IT biztonság
2020/2021 tanév ősz

Bemutatkozás

Giesz István
- okl. Gépészmérnök, okl. Rendszerszervező, Információbiztonsági menedzser, ISO27k1IA&LA
- KÖFÉM/ALCOA/ARCONIC, BUSZESZ, HUNGRANA, Csemege Julius_Meinl, SPAR, TESCO - IT vezető/ügyvezető
- GIRO Zrt – vezérigazgató helyettes
- Progadat - ügyvezető

Agenda

- Irányítási rendszerek
- Az információbiztonsággal kapcsolatos jogszabályok
- Állami és önkormányzati szervek információbiztonsága (2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról – Ibtv.)
- Az Európai Parlament és a Tanács 2016/679 rendelete (GDPR).

… kezdjük az élettel …

- Kis magyar szoftverfejlesztő (Fejlesztő) cég bérbe adná (SaaS) saját fejlesztésű rendszerét egy nagy magyarországi multi (Multi) közüzemi szolgáltatónak.
- Multi-ra legalább az alábbi jogszabályok vonatkoznak:
  - Infotv. (Információbiztonsági törvény)
  - GDPR
  - Ibtv. (Informatikai biztonsági törvény)
  - Lrtv (Létfontosságú rendszerek törvény)
- Azaz a Multi IT rendszereinek zártnak és megbízhatónak kell lennie, azaz működtetnie kell Információbiztonsági Irányítási Rendszert (IBIR).
- Az Ibtv. kötelezi a Multi-t, hogy a beszállítóktól (Fejlesztő) is követelje meg IBIR működtetését.
- <InfoSec_Suppl.docx>

Mi az Irányítási Rendszer (IR)?

Az az eszköz, amivel egy szervezet **irányítja** üzleti tevékenységének **egymással összefüggő részeit céljainak elérése** érdekében.

A célok lehetnek: a tulajdonosi érdek, termékek vagy szolgáltatások **minőség**e, az üzemeltetési **hatékonyság**, a környezet védelem **teljesítmény**e, a munkahelyi **egészség**, **biztonság** és még sok mást.

Az irányítási rendszer komplexitása a szervezettől függ, kisebb cégeknél ez **erős vezetői irányítást**, míg nagy, kiterjedt, bonyolult vállalkozásoknál ez **részletes szabályozási rendszert** jelent.

IR jellemzői

- Vállalati stratégia (politika és célok)
- IR témájának megfelelő szempontrendszer beintegrálása, figyelése, előtérbe hozása
- Vállalat működése tervezett, szabályozott, kontrollált
- Tevékenységekre – folyamatokba rendezve – dokumentált végrehajtási utasítások
- Erőforrások figyelése, kezelése, biztosítása
- Hibák figyelése, javítás, tanulás
- Folyamatos javítás, fejlesztés

Integrált Irányítási Rendszer (IIR)

Olyan rendszer, amely **kettő vagy több** Irányítási Rendszer követelményeit **összevontan** tartalmazza.

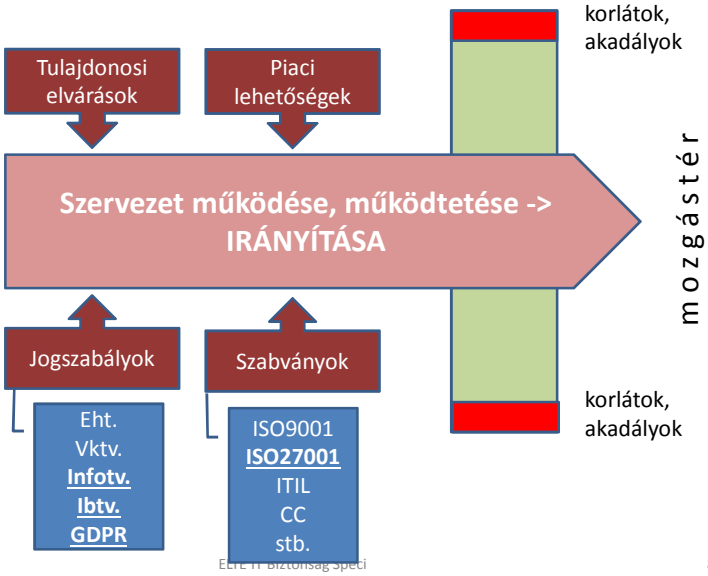
Előnyei:

- gyors, hatékony döntési mechanizmus
- kevesebb papírmunka
- dokumentált
- kontrolált
- erőforrások takaríthatók meg
- PDCA (Plan, Do, Act, Check)
- jobb kommunikáció

Hátrányok:

- hosszú, fáradságos tervezés
- esetleg a már meglévő, gyenge rendszerekre építik rá

Szervezet működési környezete



ISO járatos IIR

ISO 9001:2015 Quality management systems. Requirements
MSZ EN ISO 9001:2015 Minőségirányítási rendszerek. Követelmények

ISO 14001:2015 Environmental management systems. Requirements with guidance for use
MSZ EN ISO 14001:2015 Környezetközpontú irányítási rendszerek. Követelmények alkalmazási útmutatóval

ISO 45001:2018 Occupational health and safety management systems. Requirements.
MSZ EN ISO 45001:2018 A munkahelyi egészségvédelem és biztonság irányítási rendszere (MEBIR). Követelmények.

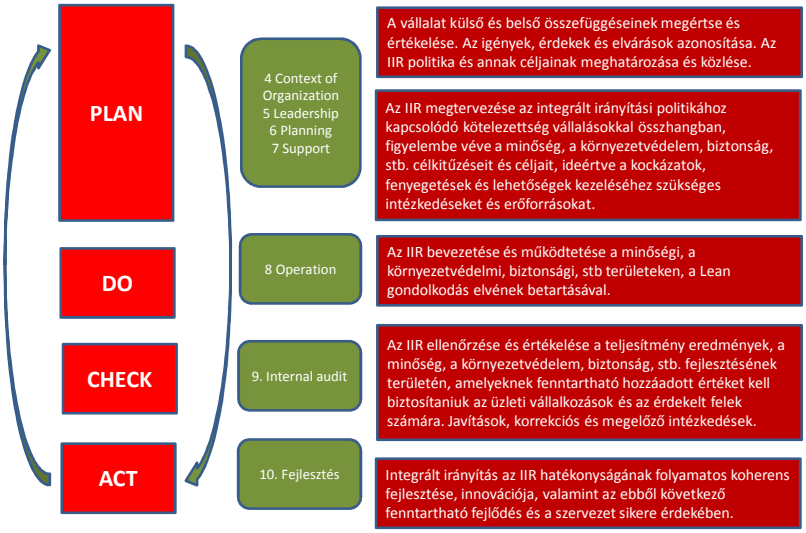
ISO 50001:2018 Energy management systems. Requirements with guidance for use.
MSZ EN ISO 50001:2019 Energiagazdálkodási irányítási rendszerek. Követelmények alkalmazási útmutatóval.

ISO/IEC 27001:2013 Information technology. Security techniques. Information security management systems. Requirements
MSZ ISO/IEC 27001: 2014 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények

ISO - International Organization for Standardization
IEC - International Organization for Standardization

