot és az eszközt – figyelemmel az Informatikai Biztonsági Szabályzat rendelkezéseire – a vezető köteles biztonságosan őrizni, azt másnak átadni tilos.

5. Letöltési kötelezettség és átmeneti tárolás: Az aláíró szoftver felületére feltöltött és ott aláírt iratokat a rendszer a felhasználói csomagtól függően csak korlátozott ideig tárolja (Platina csomag esetén 180 nap), majd automatikusan törli. Ezért a teljesen aláírt iratot a folyamat lezárulása után haladéktalanul le kell tölteni, és a vonatkozó iratkezelési szabályoknak megfelelően iktatva kell tartósan tárolni az iratkezelő rendszerben.

6. Fiók törlés: Mivel az e-Szignó fiókok és a bennük elmentett sablonok, folyamatok személyhez kötöttek, egy aláíró tanúsítvánnyal rendelkező, az elektronikus aláírási folyamatban résztvevő munkatárs jogviszonyának megszűnése esetén az Egyetem kijelölt szervezeti ügyintézőjének jeleznie kell a kilépés tényét a bizalmi szolgáltató (Microsec) felé. A fiókot a szolgáltató törli, biztosítva ezzel az adatvédelmi szabályok érvényesülését.