Az EU és az USA információbiztonsági szabályozásának összehasonlítása

# Kiberbiztonsági szabályozás Európában

# Dr. Debreceni Csaba

# Nemzeti Közszolgálati Egyetem, Közigazgatási Továbbképzési Intézet Elektronikus információbiztonsági vezető szakirányú továbbképzési szak

## csaba.debreceni@incquerylabs.com

## *A prezentáció alapvető kulcsszavai (4-7 db): Európai Unió, Amerikai Egyesült Államok, információbiztonság, szabályozás, magánszektor, összehasonlítás*

Bevezetés

Léteznek olyan, a magánszektorban működő cégcsoportok, amelyek az Amerikai Egyesült Államokban (a továbbiakban: USA) és az Európai Unióban (a továbbiakban: EU) is rendelkeznek leányvállalattal. Ezen szervezetek esetében fontos tisztában lenni az USA és az EU információbiztonsággal kapcsolatos szabályozásával, illetve érdemes megvizsgálni, hogy milyen hasonlóságok és különbségek figyelhetők meg a két szabályozási rendszer között.

Tekintettel arra, hogy előfordulhat, hogy a szervezet különböző folyamatai eltérő kontinenseken találhatóak meg, és az egyes folyamatok között van információáramlás is, nem minden esetben egyértelmű, hogy az egyes folyamatoknak, illetve az egyes szervezeti egységeknek milyen kötelezettségei vannak, amennyiben vannak.

Jelen dolgozat célja (i) az EU és az USA információbiztonsági szabályozásának meghatározott szempontok szerinti összevetése, (ii) egy esettanulmányon keresztül a szabályozások implikációinak bemutatása, (iii) végül az esettanulmányban szereplő cégcsoport számára konkrét javaslatok meghatározása.

Esettanulmány: EU-ban és USA-ban leányvállalattal rendelkező cégcsoport

Az esettanulmányban szereplő kutatás-fejlesztési cégcsoport elsősorban biztonságkritikus rendszerek fejlesztésével kapcsolatos innovatív megoldásokon dolgozik a tématerület kiemelkedő partnereivel (pl.: űrtechnológia, haditechnika, önvezető autók, ipari automatizáció, kiberfizikai rendszerek stb.). A szervezet jövőbeli tervei között szerepel az Európai Unióban és az USA-ban található nagyvállalatokkal történő együttműködés, szerződéskötés ezeken a területeken. Ennek érdekében egy olyan cégcsoport struktúrát alakított ki, amelynek egyik leányvállalata Budapesten, míg másik leányvállalata Austinban, Texas államban található meg. A szervezet célja olyan információbiztonsági szintet elérni mindegyik leányvállalatánál, amellyel képes lehet az EU-ban, illetve az USA-ban egyaránt akár hadiipari nagyvállalatokkal együtt dolgozni, pl.: Saab, Thales vagy Lockheed Martin.

# Korábbi nemzetközi összehasonlítások

Több nemzetközi összehasonlítás is készült már az információbiztonsági szabályozásokról. Az összefoglalók közötti különbséget elsősorban a *kulcsindikátorok* és a *vizsgált országok* adják, valamint az, hogy az EU és az USA tekintetében tagállami és uniós/szövetségi szinten történik-e az elemzés.[[1]](#footnote-1)

Johnson et al [1] több vezető hatalom információbiztonsági szabályozását elemezte (Brazília, Kína, Indonézia, India, EU és USA). A tanulmány megvizsgálja a hatályban lévő *kiberbűnözéshez köthető jogszabályokat/jogi eszközöket*, a *kikényszerítés eszközeit* és a *gyakorlati eljárásokat*. Az EU esetében nincs általános – közösségi szintű – bemutatás, az értekezés csak Németországot vizsgálja meg az adott szempontok szerint, míg az USA vonatkozásában szövetségi szintű vizsgálatot folytattak le a szerzők.

Az EU Cyber Direct [2] az EU által támogatott weboldal, amelyen keresztül különböző országokat lehet összehasonlítani az információbiztonság témakörében az EU-val az alábbi indikátorok szerint: *általános információk*, *nemzetközi törvények*, *magatartási normák*, *ellenálló képesség*, *kiberbűnözés*. Az összehasonlítás bővíthető további országokkal (pl.: Kína, Ausztrália, Nagy-Britannia stb.), azonban a tagállamok egymással történő összehasonlítása nem lehetséges.

