

A jegykezelő rendszer bejegyzései jogilag elfogadhatóak-e audit bizonyítékként?

VFP3 KiberVéd - NIS2 Audit felkészítés jogi
állásfoglalás 2026/52

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.23	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

- **A jegykezelő rendszer jegy elfogadható audit bizonyíték.** A kiberbiztonsági jogszabályok és az audit rendjét meghatározó SZTFH rendelet nem írnak elő papíralapú vagy pecsétetes formát. Az auditor bizonyítékokat gyűjt és értékeli, a bizonyíték formája szabad, a teszt módszere pedig a naplózási nyomok lekérdezésére épül.
- **A jogszabályok** a hozzáférés, a változás, a karbantartás és az incidens kezelésénél **jóváhagyást, dokumentálást és nyilvántartást várnak el, aláírást nem.** Az írásbeliség a Ptk. szerint elektronikus formában is teljesül, ha a tartalom változatlanul visszaidézhető, a nyilatkozó személye és a nyilatkozat időpontja azonosítható.
- **Nem a forma, hanem a minőség számít.** A jegy akkor jó bizonyíték, ha egyedi, hitelesített felhasználóhoz kötődik, a jóváhagyás kifejezett munkafolyamat-lépés, a lezárt jegy nem módosítható, a változtatások naplózottak, az időbélyeg pontos, a bejegyzés legalább öt évig visszakereshető és exportálható.
- **A magas biztonsági osztály kifejezetten automatizált nyilvántartást vár el** a változások, az incidensek és a karbantartások dokumentálására. Egy jól beállított jegykezelő ezeket egy helyen teljesíti, a papír nem.
- **Az aláírással való hitelesítés néhány helyen indokolt marad.** A vezetőnek fenntartott döntéseknél, a hatóságnak megküldött dokumentumoknál, a külső felekkel kötött szerződéseknél és ott, ahol jogszabály kifejezetten aláírást ír elő, a saját kezű vagy a minősített elektronikus aláírás a biztonságos választás. Ezek évente néhány dokumentumot jelentenek.
- **Az adminisztráció úgy csökkenthető, hogy a működés maga termeli a bizonyítékot.** A jegykezelőt az IBSZ-ben hivatalos nyilvántartásnak kell kijelölni, a jóváhagyást a jegybe kell építeni, a rutinváltozásokat előre jóváhagyott sablonnal kell kezelni, a párhuzamos nyilvántartásokat meg kell szüntetni, az auditra pedig a rendszerből készített riportok szolgálnak.

2. A VIZSGÁLANDÓ KÉRDÉS

Egy NIS2¹-kötelezett szervezet (a továbbiakban mint „Szervezet”) a hozzáférés-igényléseket, a változaskéréseket, az incidenseket, a karbantartási feladatokat és a felhasználói kéréseket jegykezelő (ticketing) rendszerben kezeli.

A felkészülés során felmerült, hogy az auditor elfogadja-e ezeket a bejegyzéseket, vagy a hozzáférési és változási döntésekről továbbra is papíralapú, aláírt és pecséttel ellátott dokumentumot kell készíteni.

A második kérdés az, hogy milyen más módon csökkenthető a megfelelés adminisztrációs terhe anélkül, hogy a bizonyíthatóság sérülne.

¹ Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről (NIS 2 irányelv)

A jegykezelő kiválasztása és technikai beállítása, valamint a szabályozási dokumentumok (IBSZ, rendszerbiztonsági terv) jóváhagyásának formája nem tárgya ennek az állásfoglalásnak; ez utóbbival a 2026/40. számú állásfoglalásunk foglalkozik.

3. GYAKORLATI JAVASLATOK

3.1 Mikor jó bizonyíték a jegy?

A jegykezelő bejegyzése akkor felel meg az audit és a jogi bizonyítás elvárásainak, ha a következő, az IBSZ-ben rögzítendő és a rendszer beállításaival kikényszerítendő feltételek együttesen teljesülnek.

