Szerzők: Horváth István, Dr. Horváth Zsolt, Tóth Zoltán (INFOBIZ Kft.)

IRÁNYÍTÁSI SZABVÁNYOK A GDPR SZOLGÁLATÁBAN

Az INFOBIZ Informatikai, Információ-biztonsági és Vezetési Tanácsadó Kft. 2006-ban alakult, magyar tulajdonban lévő tanácsadói tevékenységet végző vállalkozás. Kiemelt üzleti területeink az információbiztonsági, a minőségügyi / vezetési tanácsadás, a személyes adatvédelmi és az üzletmenet-folytonossági tanácsadás. Az információbiztonsági tanácsadási tevékenységeink során nagy tapasztalattal rendelkezünk a szoftverfejlesztés és -üzemeltetés, az informatikai szolgáltatások, a startup vállalkozások, az autóipari beszállító vállalkozások és a pénzügyi szektor informatikai beszállító vállalkozásainak ágazati speciális követelményeinek megoldásában is.

1. BEVEZETÉS

Felmerülhet a kérdés, hogy mi a kapcsolat a GDPR rendelet és az ISO szabványok között? A válasz kézenfekvő. A rendelet a személyes adatok kezelésének teljes felelősségét és kockázatát az adatkezelőkre hárítja, amit a hatóságokon keresztül komoly szankciórendszerrel képes kikényszeríteni. Ráadásul csak a szigorú elvárásokat fogalmazza meg, a megfelelő kivitelezést az adatkezelőre bízza. Ezzel párhuzamosan az elszámoltathatóság elvével folyamatos bizonyíthatóságra kényszeríti az adatkezelőket. A szervezetek vezetőinek így egyszerre kell jogi, szervezési és technikai kihívásokkal megbirkózniuk. A jogi megfelelés mellett komoly kihívást jelent a kezelt adatok biztonságának garantálása, a kockázatok menedzselése, az esetleges incidensek kezelése és a rendelkezésre állással összefüggő folytonossági kérdések. Mivel egy jól kiépített irányítási rendszer nagymértékben képes csökkenteni azokat a kockázatokat, amelyeknek az adatkezelők, adatfeldolgozók és nem utolsó sorban az érintettek ki vannak téve, fontos kérdéssé vált a szabványok bevezetésének lehetősége és ennek gyakorlati kérdései.

A cikk nagyrészt az ELTE Állam- és Jogtudományi Kar Jogi Továbbképző Intézetéhez 2021-ben benyújtott és megvédett azonos témájú szakdolgozat kivonatán alapszik.[1]

2. ADATVÉDELEM FEJLŐDÉSE A GDPR RENDELETIG

Mai világunkat nagymértékben meghatározzák és befolyásolják a nagy technológiai cégek és az általuk közvetített tartalom. Az elmúlt pár évben több olyan, a személyes adatok megszerzésével és felhasználásával kapcsolatos botrány robbant ki (pl. Facebook és hozzá kapcsolható cégek), ami rávilágított arra a tényre, hogy az emberek személyes adatai nincsenek biztonságban. Ezt a tényt a nemzetközi és hazai jogalkotók is felismerték, és ez alapján dolgozhatták ki az Általános Adatvédelmi Rendeletet (GDPR)[2].

Az adatvédelem szabályozása – nemzetközi kitekintés

Az európai országok az 1970-es évektől kezdtek el adatvédelmi törvényeket kialakítani, amelyek a személyes adatok hatóságok és nagy cégek általi gyűjtésének és feldolgozásának ellenőrzését célozták meg. A személyes adatok védelméhez való jog a technikai fejlődés hozományaként alakult ki.

A személyes adatok védelméhez való jogot csak szűkebb körben értelmezhetjük. Itt a fő kérdés az, hogyan védjük az adatokat, amikor azok valamilyen módon feldolgozásra kerülnek. Minden olyan

esetben, amikor személyes adatainkat feldolgozzák, automatikusan ezen jogunk védelme életbe lép. A technika fejlődésével egyre sürgetőbb lett, hogy a személyes adatok feldolgozását központosított, jogi formában is kontrollálják az államok. 1981-ben az Európai Tanács elfogadta a 108-as egyezményét, amely az automatikus adatfeldolgozásról szól. Ez az egyetlen olyan nemzetközi egyezmény az adatvédelem területén, amely jogilag kötelező minden tagra, aki aláírta.