Susan Lincke [3] könyvrészletében az alábbi aspektusokat vizsgálja meg elsősorban az USA kontextusában: *kiberbiztonsághoz és kiberbűnözéshez köthető jogszabályok, kiberbiztonsági érintettségű szabványok*, amelyeknek meg kell felelni a szervezeteknek. A tanulmány kitekintésként vizsgál meg egyéb területeket, mint az EU vagy India.

A Gibson, Dunn & Crutcher LLP egy nemzetközi ügyvédi iroda, amelynek az USA-ban, Európában, Afrikában, valamint Ázsiában is található irodája és az egyik fő szakterületük az információ- és adatbiztonság. Beszámolójukban [4] összeszedték, hogy milyen *jogi és gyakorlati változások* történteka 2021-es évben az információbiztonság területén. Az összefoglaló külön kitér az EU-s tagállamokra is, azonban az USA-ról nem tartalmaz információt.

Összegzésképp megállapítható, hogy a nemzetközi összehasonlító tanulmányok száma limitált, illetve az egyes tagállamokra jellemző összehasonlítás publikusan nem elérhető. Továbbá az is látható, hogy a kiberbiztonsághoz és kiberbűnözéshez köthető jogszabályok, valamint a kikényszerítés eszközei több tanulmányban is megtalálhatóak.

# Nemzetközi információbiztonsági szabványok

Nemzetközi viszonylatban két nagyobb szabvány határozza meg a köz- és magánszektorban szereplő szervezetek információbiztonsági követelményeit: *ISO/IEC 27001* és *NIST SP 800-171*. Ezen kívül természetesen még léteznek egyéb fontos szabványok is (ITIL, CC, INFOSEC stb.), ezek azonban jelen dolgozat kontextusában nem relevánsak.

*ISO/IEC 2700x-es szabványcsoport:* a Nemzetközi Szabványügyi Szervezet (ISO) és a Nemzetközi Elektrotechnikai Bizottság (IEC) által kiadott szabványcsoport, amely segítséget nyújt a szervezetek számára információbiztonsági irányítási rendszer (ISMS) létrehozásában, karbantartásában és folyamatos fejlesztésében. Az irányítási rendszer magában foglalja a szervezetet, a struktúrát, a szabályzatokat, a tervezési tevékenységeket, a felelősségeket, a gyakorlatokat, az eljárásokat, a folyamatokat és az erőforrásokat. Fontos kiemelni az ISO 27001:2013[5] szabványt, amely a kialakítandó ISMS-hez kapcsolódó követelményrendszert határozza meg, illetve az ISO 27002:2016 [6] szabványt, amely az ISMS-hez kapcsolódó információbiztonsági intézkedéseket definiálja.

*NIST SP 800-171 szabvány:* Az USA Nemzeti Szabványügyi és Technológiai Intézete (NIST) által kiadott szabvány fő fókuszában az ellenőrzött, de nem minősített adatok védelmével kapcsolatos követelmények állnak. Ez azt jelenti, hogy a NIST SP 800-171[7], hasonlóan az ISO27002:2016-os szabványhoz, konkrét intézkedéseket határoz meg a szervezet ISMS-éhez kapcsolódóan. Továbbá tartalmazza az összes ISO27002:2016 által meghatározott intézkedést is, amelyet további elemekkel bővít. Az NIST SP 800-171 párjaként érdemes még az NIST SP 800-53 [8] szabványt is megemlíteni, amely olyan biztonsági és adatvédelmi intézkedéseket definiál, amelyek kötelezőek a szövetségi szervezetekre nézve.

# Releváns jogi környezet

Az esettanulmány alapján a jogi szabályozásokat külön kell vizsgálni EU-s szinten és külön elemezni szükséges az USA viszonylatában. Végül meg kell állapítani, hogy létezik-e a szabályozásoknak olyan közös metszete, amely az USA-ban és az EU-ban egyaránt érvényes.