- a) Azonosított személy. Minden bejegyzés egyedi, névre szóló és többtényezős hitelesítéssel védett fiókhoz kötődik, közös fiók a jegykezelőben nincs. A jóváhagyó és az igénylő nem lehet ugyanaz a személy.
- b) Kifejezett jóváhagyás. A jóváhagyás a munkafolyamat külön lépése (jóváhagyó gomb, státuszváltás), amelyet csak az arra jogosult szerepkör hajthat végre.
- c) Sértetlenség. A lezárt jegy nem szerkeszthető, minden módosítás naplózott (ki, mikor, miről mire), a jegy és a napló törlése a rendszergazda számára sem lehetséges észrevétlenül.
- d) Pontos idő. A rendszer szinkronizált órát használ, az időbélyeg a koordinált világidőt és a helyi időeltolódást is tartalmazza.
- e) Teljes tartalom. A jegyből megállapítható, milyen esemény történt, mikor, hol, ki kezdeményezte, ki döntött, mi lett a kimenetele, és mely rendszert vagy fiókot érintette.
- f) Megőrzés és export. A jegyek és naplók legalább az audit lezárásától számított öt évig megőrzöttek, és rendszertől független formában (PDF, CSV, lenyomattal) exportálhatók.
- g) Védett rendszer. A jegykezelő szerepel az EIR-nyilvántartásban, hozzáférése a legkisebb jogosultság elvén alapul, felhőszolgáltatásnál a szerződés az adatok kiadását, megőrzését és az auditor hozzáférését biztosítja.

3.2 Az adminisztráció csökkentésének további módjai

A jegykezelő önmagában nem csökkenti az adminisztrációt, ha a papír mellette megmarad. A következő lépések együtt hoznak könnyebbséget.

- Az IBSZ-ben ki kell mondani, hogy a hozzáférési, változási, incidens- és karbantartási nyilvántartás hivatalos forrása a jegykezelő, a párhuzamos papír-, e-mail- és táblázatnyilvántartásokat pedig meg kell szüntetni.
- Jóváhagyás a jegyben. A hozzáférés-igényléshez és a változaskéréshez nem kell külön aláírt űrlap, ha a jegy munkafolyamata tartalmazza a jóváhagyó lépést és a jóváhagyó személyét.
- Előre jóváhagyott rutinváltozások. A rendelet a Szervezetre bízza, mely módosítások tartoznak a változáskezelés hatálya alá. Az alacsony kockázatú, ismétlődő változásokat (biztonsági frissítés, szabványos munkaállomás kiadása) érdemes az eljárásrendben

egyszer jóváhagyott sablonként kezelni, amelynél a jegy csak a végrehajtást dokumentálja.

- Kötelező mezők és integráció. A jegytípusonként kötelező mezők (érintett rendszer, kockázat, tesztelés, visszaállítás, lezárás oka) biztosítják, hogy a bejegyzés az audit elemi követelményeit lefedje. Ha a jegykezelő az identitáskezelővel, a leltárral vagy a felügyeleti rendszerrel összekapcsolt, a fiók létrehozása vagy a riasztás automatikusan jegyet nyit, a lezárás pedig a végrehajtást igazolja.
- Bizonyítéktérkép és riport. Egy egyszerű táblázat, amely a rendelet követelménycsoportjaihoz hozzárendeli a megfelelő jegytípust és riportot, megszünteti az audit előtti dokumentumgyűjtést, mert ugyanaz a jegy több követelményt is bizonyít. A rendszerből készített, dátumozott riport és az auditor olvasási hozzáférése a dokumentumvizsgálatot és a tesztet egyaránt kiszolgálja, nyomtatás nélkül.

4. VÁLASZ ÉS RÉSZLETES INDOKOLÁS

4.1 A vizsgálat kiindulópontjai

Az állásfoglalás abból indul ki, hogy a Szervezet a Kiberbiztonsági tv. 1. § (1) bekezdés d) pontja alá tartozik, felügyeletét a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) látja el, és kétévente kiberbiztonsági auditra kötelezett.² A válasz lényege a többi szervezettípusra is irányadó, az 1. § (1) bekezdés a)-c) és f) pontja alá tartozó szervezetek eltéréseit a 4.6. pont foglalja össze.