Az egyezmény minden állami- és magán szektorban végzett adatfeldolgozásra vonatkozik, beleértve a bűnüldöző és igazságszolgáltatási szervek által végzett adatfeldolgozást is. Védi az egyéneket a személyes adatok feldolgozását kísérő visszaélésekkel szemben, és ezzel egyidejűleg a személyes adatok határokon átnyúló áramlásának szabályozására törekszik. Valamennyi EU-tagállam ratifikálta a 108-as egyezményt, majd 2001-ben elfogadták a 108-as egyezmény kiegészítő módosítását, melynek értelmében rendelkezéseket vezettek be az úgynevezett harmadik országokba irányuló, határon túlnyúló adatáramlásokról és a nemzeti adatvédelmi felügyeleti hatóságok kötelező létrehozásáról. A fentiekben láthattuk, hogy mennyi idő is kellett ahhoz, hogy kialakuljon egyfajta emberi és társadalmi igény az adatvédelemre, illetve milyen technikai hatások kellettek az igény felmerülésére.

A GDPR hatálybalépése előtt az Európai Uniónak egy adatvédelmi eszköze volt. Az európai parlamenti és tanácsi 95/46 / EK irányelve a személyes adatok védelméről és azok feldolgozásáról, valamint azok harmadik fél számára történő továbbításáról szól. Ezen irányelv elfogadása abban az időben történt, amikor már több tagállam kialakította saját, nemzeti adatvédelmi törvényét. Ezzel párhuzamosan jelentkezett a tagállamok részéről az az igény, hogy ezeket a jogszabályokat harmonizálják annak érdekében, hogy a tagállamok közötti szabad adatáramlást biztosítsák, illetve egy magasabb szintű biztonságot adjanak.

A 95/46 / EK adatvédelmi irányelv részletes és átfogó adatvédelmi rendszert hozott létre az Európai Unióban. Az Európai Unió jogrendjével összhangban azonban az irányelvek nem közvetlenül alkalmazandók, hanem át kell ültetni a tagállamok nemzeti jogrendszerébe. A gyakorlat azt mutatja, hogy az irányelvet minden tagállam eltérően ültette át. Ennek eredményeként különféle adatvédelmi szabályok jöttek létre az Európai Unióban, a fogalommeghatározásokat és a szabályokat eltérően értelmezték a nemzeti törvényekben, valamint a végrehajtás szintje és a szankciók súlyossága szintén különböző volt az egyes tagállamokban.

Az információs technológiában jelentős változások történtek az irányelv 1990-es évek közepén történő megfogalmazása óta, így ezen okok együttesen az Európai Unió adatvédelmi jogszabályainak reformjához vezettek. Hosszú tárgyalások eredményeképpen 2016. áprilisában fogadták el az Európai Unió Általános Adatvédelmi Rendeletét, amely 2016. május 24-én lépett hatályba, de csak 2 éves átmeneti állapotot követően 2018. május 25-én vált alkalmazandóvá.

Az adatvédelem szabályozása – Magyarországon

1989-ben a Minisztertanács határozatot hozott a személyes adatok kezeléséről és a közérdekű adatok nyilvánosságáról szóló jogszabály elkészítéséről. A törvény 1992-ben lépett hatályba, így a magyar adatvédelmi szabályozás első lépése az 1992-es adatvédelmi törvény (Avtv.) elfogadása volt. A fenti törvény, nevétől eltérően, nemcsak a személyes adatvédelemre összpontosít, hanem az információs szabadságjogokra is kitér, ami ebben az időben a világon egyedülállónak minősült.

Ezen törvényben deklarált jogok szavatolására független adatvédelmi biztost nevez ki az Avtv., akinek a feladatát, illetve hatáskörét közösen az állampolgári jogok országgyűlési biztosáról szóló 1993. évi LIX. törvénnyel határozta meg. A korábban említett 1995-ös 95/46/EK irányelvben lefektetett elv szerint minden tagállamban létre kell hozni egy független hatóságot és olyan jogosítványokkal, jogi eszközökkel kell felruházni, amelyekkel hatékonyan fel tud lépni a jogsértések ellen.
Ezt a jogi harmonizációt a Magyar Köztársaság Alkotmánya (ma már Alaptörvény VI. cikke) írta elő. Magyarországon a jogi modernizáció az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényben (Info tv.)[3] manifesztálódott. Az Info tv. hasonlóan az Avtv.-hez egymagában rendelkezik az alapvető emberi jogok védelmének feltételeiről és keretéről.