*EU.* Az EU jogalkotói szerepkörben többek között definiálhat rendeletet és irányelvet. A rendelet olyan kötelező jogalkotási aktus, amely az EU egész területén teljes egészében alkalmazandó. Az irányelv ettől eltérően olyan jogalkotási aktus, amely minden tagállam számára kötelezően elérendő célkitűzést állapít meg, de az azzal kapcsolatos döntéshozatal módja az egyes országokra van bízva.

*Uniós szintű.* Az információbiztonsághoz kapcsolódóan egyetlen irányelv létezik jelenleg, amely minden tagállamra nézve kötelező érvényű. A NIS irányelv [9] célja, hogy minden tagállam rendelkezzen minimális képességekkel, intézményrendszerrel és szabályokkal annak érdekében, hogy az információbiztonság nemzeti – és közösségi – szinten biztosítva legyen. Az irányelv bizonyos feltételek mentén meghatározható szervezetek csoportjaira vonatkozó, speciális szabályokat állapít meg, amelyekhez a tagállamoknak jogszabályokban rögzített, információbiztonsági követelményeket kell társítaniuk. Az irányelv uniós szintű együttműködést ír elő minden olyan helyzet esetén, ahol határon átnyúló biztonsági incidens történik, ezek hatékony kezelése (és megelőzése) érdekében életre hívta az Együttműködési Csoportot tapasztalatmegosztási és szabályozási, valamint a CSIRT Hálózatot operatív kapacitásépítési és eseménykezelési céllal. A Kiberbiztonsági jogszabály [10] az információs és kommunikációs technológiák (IKT) kiberbiztonsági tanúsítási rendszerét definiálja, amely kihat az IKT termékek, szolgáltatások és folyamatok fejlesztésére, illetve meghatározza az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) feladatait. Ezen kívül a GDPR [11] tartalmaz részben az információbiztonsághoz kapcsolódó intézkedéseket, amely érvényes minden szervezetre az EU-n belül. Ennek megfelelően kötelezettségként rögzíti a kockázat mértékének megfelelő szintű adatbiztonság garantálását.

*Tagállami szintű: Magyarország.* Hazánkban elsősorban a 2013. évi L. törvény (a továbbiakban: Ibtv.) [12] határozza meg az információbiztonsághoz kapcsolódó előírásokat, amelynek hatálya azonban nem terjed ki minden magánszektorban megtalálható szervezetre. A törvényhez kapcsolódóan a 41/2015. BM rendelet [13] definiálja az Ibtv.-ben megtalálható kockázatelemzési módszer gyakorlatban történő alkalmazásának részleteit, illetve, hogy meghatározott biztonsági osztályban lévő elektronikus információs rendszer esetén milyen védelmi intézkedéseket szükséges implementálnia a szervezetnek. Továbbá a 2001. évi CVIII. törvény (Ekertv.) [14] foglalkozik még az információs társadalommal összefüggő szolgáltatások egyes kérdéseivel.

*USA.* Az USA-ban az információbiztonsághoz kapcsolódó szabályozások két szinten kerülnek meghatározásra. A szövetségi szinten meghozott döntések az összes tagállamra vonatkoznak, azonban az egyes államok meghatározhatnak tagállami szintű szabályozásokat is.

*Szövetségi szintű.* A kiberbiztonsághoz kapcsolódó bűnesetekről a CFAA [15] törvény rendelkezik elsődlegesen szövetségi szinten az USA területén. Emellett a FISMA [16] 2014-es kiegészítése elrendeli minden olyan szervezet számára, amely kapcsolatban áll a szövetségi kormányzattal, hogy teljesítse a NIST által meghatározott információbiztonsági követelményeket (NIST SP 800-53 [8]). A 2015-ös CISA [17] törvény felhatalmazást ad arra, hogy a cégek maguk monitorozhassák a saját rendszereiket és védelmi intézkedéseket hozzanak létre az információs rendszereik védelme érdekében. Ezen felül a törvény biztosítja a lehetőséget az incidensekkel és kiberfenyegetésekkel kapcsolatos információk kormányzati szervekkel történő megosztására. Az információmegosztáshoz kapcsolódóan pedig szigorú követelményeket határoz meg. A privát szektorhoz kapcsolódó egyik legfontosabb szövetségi szintű szabályozást az FTCA [18] 5. fejezete tartalmazza, amely a cégek jelentős többségére nézve definiál információbiztonsági és adatvédelmi előírásokat, amelyek szerint a hatálya alá tartozó szervezeteknek ésszerű keretek között szükséges meghatározniuk védelmi intézkedéseiket. Végül a DFAR [19] olyan szervezetekre nézve hatályos, akik az USA Védelmi Minisztériumának beszállítóiként, valamint e szervezetek számára beszállítást végző szervezetként tevékenykednek. Ezen cégek számára pedig kötelezővé teszi az NIST SP 800-171-es [7] szabványnak történő megfelelést.