4.2 Mit vár el az audit? A bizonyíték fogalma

A kiberbiztonsági audit célja a törvény szerint a megfelelés bizonyítása. A Szervezet

az e törvény szerinti kiberbiztonsági követelményeknek való megfelelés bizonyítására köteles kétévente, illetve a 23. § (1) bekezdése szerint illetékes kiberbiztonsági hatóság általi elrendelés esetén kiberbiztonsági auditot végeztetni. [2024. évi LXIX. tv. 16. § (1) bekezdés]

Az auditor a biztonsági osztályba sorolás és a védelmi intézkedések megfelelőségét ellenőrzi. Az audit rendjét az SZTFH elnökének rendelete határozza meg, amely a bizonyíték fogalmát a nemzetközi auditszabványokkal azonos módon írja le. Az auditor

felméri a védelmi intézkedések megfelelőségét bizonyítékok begyűjtésére és az azok objektív kiértékelésére irányuló módszeres, független és dokumentált eljárás lefolytatásával. [1/2025. (I. 31.) SZTFH rendelet 1. § (2) bekezdés b) pont]

Ez az ISO 19011 auditfogalmának átvétele, amely szerint auditbizonyíték minden, az auditkritériumok szempontjából releváns és ellenőrizhető feljegyzés, tényállítás vagy egyéb

² 2024. évi LXIX. tv. 16. § (1) bekezdés, 21. § (1) bekezdés és 23. § (1) bekezdés b) pont

információ.³ A bizonyíték tehát nem dokumentumtípus, hanem tulajdonság, és a jegykezelő bejegyzése ellenőrizhető feljegyzés, ha a rendszer a keletkezését és változását hitelesen őrzi.

Az auditor dokumentumvizsgálatot, interjút, tesztet és a törvény szerinti egyéb vizsgálatokat alkalmazhat.⁴ Az auditori módszertan a NIST SP 800-53A alapján készült⁵, és a teszt módszerét így írja le. Az auditor

automatizált ellenőrző programokkal, vagy – a szervezet munkatársainak közreműködésével végrehajtott – céltesztekkel, a szervezeti tevékenységek és céltesztek naplózási nyomainak lekérdezésével a szervezetnek azokat az informatikai mechanizmusait és tevékenységeit ellenőrzi, amelyek megvalósítják az adott követelménycsoportra elvárt intézkedéseket.
[1/2025. (I. 31.) SZTFH rendelet 5. melléklet 1.2.3.1. pont]

A módszertan tehát elvárja, hogy az auditor a rendszerekben keletkezett elektronikus nyomokat közvetlenül lekérdezze, a dokumentumvizsgálat körébe pedig kifejezetten bevonja a változáskezeléssel, az incidenskezeléssel és a naplózással kapcsolatos dokumentációkat.⁶ Papíralapú, pecsétes iraton teszt nem végezhető; egy aláírt űrlap azt bizonyítja, hogy valaki aláírta, azt nem, hogy a fiók valóban akkor és úgy jött létre. Az auditor jogosult minden, a Szervezet és rendszerei biztonságával kapcsolatba hozható dokumentum megismerésére, a bizonyíték hiánya pedig az adott elemi követelménynél „nem megfelelt” döntést eredményez.⁷ Maga az auditjelentés is elektronikus aláírással vagy bélyegzővel ellátott elektronikus dokumentum, az átadott bizonyítékokat pedig a Szervezet az audit lezárásától számított öt évig őrzi meg.⁸

Ugyanez a logika érvényesül az ISO/IEC 27001 szerinti tanúsítási auditon. A szabvány a dokumentált információt hordozótól függetlenül kezeli, és a feljegyzéseknél rendelkezésre állást, védelmet, változáskövetést és megőrzést kíván, formát nem. Az informatikai auditorok szakmai szabványa szerint a kontrollált rendszerből kinyert elektronikus feljegyzés megbízhatóbb, mint a szóbeli nyilatkozat vagy a kézzel vezetett lista.⁹

Az audit felől nézve tehát a válasz egyértelmű. A jogszabály papírt és pecsétet sehol nem kíván, a digitális bejegyzés bizonyíték, ha releváns és ellenőrizhető.

4.3 A jogszabályok formát nem, dokumentálást és nyilvántartást viszont előírnak

A 7/2024. (VI. 24.) MK rendelet védelmi intézkedései a jegykezelőben kezelt folyamatoknál következetesen a „jóváhagy”, „dokumentál”, „nyomon követ” és „nyilvántart” fordulatokat használják. A fiókkezelésnél a szervezet

³ MSZ EN ISO 19011:2018, 3.1. pont (audit) és 3.8. pont (auditbizonyíték)

⁴ 1/2025. (I. 31.) SZTFH rendelet 2. § (2) bekezdés a)-d) pont

⁵ 1/2025. (I. 31.) SZTFH rendelet 5. melléklet 1.1.1. pont; NIST SP 800-53A Rev. 5, az examine, interview és test vizsgálati módszerek leírása