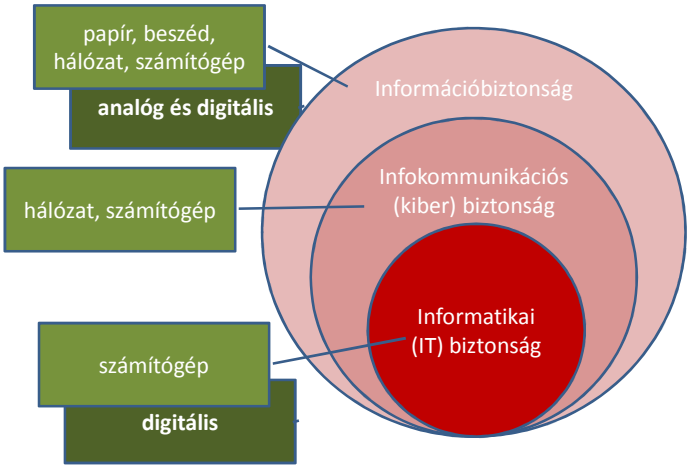
2020.09.14. ELTE IT Biztonság Speci 9

IIR fejlődési modell

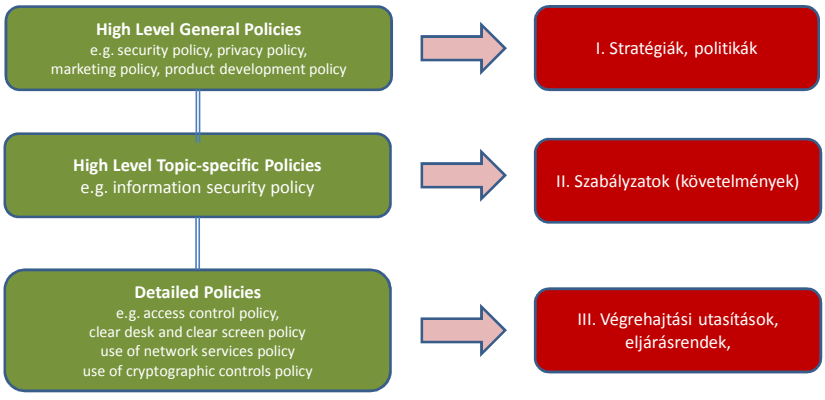


2020.09.14. ELTE IT Biztonság Speci 10

A biztonság különböző szintjei



IR – Szabályozási struktúra



Adatkezelés

”a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés”

(EU) 2016/679 RENDELETE 4. cikk 2.

Jogszabályok

Előzmények …

INFORMATIKAI TÁRCAKÖZI BIZOTTSÁG (1994-től)

ITB 8. számú ajánlása: **Az informatikai biztonság módszertani kézikönyve**

ITB 12. számú ajánlása: **Az informatikai rendszerek biztonsági követelményeiről**

ITB 16. számú ajánlás: **A Common Criteria (CC), az informatikai termékek és rendszerek biztonsági értékelésének módszertanáról.**

Előzmények …

KÖZIGAZGATÁSI INFORMATIKAI BIZOTTSÁG (2008)

25. számú ajánlása: **Magyar Informatikai Biztonsági Ajánlások (MIBA)**
<https://regi.ugyintezes.magyarorszag.hu/dokumentumok>

- 25/1 Magyar Informatikai Biztonság Irányítási Keretrendszer (MIBIK)
  - Informatikai Biztonság Irányítási Rendszer (IBIR)
  - Informatikai Biztonság Irányítási Követelmények (IBIK)
  - Az Informatikai Biztonság Irányításának Vizsgálata (IBIV)
- 25/2 Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS)
- 25/3 Informatikai Biztonsági Iránymutató Kis Szervezeteknek (IBIX)

Általános jogszabályok

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről (Lrtv.)

65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

Ágazati jogszabályok példák

42/2015. (III. 12.) Korm. rendelet a pénzügyi intézmények, a biztosítók és a viszont biztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről

A Magyar Nemzeti Bank 8/2020. (VI.22.) számú ajánlása az informatikai rendszer védelméről

Ágazati jogszabályok

2014. évi XLI. törvény egyes közszolgáltatási tárgyú törvények módosításáról, mint néhány példa

- 2003. évi C. az elektronikus hírközlésről szóló törvény
- 2007. évi LXXXVI. a villamos energiáról szóló törvény
- 2008. évi XL. a földgázellátásról szóló törvény
- 2011. évi CCIX. a víziközmű-szolgáltatásról szóló törvény

„Számla kiállítására csak olyan informatikai rendszer felhasználásával kerülhet sor, amely biztosítja **a díjak hibátlan kiszámítását végző rendszerelemek zártságát, és megakadályozza a számlázási rendszerhez történő jogosulatlan hozzáférést, valamint a számlázási információk észrevétlen módosítását**. A számlázási rendszernek továbbá meg kell felelnie az általános információbiztonsági zártsági követelményeknek is. Ennek érdekében a szolgáltatónak **adminisztratív, fizikai és logikai intézkedésekkel** biztosítani kell „az általános információbiztonsági zártsági követelmények teljesülését.”