*Tagállami szintű: Texas.* Bár több tagállamnak vannak részletes szabályozásai az információbiztonság tekintetében, Texas-ban csak az állami szervezetekre, valamint a közép- és felsőoktatási intézményekre vonatkozóan létezik jogszabály [20]. Az egyetlen releváns jogszabály a TSB 2126 [21], amely megtiltja, hogy külföldi tulajdonban lévő cég bármilyen jogviszonyba kerüljön olyan kritikus infrastruktúrákkal, amelyek Texas állam területén találhatóak. Mindemellett Texas államnak saját állami kiberbiztonsághoz kapcsolódó szervezete működik, a Texas Cybersecurity Council, amelynek célja az állami kiberbiztonság megvalósítása és fejlesztése együttműködve a magánszektorban található cégekkel. Az állam kidolgozott egy kiberbiztonsági keretrendszert is (Texas Cybersecurity Framework), amely általánosan alkalmazható – de nem kötelező – bármely szervezet számára annak érdekében, hogy meghatározza a kiberbiztonsági kockázatokat és a kockázatokhoz kapcsolódó költséghatékony megoldásokat ajánljon.

*EU és USA közös szabályozásai.* Jelenleg nincs közös szabályozás[[2]](#footnote-2).

Szabályozások összehasonlítása

*Kulcsindikátorok meghatározása.* Egy privát szférában működő szervezet esetében fontos azokat az indikátorokat meghatározni, amelyek relevánsak lehetnek mindkét földrészen működő leányvállalat számára. Ennek megfelelően jelen pontban kizárólag olyan indikátorokat azonosítok, amelyek feltétlenül szükségesek a tárgyi szervezet törvényes működése szempontjából:

* releváns hatóságok és eseménykezelő központok: fontos meghatározni, hogy a szervezetnek mely hatóságokkal kell kapcsolatot tartania, illetve mely hatóságoktól kérhet segítséget, akár sérülékenységvizsgálat vagy incidensbejelentéssel kapcsolatban.
* követelmények: a jogi szabályozás miatt meg kell vizsgálni, hogy melyek azok a kötelező intézkedések, dokumentációk, képességek stb., amelyekkel egy magánszervezetnek rendelkeznie kell ahhoz, hogy jogszerűen működhessen.
* elvárt szabványok és tanúsítványok: melyek azok a szabványok, illetve tanúsítványok, amelyekkel a szervezetnek rendelkeznie kell.

*Releváns hatóságok és központok[[3]](#footnote-3).* Az EU szintjén a NIS irányelv [9] megköveteli a tagállamoktól, hogy határozzák meg a kompetens nemzeti hatóságokat. Uniós szinten a cégek, illetve magánszemélyek információbiztonsági kérdéseikkel az ENISA[[4]](#footnote-4)-t kereshetik meg, amely azonban nem hatósági tevékenységet lát el, hanem ügynökségként működik. Magyarország tekintetében elsősorban a Nemzetbiztonsági Szakszolgálat keretein belül működő Nemzeti Kibervédelmi Intézet (NKI) szolgáltatásait vehetik igénybe a cégek és magánszemélyek. Így például a kiberbiztonsághoz kapcsolódó incidenseket az NKI felületén lehet jelezni, illetve sérülékenységvizsgálatot, vagy az incidens kivizsgálását is lehet kérni a szervezettől. Az Ibtv. és az Ekertv. hatálya alá eső szervezeteknek pedig törvényi kötelességük az NKI szolgáltatásait igénybe venni.