3. A GDPR MEGFELELÉST TÁMOGATÓ ISO SZABVÁNYOK

a) Információbiztonság

A GDPR rendelet alapvetően elvárja a megfelelő adatvédelmi intézkedések kialakítását, amelyek biztosítják a személyes adatok biztonságát, azaz azok bizalmasságát, sértetlenségét és rendelkezésre állását. Ehhez az alábbi szabványok nyújthatnak megfelelő támpontokat. Az információbiztonsági irányítási rendszerek a szervezetek által felhasznált, tárolt és kezelt összes információ biztonságának kockázatarányos védelmét hivatottak biztosítani. Miután a személyes adatok azok az információk, amelyek természetes személyekre vonatkoznak, illetve természetes személyekkel összefüggésbe hozhatók, ezért azok mind a szervezetek információbiztonsági irányítási rendszerének hatókörébe tartoznak.
Az ISO/IEC 27001:2022 szabvány[6] meghatározza az információbiztonsági irányítási rendszer (ISMS) szervezeten belüli létrehozásának, végrehajtásának, karbantartásának és folyamatos fejlesztésének követelményeit, a szervezet igényeihez igazodó információbiztonsági kockázatok felmérésére és kezelésére alapozva. Különlegessége, hogy a szabványtörzsben foglalt általános irányítási rendszer működtetési követelményeken túlmenően az „A mellékletben" felsorolja a négy kiemelt szakmai területhez (szervezeti, emberi, fizikai, technológiai biztonság) tartozó elvárt intézkedéseket. Ezek számozása megegyezik az ISO/IEC 27002:2020-es szabvány megfelelő fejezeteivel, ahol az egyes követelmények megvalósítását segítő gyakorlati útmutatások találhatók.

Az ISO/IEC 27002:2022 szabvány[7] gyakorlati útmutatót nyújt az ISO/IEC 27001:2022-es szabványon alapuló információbiztonsági irányítási rendszerben megvalósítandó információbiztonsági intézkedésekhez és eljárásokhoz (kontrollokhoz). Az iránymutatás kiterjed a megfelelő intézkedések kiválasztására, végrehajtására és felügyeletére, figyelembe véve a szervezet információbiztonsági kockázatait.

GDPR megfelelés támogatása

A szabványok nagymértékben lefedik és támogatják a GDPR IV. fejezet 2. szakaszának biztonsági és szervezési követelményeit, beleértve az áttételes jogi megfelelést, az információbiztonsági incidensek kezelését és a folytonossági követelmények biztonsági aspektusait. Fontos, hogy az incidensmenedzsment és a folytonosság kérdését is az információbiztonság folyamatos fenntartása szempontjából közelíti meg, így ezeket a témákat az ezekre készített célzott rendszerszabványok alapján lehet a valós üzleti igényeknek megfelelően, szervezeti szinten kialakítani. Az új, 2022-es változatban már önálló kontrollként is megjelennek az adatvédelemmel szorosan összefüggő elvárások:

- Adattörlés (8.10 Information deletion)
- Adatmaszkolás (8.11 Data masking)
- Az adatszivárgás megelőzése (8.12 Data leakage prevention)

A szabványnak a GDPR megfelelés támogatásában játszott szerepe kettős, részint keretet biztosít egy megfelelő információbiztonsági rendszer működtetéséhez, másrést alapszabványként szolgál az ISO 27701-es adatvédelmi irányítási rendszer (PIMS - Privacy Information Management Systems) működtetéséhez.

b) Incidenskezelés

A GDPR-ban megfogalmazott adatvédelmi követelmények egyik kulcseleme a feltárt adatvédelmi incidensek megfelelő kezelése. Ehhez a szervezeteknek előre meghatározott és megfelelő incidenskezelési eljárást kell kialakítaniuk, amelyhez az ISO/IEC 27035-as szabványok [8, 9, 10] adnak megfelelő hátteret.
Az ISO/IEC 27035-1:2016 ennek a több részből álló nemzetközi szabványcsoportnak a tagja. Bemutatja az információbiztonsági események és incidensek kezelésének alapfogalmait és fázisait. A szabvány második része (ISO/IEC 27035-2:2016) az eseményekre és incidensekre való reagálás megtervezéséhez és előkészítéséhez, a harmadik része (ISO/IEC 27035-3:2020) az ICT (Information and Communication Technology) specifikus információbiztonsági incidensekre való reagáláshoz nyújt iránymutatást.

Ezek az emberek, a folyamatok és a technológia oldaláról tárgyalják a működésbiztonsági szempontokat. Meghatározzák az ICT információbiztonsági incidensek kezelését, beleértve az információbiztonsági incidensek észlelését, jelentését, vizsgálatát,

elemzését, reagálását, megfékezését, felszámolását, helyreállítását és lezárását. Nem foglalkoznak a nem ICT incidensek elhárítási műveleteivel, például a papíralapú dokumentumok elvesztésével.

A szabványokban megadott alapelvek általánosak, és arra irányulnak, hogy minden szervezetre alkalmazhatóak legyenek, függetlenül azok típusától, méretétől vagy jellegétől. A szervezetek a szabványok útmutatásait az információbiztonsági kockázataikhoz igazítva módosíthatják. Ezen útmutatásokat az információbiztonsági esemény- és incidenskezelési szolgáltatásokat nyújtó külső szervezetek is alkalmazhatják.