⁶ 1/2025. (I. 31.) SZTFH rendelet 5. melléklet 1.2.1.2.4. és 1.2.1.2.5. pont

⁷ 1/2025. (I. 31.) SZTFH rendelet 5. § (3) bekezdés, valamint 5. melléklet 1.1.4. és 2.2.3.4.2. pont

⁸ 1/2025. (I. 31.) SZTFH rendelet 5. § (7) bekezdés és 6. § (3) bekezdés

⁹ ISO/IEC 27001:2022, 7.5.1., 7.5.3. és 9.2.2. pont, valamint az A. melléklet 5.18., 5.24-5.28., 8.15. és 8.32. pontja; ISACA ITAF, 4. kiadás, 1205 Evidence szabvány és 2205 Evidence útmutató

2.2.5. A meghatározott szerepköröket betöltő személyek jóváhagyását kéri a felhasználói fiókok létrehozására vonatkozó kérelmek esetén. [7/2024. (VI. 24.) MK rendelet 2. melléklet 2.2. pont] (A, J, M)

A változáskezelésnél a jelentős és a magas osztályban a szervezet

6.7.3. Dokumentálja az EIR-ben történt változtatásokra vonatkozó döntéseket.

6.7.4. Megvalósítja a jóváhagyott változtatásokat az EIR-ben.

6.7.5. Meghatározott időtartamig nyilvántartja és visszakereshetően megőrzi az EIR-ben megvalósított változtatások dokumentumait. [7/2024. (VI. 24.) MK rendelet 2. melléklet 6.7. pont] (J, M)

Ugyanez a követelménycsoport a változások koordinálását „egy erre a célra kijelölt egység (például személy, testület, szoftver, folyamat stb.)” feladatává teszi, a magas osztályban pedig automatizált mechanizmust ír elő a javasolt és a végrehajtott változtatások dokumentálására, a jóváhagyók értesítésére és a jóvá nem hagyott változások megakadályozására.¹⁰ Ez a leírás egy jegykezelő rendszer változáskezelési munkafolyamata. A biztonsági eseményeket a szervezet minden osztályban nyomon követi és dokumentálja, a karbantartásokat ütemezi, jóváhagyja és nyilvántartja, a magas osztályban mindkettőt automatizált mechanizmussal.¹¹ A kiléptetéskor és az áthelyezéskor a hozzáférések visszavonását szintén igazolni kell.¹²

A rendelet a forma kérdését a szervezetre bízta. Az alkalmazási útmutató szerint a követelményekben elvárt tevékenységeket és paramétereket

az adott követelménycsaládhoz és követelménycsoporthoz tartozó stratégiában, szabályzatban, eljárásrendben, eljárásban vagy munkautasításban szükséges meghatározni. [7/2024. (VI. 24.) MK rendelet 2. melléklet 20.5. pont]

Ahol a jogalkotó aláírást akart, azt kimondta, például a sérülékenységvizsgálati alapidokumentumnál¹³; a jegykezelőben kezelt folyamatoknál ilyen rendelkezés nincs. A pecsétet pedig a magyar jog egyetlen itt vizsgált jognyilatkozatnál sem tekinti alaki kelléknek; a bélyegző szokás, nem jogszabályi követelmény. Az írásbeliséget a Ptk. sem köti hozzá.

(3) Írásba foglaltnak kell tekinteni a jognyilatkozatot akkor is, ha annak közlésére a jognyilatkozatban foglalt tartalom változatlan visszaidézésére, a nyilatkozattevő személyének és a nyilatkozat megtétele időpontjának azonosítására alkalmas formában kerül sor. [2013. évi V. tv. 6:7. § (3) bekezdés]

¹⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 6.7.7. pont (J, M) és 6.8. pont (M)

¹¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 9.25. pont, valamint 10.2.1., 10.2.2. és 10.2.6. pont (A, J, M); 9.26. és 10.3. pont (M)

¹² 7/2024. (VI. 24.) MK rendelet 2. melléklet 14.5. és 14.8. pont (A, J, M)