Az USA-ban több olyan szövetségi szintű hatóság is van, amely a kibertámadások esetén eljárhat. A szervezeteknek és magánszemélyeknek pedig annak megfelelően kell jelenteniük a kiberbiztonsági incidenst, hogy milyen típusú volt a támadás. Néhány fontosabb szervezet:

* az FBI IC3 központja, ahol magánszemélyek jelezhetnek kiberincidenseket;
* az FBI Field Office Cyber Task Forces-nál lehet olyan kiberincidenst jelenteni, amely szövetségi szintű terrorista támadásnak, vagy hírszerzésnek, esetleg külföldről érkező ipari kémkedésnek tekinthető; valamint
* általánosan a Cybersecurity and Infrastructure Security Agency részére lehet jelenteni a kiberbiztonsági incidenseket, úgy mint adathalász email-ek, szoftver sebezhetőségek stb.

Állami szinten viszont nincs olyan hatóság, amelynek kezelnie kellene a bejelentéseket. Kiberbiztonsági kérdésekben egyetlen releváns állami szintű szervezet Texas államban az Information Sharing and Analysis Organization, amely elsősorban a kiberbiztonsághoz kapcsolódóan biztosít tudásmegosztó platformot kormányzati és magánszervezetek között.

*Kötelező intézkedések:* A releváns törvények és jogszabályok alapján Magyarországon az Ibtv. és Ekertv. hatálya alá eső szervezetek számára kötelezően előírt intézkedések kerültek megfogalmazásra az információbiztonsághoz kapcsolódóan (pl. informatikai biztonsági szabályzat, biztonsági osztályba és szintbe sorolás, incidensjelentési kötelesség stb.), azonban egyéb - a törvény hatálya alá nem tartozó – szervezetek számára nincs olyan kötelező jogszabályi előírás, amely a törvényes működéshez szükséges. Mindemellett EU-s szinten a GDPR a szervezet kötelezettségeként rögzíti a kockázat mértékének megfelelő szintű adatbiztonság garantálását.

Az USA vonatkozásában megjelenik a szövetségi szintű törvényi kötelezettség az FTCA 5. fejezete szerint, amely alapján minden szervezetnek kötelező ésszerű kereteken belül adatvédelmi és információbiztonsági intézkedéseket definiálni és megvalósítani. A törvény azonban nem azt vizsgálja, hogy léteznek-e ilyen intézkedések, hanem elvárja, hogy amennyiben incidens történik, a szervezet bizonyítani tudja, hogy minden tőle telhető intézkedést megtett az incidens elkerülése érdekében. Texas esetében viszont nincs további jogszabályi kötelezettség, amely szükséges lenne ahhoz, hogy a szervezet információbiztonsági aspektusból törvényesen működhessen.

*Elvárt szabványok és tanúsítványok:* Az EU-ban jellemzően az ISO/IEC 27001-es tanúsítvány meglétét vizsgálják a magánszférában működő nagyvállalatok és szervezetek, amikor szerződéses viszonyba kerülnek más cégekkel. Azonban erre nincs törvényi kötelezettség sem uniós szinten, sem Magyarország tekintetében.

Az USA esetében jellemzően az NIST SP 800-171 követelmények megvalósulását vizsgálják. Törvényi kötelezettség azonban csak olyan cégek számára létezik, amelyek beszállítói az USA Védelmi Minisztériumának, illetve beszállítói feladatot látnak el e cégek számára.

Ajánlások az esettanulmányban szereplő szervezetre vonatkozóan

Az esettanulmányban szereplő szervezet esetén meg kell vizsgálni a jogszabályi kötelezettségeket az információbiztonság szempontjából, illetve a cég stratégiájából adódóan érdemes további ajánlásokat megfogalmazni.

*Leányvállalat az USA-ban:* törvényi szempontból csak az FTCA 5. fejezetében szereplő kockázatarányos védelmi intézkedések bevezetése tekinthető kötelezőnek. Mindemellett mivel a szervezet céljai között szerepel olyan partnerekkel történő együttműködés, akikre érvényes a DFAR, ezért a cégcsoport amerikai részlegének teljesítenie kell az NIST SP 800-171 követelményeket és meg is kell szereznie a kapcsolódó tanúsítványt.