GDPR megfelelés támogatása

A GDPR 4. cikke definiálja az adatvédelmi incidens fogalmát, ami a „… biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi." A 33. és 34. cikkek határozzák meg az adatvédelmi incidensek kezelésének megfelelő módját. Ez az adatkezelőkre nyilvántartási, feltárási és dokumentálási kötelezettséget ró, amelyhez szigorú időkeret is társul a 72 órán belüli bejelentési kötelezettséggel. Továbbá szükség esetén az érintettek felé történő indokolatlan késedelem nélküli tájékoztatási kötelezettséget is meghatároz.
Ezek megfelelő teljesítése akkor lehetséges, ha a szervezet valóban felkészült és kialakította a megfelelő incidenskezelési eljárását. A szabványok ezekben szervezeti szintű támogatást képesek nyújtani, a szervezeti folyamatokba integrálva az adatvédelmi incidensek megfelelő kezelését is. Ezt a felkészülési szakaszban, a megfelelő eljárások, reagáló csapatok, erőforrások és kommunikációs panelek előzetes meghatározásával és kialakításával képes támogatni. Az incidenskezeléskor pedig a rendelkezésre álló eljárások képesek hatékonyan csökkenteni az incidensek okozta károkat és támogatni a törvényi megfelelést a határidők betartásával és a szükséges evidenciák összegyűjtésével.

c) Üzletmenet folytonosság

A GDPR rendelet meghatározza a személyes adatok kezelésével összefüggő folytonossági követelményeket is. Ehhez az üzletmenet-folytonossági irányítási rendszerszabvány (ISO 22301:2019) és az ahhoz kapcsolódó szabványok (ISO 223xx szabványok) adnak támogatást. Az üzletmenet-folytonosság alatt a szervezet azon képességét értjük, amely biztosítja, hogy a termékek és szolgáltatások szállítását/ teljesítését elfogadható időkereten belül, előre meghatározott kapacitással folytathassa bármely váratlanul bekövetkező incidens vagy zavar során.
Az ISO 22301:2019 szabvány[11] követelményeket határoz meg az üzletmenet-folytonossági irányítási rendszer (BCMS = Business Continuity Management Systems) bevezetésére, fenntartására és fejlesztésére. A BCMS célja tehát az, hogy védelmet nyújtson a zavarok ellen, csökkentse azok előfordulásának valószínűségét, felkészüljön a zavarokra, reagáljon rájuk és helyreállítsa a normál működést, amikor azok bekövetkeznek. Ezen keresztül a szervezet képes növelni rugalmasságát és ellenállóképeségét. A rendszer bevezetésével egy szervezet képes megfelelni az elvárt üzletmenet-folytonossági igényeknek és kötelezettségeknek. Fontos, hogy a szabványhoz kapcsolódik egy ISO 22313:2020-as szabvány, amely útmutatást ad az ISO 22301:2019 szabvány követelményeinek értelmezéséhez és használatához.

GDPR megfelelés támogatása

A GDPR 32. cikk (1) b) és c) bekezdés alapján elvárt, hogy az adatkezelők és adatfeldolgozók az adatkezeléssel összefüggő tevékenységeiket olyan rendszerekben végezzék, amelyek képesek megfelelni az elvárt folytonossági követelményeknek. Ennek kialakításában a szabvány alkalmazása oly módon képes segítséget nyújtani, hogy meghatározza egy ilyen rendszer kiépítésének folyamatát, követelményeit és eszközeit. A folytonossági tervek és eljárások pedig nagymértékben hozzájárulnak az adatkezelés biztonságának kialakításához. Az elszámoltathatóság igazolására egy jól kiépített üzletmenet-folytonossági rendszer több ponton is kínál evidenciát. Példák:

- Az üzleti hatáselemzés része a kritikus folyamatok erőforrásoknak és más (külső és belső) folyamatoknak való kitettség-vizsgálata is. Ebbe a vizsgálatba az adatkezelési folyamatokat bevonva vizsgálandók az adatfeldolgozók és szolgáltatásaik megfelelősége és folytonossága is, amelyek szintén a GDPR követelmények részét képezik.

- A BCMS részét képezi az a követelmény is, hogy a folytonossági tervek tartalmazzák a megfelelő kommunikációs terveket, amelyekben leírják, hogy ki, mikor, mit, kivel és hogyan kommunikáljon. Ez támogatja a GDPR által megfogalmazott, a zavarok (incidensek) bekövetkezésekor történő kommunikációra vonatkozó követelményeknek való megfelelést is.
- Noha a GDPR 32. cikkéből is következő adatmentés és visszaállítás követelménye más releváns szabványok segítségével is teljesíthető, azonban a mentési eljárás folytonossági követelményeknek történő megfelelése igazából csak egy dokumentált, rendszeresen tesztelt és karbantartott üzletmenet-folytonossági tervvel igazolható.
- A BCMS során alkalmazott üzleti hatáselemzés és a kritikus folyamatok kockázatfelmérései során feltárt információk támogathatják a megfelelő adatvédelmi hatásvizsgálat elkészítését.

d) Kockázatmenedzsment

A GDPR által elvárt megfelelő kockázatfelmérési és kezelési eljárások lefolytatásához két szabvány nyújt alapvető támogatást. Ezek az ISO 31000:2018 és az ISO/IEC 27005:2022 szabványok.