¹³ 418/2024. (XII. 23.) Korm. rendelet 53. § (2) bekezdés 14. pont

A Kúria tanácsadó testületének többségi álláspontja szerint az elektronikus közlés is írásbeli, ha e három feltétel a konkrét esetben fennáll, a munkajog pedig ugyanezt mondja ki a munkaviszonyban tett jognyilatkozatokra.¹⁴ Egy hitelesített felhasználóhoz kötött, időbélyeggel ellátott és utólag nem módosítható jegy mindhárom feltételt teljesíti. Az uniós jog pedig kizárja, hogy egy elektronikus dokumentum joghatását vagy bizonyítékként való elfogadhatóságát pusztán az elektronikus forma miatt tagadják meg.¹⁵

Az audit nem per és nem hatósági eljárás, a bizonyítás szabályait mégis érdemes ismerni, mert megállapításai hatósági ellenőrzést vonhatnak maguk után. A hatósági eljárásban minden, a tényállás tisztázására alkalmas bizonyíték felhasználható, és a hatóság azt szabad meggyőződése szerint értékeli; a polgári perben ugyanez érvényesül.¹⁶ A teljes bizonyító erejű magánokirat (például a minősített elektronikus aláírással ellátott irat¹⁷) csak a nyilatkozat megtételének bizonyítását könnyíti meg; a jegy ezt az erőt nem éri el, hitelességét vita esetén a rendszer naplójával és szükség esetén szakértővel kell alátámasztani. A napi üzemeltetési bejegyzéseknél ez nem indokolja a papírt.

4.4 A jegy bizonyító erejének feltételei

Ha a forma szabad, a bizonyíték értékét a rendszer minősége adja. A rendelet naplózási követelményei a jegykezelőre mint bizonyítékforrásra közvetlenül alkalmazhatók. A naplóbejegyzésből minden osztályban megállapíthatónak kell lennie, milyen esemény történt, mikor, hol, miből származott, mi lett a kimenetele, és mely személyek és objektumok kapcsolódtak hozzá. Az időbélyegeket a szervezet belső rendszerével, a koordinált világidő és a helyi időeltolódás feltüntetésével állítja elő, a naplóinformációt a jogosulatlan hozzáféréssel, módosítással és törléssel szemben védi, és a megőrzési követelmények szerinti ideig megőrzi. A magas osztályban a rendszernek megcáfolhatatlan bizonyítékot kell szolgáltatnia arról, hogy egy személy a letagadhatatlanság követelménye alá eső tevékenységet végrehajtotta.¹⁸

A törvény a sértetlenség fogalmába a hitelességet és a letagadhatatlanságot is beleérti, a szervezet vezetője pedig köteles gondoskodni a rendszer eseményeinek nyomonkövethetőségéről.¹⁹ Egy jegy, amely egyedi fiókhoz, kifejezett jóváhagyó lépéshez, mezőszintű naplóhoz és pontos időbélyeghez kötődik, erősebb bizonyíték, mint egy aláírt papír, mert a keletkezésének körülményei utólag ellenőrizhetők.

A jegykezelő emellett maga is elektronikus információs rendszer a törvény fogalma szerint, és a szervezet legérzékenyebb üzemeltetési adatait tartalmazza, ezért az EIR-nyilvántartásban szerepelnie kell. Felhőalapú jegykezelőnél a közreműködővel szemben a kiberbiztonsági követelményeket, különösen az adatok exportját, megőrzését és a szolgáltatás megszűnéskor történő kiadását, szerződésben kell érvényesíteni.²⁰

¹⁴ A Kúria Új Ptk. Tanácsadó Testületének véleménye a jognyilatkozat írásbeliségének követelményeiről a Ptk. 6:7. § (3) bekezdésének alkalmazásában (kuria-birosag.hu); 2012. évi I. tv. 22. § (2) bekezdés a) pont

¹⁵ 910/2014/EU rendelet (eIDAS) 46. cikk; az elektronikus aláírásra ugyanezt a 25. cikk (1) bekezdése mondja ki

¹⁶ 2016. évi CL. tv. 62. § (2) és (4) bekezdés; 2016. évi CXXX. tv. 279. § (1) bekezdés

¹⁷ 2016. évi CXXX. tv. 325. § (1) bekezdés f) pont

¹⁸ 7/2024. (VI. 24.) MK rendelet 2. melléklet 4.3., 4.24., 4.25. és 4.38. pont (A, J, M), valamint 4.33. pont (M)