*Leányvállalat az EU-ban:* a jogszabályi megfelelés szempontjából csak a GDPR-ban meghatározott adatbiztonságot kell kockázatokkal arányos mértékben garantálni. Mivel a szervezetcéljai között szerepel az EU-n belül további nagyvállalatokkal történő együttműködés, ezért célszerű az ISO/IEC 27001 tanúsítvány megszerzése. Bár a szervezet nem tervezi, hogy Magyarországon olyan tevékenységekbe kezdjen, amely miatt az Ekertv. hatálya alá kerülne (pl.: online piactér üzemeltetése, keresőmotor üzemeltetése stb.), vagy az Ibtv. hatálya alá kerülne (pl.: alapszolgáltató beszállítója) célszerű az Ibtv. által meghatározott törvényi előírások gyakorlatba történő átültetése is, hiszen közbeszerzések esetén ez előnyt jelenthet.

*Kapcsolat a két leányvállalat között.* Mivel a két leányvállalat között folyamatos a kommunikáció és együttműködés, ezért célszerű a szervezet információbiztonsági stratégiáját közösen meghatározni. Ennek megfelelően mindkét szervezet esetén ajánlott legalább az NIST SP 800-171 által meghatározott követelmények és kontrollok implementálása.

Összességében elmondható, hogy az egész szervezetnek célszerű végrehajtani az ISO 27001-ben és NIST SP 800-171-ben meghatározottakat. Mivel utóbbi építkezik az ISO/IEC 2700x-es szabványcsoportra, ezért érdemes a két leányvállalat esetében először az ISO 27001 tanúsítvány által megkövetelt kontrollokat bevezetni, majd utána az NIST SP 800-171-es követelményeknek megfelelni. Végül a magyar leányvállalat esetében az Ibtv. és a 41/2015 BM rendelet által meghatározott előírások és kontrollok bevezetése következhet, amely egyébként az NIST SP 800-53 szabvány alapján készült.

Összefoglalás

Jelen dolgozatban információbiztonsági kötelezettségek aspektusából összehasonlítottam az EU és az USA kiberbiztonsági szabályozását. Az összehasonlítást egy esettanulmányban szereplő szervezet viszonylatában végeztem el, amely az EU-ban és az USA-ban egyaránt rendelkezik leányvállalattal.

Az összehasonlításhoz kapcsolódóan 1) áttekintettem a releváns szakirodalmat és jogi eszközöket, 2) azonosítottam azokat a kulcsindikátorokat, amelyek alapján releváns összehasonlítás képezhető, 3) végrehajtottam a kulcsindikátorok szerint az összehasonlítást, végül 4) ajánlásokat fogalmaztam meg a szervezet számára.

A dolgozatból kiderül, hogy az esettanulmányban szereplő szervezet számára az USA-ban FTCA 5. fejezete alapján, míg az EU-ban a GDPR alapján van jogszabályi kötelezettség részben az információbiztonsághoz kapcsolódóan. Azonban a szervezet stratégiai céljainak elérése érdekében érdemes az ISO/IEC 27001, az NIST SP 800-171 és a Ibtv., illetve a 41/2015 BM rendelet által meghatározott követelményeket teljesíteni.