Az ISO 31000:2018 szabvány[12] a kockázatmenedzsment alapelveit és megvalósításának kereteit bemutató szabvány. Az iránymutatások bármely szervezetre és annak működési környezetére illeszthetőek, és bármely tevékenységre alkalmazhatóak, beleértve a döntéshozatal minden szintjét a szervezet teljes életciklusában. A szabvány definiálja a kockázatmenedzsment alapvető szakkifejezéseit és meghatározásukat, ezért sok egyéb szabvány hivatkozási alapja is. Fontos üzenete, hogy a kockázatmenedzsment értékteremtő folyamat.

Az ISO/IEC 27005:2022 szabvány[13] már az új ISO/IEC 27001:2022-es szabvány információbiztonsági kockázatainak felmérésére és kezelésre vonatkozó követelmények végrehajtásához nyújt iránymutatásokat. A szabvány teljes megértéséhez szükséges az ISO/IEC 27001:2022-es és ISO/IEC 27002:2022-es szabványokban leírt fogalmak, modellek, folyamatok és terminológiák ismerete. A szabvány fontos segédeszköz minden olyan szervezet számára, amely az információ biztonságát veszélyeztető kockázatokat megfelelő módon és egységesen kívánja kezelni.

A szabvány alkalmazza az ISO/IEC 31000-es szabvány magas szintű kockázatmenedzsment folyamatának terminológiáját és lépéseit, és részletesen kibontja azokat az információbiztonsági kockázatok vonatkozásában. Nem tartalmaz konkrét módszert az információbiztonsági kockázatok meghatározására, azaz nem nevesít egyetlen kockázatok felmérésével vagy kezelésével kapcsolatos konkrét megközelítést vagy módszertant sem (pl. CRAMM vagy FMEA). A kockázatelemzés folyamata megengedi mind a kvantitatív (számszerűsítő), mind kvalitatív (minősítő) módszerek alkalmazását, igazodva ezzel az adott elemzés bonyolultságához, időkeretéhez és egyéb erőforrás-ráfordítási lehetőségeihez. A szabvány „A melléklete" példákat mutat be a kockázatfelmérési folyamatot támogató technikákra.

GDPR megfelelés támogatása

Az adatkezelők és adatfeldolgozók, a szabványok iránymutatásait követve, azokat a szervezetükre és a konkrét tevékenységeikre szabva, képesek – a szervezeti szintű kockázatok felmérésének és kezelésének részeként, vagy önállóan – az információbiztonsági és az adatvédelmi kockázatok GDPR által elvárt szintű menedzselésére és dokumentálására. Az ISO/IEC 31000 az átfogó szervezeti és integrált kockázatmenedzsment folyamat kialakításában segít, ami egyben az adatvédelmi hatásvizsgálat fontos része is. A WP 29-es munkacsoport 248-as számú iránymutatása[5] is egyértelműen hivatkozik a szabvány kockázatfelmérési és kezelési eljárására.
Az ISO/IEC 27005:2022 szabvány a GDPR által nevesített és kockázatkezelést igénylő kötelezettségeiben nyújt konkrét megvalósítási támogatást. A GDPR 32. cikk (1) bekezdése alapján elvárás az adatkezelés biztonságának megteremtése, amelynek nélkülözhetetlen része egy megalapozott, kellően szakszerű és működő kockázatfelmérési és kockázatkezelési eljárás fenntartása.
A 33. cikk szerinti adatvédelmi incidensek megfelelő kezelésében és dokumentálásában szintén fontos szerepe van a kockázati szintek megfelelő értékelésének, amely alapján eldönthető, hogy milyen mér-

tékű kockázattal jár az incidens az érintettre nézve. Ennek tétje nem kisebb, mint hogy kell-e bejelentést tenni a felügyeleti hatóságok felé, illetve kell-e értesíteni az érintetteket.
A GDPR 35. cikk (7) d) pontjában megfogalmazott minimális tartalmi követelmények alapján az esetlegesen elvégzendő adatvédelmi hatásvizsgálat megfelelő lefolytatása és dokumentálása is megköveteli a kockázatok felmérését és kezelését célzó intézkedések bemutatását. Ehhez természetesen el kell végezni a kellően részletes kockázatfelmérést és meg kell tervezni a megfelelő kockázatkezelési intézkedéseket. Bár a megfelelő információbiztonsági kockázatfelmérés és kezelés csak része a hatásvizsgálatnak, de a 29-es munkacsoport WP 248 iránymutatása kiemeli, hogy annak „helytelen elvégzése" is jelentős közigazgatási bírsággal sújtható.

e) Adatvédelem

Az adatvédelemmel közvetlenül foglalkozó szabványok is megjelentek az elmúlt évtizedekben, amiből hármat érdemes megemlíteni a GDPR-ral kapcsolatban. Ezek az ISO 29100:2011, az ISO/IEC 27018:2019 és az ISO/IEC 27701:2019 szabványok.