¹⁹ 2024. évi LXIX. tv. 4. § 86. pont és 6. § (5) bekezdés c) pont

4.5 Ahol az erősebb forma indokolt marad

A jegykezelő nem váltja ki az összes dokumentumot. Három esetkörben javasoljuk továbbra is a saját kezű vagy a minősített elektronikus aláírást. Az első a vezetőnek fenntartott döntések köre (az IBSZ kiadása, a biztonsági osztályba sorolás, a használatbavételi jegyzőkönyv), ahol a vezetői felelősség miatt a teljes bizonyító erő értékes.²¹ A második a hatóságnak megküldött vagy külső féllel kötött dokumentum, ahol a másik fél alaki elvárásai is számítanak. A harmadik az a néhány követelmény, ahol a rendelet kifejezetten aláírást említ, mint a munkaviszony megszűnése utáni kötelezettségek aláírt elismerése, amely egyik osztályban sem kötelező.²² A felhasználói nyilatkozatokat (a hozzáférési szabályok megismerése és elfogadása) a rendelet „dokumentált módon” kívánja²³, ezért ezek elektronikusan is rögzíthetők.

Az adatvédelmi incidensek dokumentálását a GDPR is megköveteli, a bejelentési kötelezettségtől függetlenül.²⁴ A jegykezelő incidensjegye ezt is kiszolgálhatja, ha a személyes adatokat érintő incidensek külön jelölhetők, és a jegy tartalmazza az incidens tényeit, hatásait és a megtett intézkedéseket.

5. FELHASZNÁLT FORRÁSOK

- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (NIS 2 irányelv)
- Az Európai Parlament és a Tanács 910/2014/EU rendelete az elektronikus azonosításról és bizalmi szolgáltatásokról (eIDAS), az (EU) 2024/1183 rendelettel módosított szöveg
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (általános adatvédelmi rendelet, GDPR)
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 2013. évi V. törvény a Polgári Törvénykönyvről (Ptk.)
- 2012. évi I. törvény a munka törvénykönyvéről (Mt.)
- 2016. évi CL. törvény az általános közigazgatási rendtartásról (Ákr.)
- 2016. évi CXXX. törvény a polgári perrendtartásról (Pp.)
- 1995. évi LXVI. törvény a köziratokról, a közlevéltárakról és a magánlevéltári anyag védelméről (Ltv.), valamint 335/2005. (XII. 29.) Korm. rendelet a közfeladatot ellátó szervek iratkezelésének általános követelményeiről
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről

²⁰ 2024. évi LXIX. tv. 4. § 24. pont, 6. § (3) bekezdés 1. pont d) alpont és 6. § (5) bekezdés d) pont; 7/2024. (VI. 24.) MK rendelet 2. melléklet 1.5. pont (A, J, M)

²¹ VFP2 KiberVéd jogi állásfoglalás 2026/40, A NIS2-kompatibilis információbiztonsági szabályozás és egyéb dokumentumok jóváhagyása és kihirdetése, 3.4. pont

²² 7/2024. (VI. 24.) MK rendelet 2. melléklet 14.6.2. és 14.10.2. pont (O)

²³ 7/2024. (VI. 24.) MK rendelet 2. melléklet 14.9.3.1. pont (A, J, M)

²⁴ (EU) 2016/679 rendelet 33. cikk (5) bekezdés; EDPB 9/2022. számú iránymutatás a személyes adatok megsértésének bejelentéséről; a NAIH honlapján közzétett tájékoztató az adatvédelmi incidensek bejelentéséről (naih.hu)

- 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
- 1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról
- A Kúria Új Ptk. Tanácsadó Testületének véleménye a jognyilatkozat írásbeliségének követelményeiről a Ptk. 6:7. § (3) bekezdésének alkalmazásában
- Európai Adatvédelmi Testület (EDPB), 9/2022. számú iránymutatás a személyes adatok megsértésének az általános adatvédelmi rendelet szerinti bejelentéséről (2.0 verzió, 2023)
- MSZ EN ISO 19011:2018, Irányelvek irányítási rendszerek auditálásához
- ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection. Information security management systems. Requirements
- ISACA, Information Technology Audit Framework (ITAF), 4. kiadás (2020), 1205 Evidence szabvány
- NIST Special Publication 800-53A Revision 5, Assessing Security and Privacy Controls in Information Systems and Organizations (2022)
- VFP2 KiberVéd jogi állásfoglalás 2026/40, A NIS2-kompatibilis információbiztonsági szabályozás és egyéb dokumentumok jóváhagyása és kihirdetése