Irodalomjegyzék

|  |  |
| --- | --- |
| [1] | J. Johnson, S. J. Lincke, R. Imhof és C. Lim, „A comparison of international information security,” *Interdisciplinary Journal of Information, Knowledge, and Management,* 9. kötet, pp. 89-116, 2014. |
| [2] | EU Cyber Direct, „Compare United States and European Union,” [Online]. Available: https://eucyberdirect.eu/atlas/country/united-states/compare/european-union. [Hozzáférés dátuma: 02 04 2022]. |
| [3] | S. Lincke, „Complying with Security Regulation and Standards,” in *Security Planning*, Cham, Springer, 2015, pp. 39-58. |
| [4] | Gibson Dunn, „International Cybersecurity and Data Privacy Outlook and Review,” Gibson, Dunn & Crutcher LLP, 31 01 2022. [Online]. Available: https://www.gibsondunn.com/international-cybersecurity-and-data-privacy-outlook-and-review-2022/. |
| [5] | ISO/IEC 27001:2013, Information technology, Security Techniques, Specification for an Information Security Management System, Geneva, Switzerland, 2013. |
| [6] | ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls, Geneva, Switzerland, 2022. |
| [7] | R. Ross, V. Pillitteri, K. Dempsey, M. Riddle és G. Guissanie, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST Special Publication (SP) 800-171, Rev 2., National Institute of Standards and Technology, Gaithersburg, MD, 2020. |
| [8] | Joint Task Force Transformation Initiative Interagency Working Group (2013), Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication (SP) 800-53, Rev 5., National Institute of Standards and Technology, Gaithersburg, MD, 2020. |
| [9] | *Az Európai Parlament és a Tanács 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjén biztosító intézkedésekről,* 2016. |
| [10] | *Az Európai Parlament és a Tanács 2019/881 rendelete az ENISA-ról és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről,* 2019. |
| [11] | *Az Európai Parlament és a Tanács 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről,* 2016. |
| [12] | *2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról,* 2013. |
| [13] | *41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági os,* 2015. |
| [14] | *2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről,* 2001. |
| [15] | *Computer Fraud and Abuse Act,* 1986. |
| [16] | *Federal Information Security Modernization Act,* 2014. |
| [17] | *Cybersecurity Information Sharing Act,* 2015. |
| [18] | *Federal Trade Commission Act,* 1914. |
| [19] | *Defense Federal Acquisition Regulation Supplement.* |
| [20] | *Texas Administrative Code Chapter 202,* 1999. |
| [21] | *Texas Senate Bill 2116,* 2021. |

## Plágium-nyilatkozat

# Nyilatkozat az absztrakt és a prezentáció készítésére vonatkozó szabályok betartásáról

# Alulírott …………………………………………………………………………(név)………………………… (Neptun kód) büntetőjogi felelősségem tudatában, a nyilatkozat aláírásával kijelentem, hogy a záróvizsgához kapcsolódó dokumentáció készítése során betartottam a szerzői jogról szóló 1999. évi LXXVI. törvény szabályait, valamint az egyetem által előírt szabályokat. Egyúttal nyilatkozom arról, hogy a záróvizsgán bemutatott prezentáció, és annak az alapját képező absztrakt a saját szellemi termékem, önálló munkám, az abban szereplő valamennyi táblázat, ábra, diagram és illusztráció fentiek alapján szerzői jogi szempontból rendezett, lehivatkozásra került, idézés nélkül azokat nem használtam fel. Jelen nyilatkozat aláírásával tudomásul veszem, hogy amennyiben bizonyítható, hogy ezen szellemi terméket nem magam készítettem vagy azzal kapcsolatban szerzői jogsértés ténye merül fel, az egyetem ellenem fegyelmi eljárást indíthat. A fegyelmi eljárás indítása nem érinti a szerzői jogsértés miatti egyéb (polgári jogi, szabálysértési jogi, büntetőjogi) jogkövetkezményeket. Tudomásul veszem, hogy prezentáció esetén plágiumnak számít különösen: Szó szerinti idézet közlése idézőjel és hivatkozás megjelölése nélkül; tartalmi idézet hivatkozás megjelölése nélkül; más publikált gondolatainak saját gondolatként való feltüntetése.

Dr. Debreceni Csaba

H1HNR5

Budapest, 2022. június 2.

Hallgató aláírása

1. A kapcsolódó munkák összehasonlítása táblázatos formában az alábbi linken érhető el:  
   <https://github.com/debrecenics/information-security-officer-thesis/blob/main/appendix/related-work.md> [↑](#footnote-ref-1)
2. Bár korábban volt egyezmény az EU és az USA között egy biztonságos adatvédelmi és információbiztonsági mechanizmus kialakítására, amelynek a neve Adatvédelmi Pajzs (Privacy Shield) volt, azonban ezt az egyezményt 2020-ban hatályon kívül helyezték. [↑](#footnote-ref-2)
3. A releváns hatóságokkal kapcsolatos tételes leírás az alábbi linken érhető el  
   <https://github.com/debrecenics/information-security-officer-thesis/blob/main/appendix/authorities-comparison.md> [↑](#footnote-ref-3)
4. Európai Uniós Kiberbiztonsági Ügynökség (European Union Agency for Cybersecurity - ENISA) [↑](#footnote-ref-4)