Az ISO 29100:2011 szabvány[14] egy közös adatvédelmi terminológián alapuló adatvédelmi keretrendszert ír le. Meghatározza a személyes adatok feldolgozásának szereplőit és szerepüket, megvilágítja az adatvédelemmel kapcsolatos megfontolásokat, összekapcsolva azokat az informatikában használt adatvédelmi elvekkel. Olyan természetes személyekre és szervezetekre alkalmazható, akik részt vesznek az ICT rendszerek vagy szolgáltatások meghatározásában, beszerzésében, architektúrájában, tervezésében, fejlesztésében, tesztelésében, karbantartásában, adminisztrálásában és üzemeltetésében. Fontos, hogy a szabvány 2011 óta van érvényben, messze megelőzve a GDPR rendeletet. Időtállóan meghatározta azt a keretrendszert, amely lefedi a személyes adatkezelés alapvető fogalmait, elveit, szerepeit, összefüggéseit, a magánélet védelmének követelményeit és az adatvédelemmel kapcsolatos ellenőrzéseket. Ezzel támpontokat ad a rendszerfejlesztőknek a beépített és alapértelmezett adatvédelem megvalósításához.

Az ISO/IEC 27018:2019 szabvány[15] gyakorlati útmutatóként szolgál a személyes adatok védelmét szolgáló intézkedések végrehajtására nyilvános felhőalapú számítástechnikai környezetben. Az ISO/IEC 29100 szabványban foglalt adatvédelmi elvekkel összhangban meghatározza a vonatkozó, általánosan elfogadott intézkedési célokat és intézkedéseket. Az ISO/IEC 27002:2013 szabvány kiegészítéseként, a felhőszolgáltatások szolgáltatóinak információbiztonsági kockázati környezetével összefüggésben iránymutatásokat határoz meg, figyelembe véve a személyes adatok védelmére vonatkozó szabályozási követelményeket. Az iránymutatások a szolgáltatásokat igénybe vevő adatfeldolgozók számára is relevánsak lehetnek.

Az ISO/IEC 27701:2019 szabvány [16] az ISO/IEC 27001:2013 és az ISO/IEC 27002:2013 szabványok kiterjesztéseként további követelményeket határoz meg a személyes adatok (PII - Personally Identifiable Information) védelmét biztosító adatvédelmi irányítási rendszerhez, és útmutatást nyújt a PII-felelősök (adatkezelők) és a PII-feldolgozók (adatfeldolgozók) számára. A szabvány hat darab mellékletet tartalmaz, amelyek további segítséget nyújtanak a bevezetéshez és a megfelelés ellenőrzéséhez. Az „A" melléklet az adatkezelők, a „B" melléklet az adatfeldolgozók PIMS specifikus intézkedési céljait és intézkedéseit tartalmazza, összhangban az ISO/IEC 27001:2013 szabvány „A" mellékletének struktúrájával. A „C" melléklet az ISO/IEC 29100 szabványnak való megfeleltetés referencia táblázatát foglalja magába. A „D" melléklet a PIMS követelmények és a GDPR cikkek kapcsolatát képezi le. A „E" melléklet a PIMS kapcsolatát mutatja be az ISO/IEC 27018 és ISO/IEC 29151 szabványokkal. Az „F" melléklet pedig az információbiztonság fogalmának a magánélet védelmével történő kiterjesztésének leképezését tartalmazza.
Fontos megjegyezni, hogy az ISO 27001:2022-es szabvány megjelenése és annak jelentős strukturális változtatása miatt az ISO 27701-es szabvány felülvizsgálat alatt áll. A közétett DIS változat tartalomjegyzéke alapján azt már a ISO/IEC 27001:2022-es változat struktúrájához igazították.

GDPR megfelelés támogatása

A felsorolt szabványok mindegyike a személyes adatok megfelelő feldolgozásának és védelmének kérdéskörét támogatja különböző aspektusokból.

Természetesen a ISO/IEC 27701:2019 szabvány önmagában a GDPR megfelelés és tanúsítás támogatására készült, így az ISO/IEC 27001 kiegészítéseként az elszámoltathatóság tekintetében is garanciákat nyújt a megfelelő adatvédelem kialakításához.
A ISMS intézkedéseinek konkrét PIMS kiegészítései megfelelő mértékben és célzottan ügyelnek a jelentkező kockázatok megfelelő csökkentésére. Ilyen az adathordozók és a kommunikáció védelme, a humán faktor kockázatainak csökkentése, a megfelelő titkosítási-, mentési- és hozzáférési eljárások, az üzemeltetés biztonságának erősítése, és a rendszerfejlesztések esetén a figyelembe veendő biztonsági szempontok érvényesítése. Ide tartozik még a beszállítók felügyelete, az incidensek kezelése, a folytonossági- és megfelelési kritériumok meghatározása. A PIMS tartalmazza az adatfeldolgozókra és külön az adatkezelőkre vonatkozó extra követelményeket, amelyek az ISMS „A" mellékletét egészítik ki konkrét GDPR megfelelést szolgáló intézkedési célokkal és intézkedésekkel, egyben ellenőrzési listaként szolgálva a szervezeteknek.

4. AKKREDITÁCIÓ ÉS TANÚSÍTÁS

Magyarországon az ISO irányítási rendszereket tanúsító szervezetek akkreditációját a kijelölt Nemzeti Akkreditáló Hatóság (NAH) végzi. Ezt a tevékenységet a Nemzeti Akkreditálási Rendszer alapján, az akkreditálásról szóló jogszabályok és a nemzeti szabványként közzétett európai és nemzetközi szabványok figyelembevételével végzi. Az ISO irányítási rendszerek tanúsítóinak akkreditálása az ISO/IEC 17021 szabványok (megfelelőségértékelés) és az adott rendszerspecifikus, a szakkövetelményeket is tartalmazó szabványa szerint zajlik. A Információbiztonsági irányítási rendszerek tanúsítását végző szervezetek akkreditációja az ISO/IEC 27001 rendszerszabvány, valamint az ISO 17021-1 és ISO/IEC 27006 szabványok (aktuális magyar kiadásai) szerint történik.

Az ISO/IEC 27701:2019-es rendszer tanúsításához már kiadásra került az ISO/IEC 27006-2:2021 szabvány, amely az adatvédelmi információkezelő rendszerek auditálási szempontjait tartalmazza. Ezzel lehetőség nyílt az információbiztonsági irányítási rendszerek tanúsítását végző szervezetek ISO/IEC 27701-es követelményekkel kiegészített akkreditációjára.

Az ISO/IEC 27001:2022-es szabványhoz igazított új ISO/IEC 27701 szabvány kiadását követően ismét lehetővé válik majd a két rendszer együttes tanúsítása.

5. ÖSSZEFOGLALÁS

Látható tehát, hogy a ISO szabványok és a GDPR kapcsolata milyen sokrétű, és a szabványok milyen fontos szerepet töltenek be az akkreditáció, a tanúsítás, a megfelelőség és elszámoltathatóság megteremtésében. Ezt a kapcsolatot szemlélteti az 1. ábra is:

1. Ábra - ISO szabványok és a GDPR kapcsolata [1]

Az elszámoltathatóság elve a Magyarázat a GDPR-ról c. könyv [4] megfogalmazása alapján: „Az elszámoltathatóság lényegében az adatvédelmi megfelelőség érdekében tett intézkedések vállalását, ennek jegyében azok dokumentálását jelenti és azt a kívánalmat, hogy ezt a megfelelőséget az adatkezelő be tudja mutatni a külvilág felé."

A bemutatott szabványok alkalmazása lehetőséget biztosít az adatkezelőknek és adatfeldolgozóknak, hogy a kötelezettségeikből fakadó adatvédelmi megfelelőség érdekében tett intézkedéseket megtervezzék, bevezessék és eredményességüket folyamatosan kontrollálják és bizonyítsák. Ezek elsődlegesen a kockázatok feltárását és ezen keresztül az információ- és adatbiztonság megteremtését biztosító intézkedések meghatározását jelentik. Másodsorban a szabványok sok kritikus helyen követelnek meg dokumentált információkat, amelyek az elszámoltathatóság elvének való megfelelést evidenciákkal képesek igazolni.

Ezek közül is kiemelkedik az adatvédelmi szempontok érvényesítését és a GDPR megfelelést legnagyobb mértékben szolgáló ISO/IEC 27701:2019-es szabvány. Ennek bevezetése és tanúsíttatása az adatkezelések résztvevői számára komoly garanciákat biztosíthat. Ez az érintettek számára garantálhatja, hogy a GDPR előírásainak megfelelő adatkezelést egy folyamatosan fejlesztett, külső és belső kontroll alatt tartott rendszer keretein belül végzik, amely kiemelten érvényesíti a jogaikat és figyelembe veszi az őket ért kockázatokat. A hatóságok számára az adatkezelések megfelelőségére előzetes garancia lehet a szabvány szerinti működés, valamint az esetleges vizsgálatokat és eljárásokat nagy mértékben megkönnyíthetik a rendelkezésre álló dokumentált információk.

Az adatkezelők (és a szervezetek vezetői) garanciákat kaphatnak azzal, hogy egy jól átgondolt keretrendszerben, kellő szakértelemmel felépített és kompetens független átvizsgálásokkal értékelt környezetben végezhetik az adatkezelési tevékenységüket. Ezzel nagymértékben csökkentik a működési és jogi kockázataikat. Az adatfeldolgozók (és a szervezetek vezetői) az adatkezelőkhöz hasonlóan szintén garanciákat kaphatnak, hogy az adatfeldolgozói tevékenységük megfelel az elvárásoknak és megfelelő jogi kontextuson alapul. Nem utolsósorban, mind a tanúsítás, mind az irányítási rendszer bevezetése, az adatkezelési lánc résztvevői számára komoly szankciócsökkentő bizonyítéka lehet annak, hogy a szervezet megfelelő szervezési és technikai intézkedéseket tett az adatkezelés biztonsága és jogi megfelelősége érdekében.

FELHASZNÁLT FORRÁSOK

[1] Horváth István (2021): ISO szabványok a GDPR szolgálatában. Adatbiztonsági és adatvédelmi jogi szakokleveles szakember képzés szakdolgozat. ELTE Állam- és Jogtudományi Kar, Jogi Továbbképző Intézet, Budapest.

[2] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 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 (általános adatvédelmi rendelet) (2016)

[3] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, URL: https://net.jogtar.hu/jogszabaly?docid=a1100112.tv (letöltés: 2019.10.10)

[4] Péterfalvi Attila, Révész Balázs, Buzás Péter (2018): Magyarázat a GDPR-ról. Budapest, Wolters Kluwer Hungary Kft.

[5] A 29. cikk alapján létrehozott adatvédelmi munkacsoport (2017). WP 248-as iránymutatás. Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e. (Utolsó letöltés: 2021. 09. 06.)

[6] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements; International Organization for Standardization (2022).

[7] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls; International Organization for Standardization. (2022).

[8] ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management; International Organization for Standardization. (2016).

[9] ISO/IEC 27035-2:2016 Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response; International Organization for Standardization. (2016).

[10] ISO/IEC 27035-3:2020 Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations; International Organization for Standardization. (2020).

[11] ISO/IEC 22301:2019 Security and resilience — Business continuity management systems — Requirements; International Organization for Standardization. (2019).

[12] ISO/IEC 31000:2018 Risk management — Guidelines; International Organization for Standardization. (2018).

[13] ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks; International Organization for Standardization. (2022).

[14] ISO/IEC 29100:2011 Information technology —

Security techniques — Privacy framework; International Organization for Standardization. (2011).
[15] ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors; International Organization for Standardization. (2019).
[16] ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines; International Organization for Standardization. (2018).

Horváth István

Horváth István 2006 óta az immunIT Információbiztonsági Tanácsadó Kft. tulajdonosa és ügyvezetője. Az INFOBIZ Kft. tanácsadói csapatának oszlopos tagja. Mérnök-informatikus és adatvédelmi jogi szakember, valamint az EOQ MNB által regisztrált információbiztonsági rendszermenedzser és auditor. Komoly szerepet töltött be az első magyarországi digitális cafeteria kártya és elszámoló rendszer tervezésében, fejlesztésében és üzemeltetésében. Több, mint tizenöt éve foglalkozik az informatika különböző területével és tanácsadóként, oktatóként és auditorként vesz részt irányítási rendszerek kiépítésében. Több akkreditált tanúsító szervezetnél számos irányítási rendszer vezető auditora.

Dr.-univ. Horváth Zsolt, a műszaki tudomány kandidátusa

Az INFOBIZ Kft. tulajdonosa és ügyvezetője 2006 óta. EOQ MNB által regisztrált minőségirányítási és információbiztonsági rendszermenedzser és auditor. Tíz évig látta el a SIEMENS magyarországi szoftverházának a minőségirányítási igazgatói feladatait. Több, mint húsz éve dolgozik a minőségirányítás és az információbiztonsági irányítás területén, több akkreditált tanúsító szervezet vezető auditoraként, valamint tanácsadóként és szakmai oktatóként. Számos szakmai konferencián elhangzott előadás és megjelent publikáció szerzője.

Tóth Zoltán

Az INFOBIZ Kft. tanácsadói csapatának tagja. Gazdaság informatikai szakon végzett közgazdász, mérlegképes könyvelő, információbiztonsági menedzser. 15 éve különböző multinacionális cégeknél töltött be pénzügyi, majd vezető elemzői pozíciókat. Az elmúlt 3 évben adatvédelemmel is foglalkozik, illetve tanácsadóként vesz részt irányítási rendszerek (ISO 27001,TISAX) kiépítésében.