Ibtv. származtatása

NIST: National Institute of Standards and Technology

NIST Special Publication 800 53 Revision 4:
Security and Privacy Controls for Federal Information Systems and Organizations

<https://nvd.nist.gov/800-53/Rev4#>

Ibtv általános rész

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

Tárgyi hatály:

központi és helyi közigazgatás, önállóan megnevezett szervek, ezek adatfeldolgozói, állami nyilvántartások kezelői, létfontosságú rendszerelemek (és akik ezekkel szerződés keretében adatcserét folytatnak)

Felügyelő hatósága:

a Nemzeti Elektronikus Információvédelmi Hatóság, (kivéve polgári nemzetbiztonsági rendszerek, honvédelmi célú rendszerek, kritikus infrastruktúrák esetében)

Adatkezelés helye: Magyarország, esetleg EU/EGK országok

Osztályok, szintek

Biztonsági szintek (1-5)

A végzett tevékenység szerint, saját kockázatelemzés alapján az infokommunikációs rendszerek besorolása

Biztonsági osztályok (1-5)

A követelményeknek való megfelelés állapota a szervezetnél (eltérés felfelé-lefelé a hatóság előzetes engedélyével lehetséges)

- Kétéves tolerancia
- Felülvizsgálati kötelezettség
- Elektronikus információs rendszer biztonságáért felelős személy kinevezése, alkalmazása
- Kijelölt központosított informatikai és elektronikus hírközlési szolgáltató, illetve központi adatkezelő és adatfeldolgozó szolgáltató kötelező igénybe vétele

További eljárásrend

271/2018. (XII. 20.) Korm. rendelet

az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól

187/2015. (VII. 13.) Korm. rendelet

az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat-és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

26/2013. (X. 21.) KIM rendelet

az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról

Biztonsági felügyelet

Kormányzati eseménykezelő központ és az eseménykezelő központok:

CERT/CSIRT funkciókat ellátó szervezet
(központi: NBSZ állományában, ágazati: hatósága mellett)
<https://nbsz.gov.hu/tevekenyseg-mukodes>

NEIH + CERT = Nemzeti Kibervédelmi Intézet
<https://nki.gov.hu/hatosag/tartalom/hataskor-ibtv/>

Nemzeti Kiberbiztonsági Koordinációs Tanács:

Egyeztető, véleményező feladatkör

Kiberkoordinátor: a Tanácsot támogatja, „kiber ombudsman”

További eljárásrend

41/2015. (VII. 15.) BM rendelet (Vhr.)

az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

Végrehajtási rendelet

Osztályba sorolás és szintek meghatározásának követelményei

1. melléklet a 41/2015. (VII. 15.) BM rendelethez:

Az elektronikus információs rendszerek biztonsági osztályba sorolása - *káralapú meghatározás* -

2. melléklet:

Az elektronikus információs rendszerrel rendelkező szervezetek vagy szervezeti egységek biztonsági szintbe sorolása - *megfelelés képességi követelményeknek* -

3. melléklet:

A 4. melléklet „3. Védelmi intézkedés katalógus” alcímben meghatározott védelmi intézkedések besorolásának táblázatai

4. melléklet:

AZ ADMINISZTRATÍV, FIZIKAI ÉS LOGIKAI BIZTONSÁGI KÖVETELMÉNYEK

Végrehajtási rendelet

Felosztása:

Öt szint
Bizalmasság, sértetlenség, rendelkezésre állás
Adminisztratív, fizikai, logikai intézkedések
<https://net.jogtar.hu/jogszabaly?docid=a1500041.bm>

Osztályba sorolás és védelmi intézkedés (OVI) űrlap

Szintbe sorolás és védelmi intézkedés (SZVI) űrlap

Útmutatók az űrlapokhoz

Előnyök

- Jogszabályba foglalt kötelezettség, hatósági felügyelettel
- Pontosan meghatározott biztonsági osztály és szint kategóriák
- Teljeskörű, erőteljes követelménylista
- Excel makrós űrlapokkal támogatott bejelentés, kiértékelés
- Jól kiszámítható megfelelési eredmények
- Cselekvési terv beépíthető (kötelező ígéretek)
- Elvileg a szerződött partnerekkel szemben is érvényesíthető
- Vannak szakmailag kompetens ágazati hatóságok
- Ingyenes bárki számára (mint IBIR)
- Ott van mögötte az NIST
- Büntethető

Hátrányok

- Jogszabállyal nem lehet folyamatosan követni a technológiai fejlődést
- A követelménylista abszolút rugalmatlan, helyettesítő intézkedéseket a hatóság egyenként hagyhat jóvá, szinte nincs is mozgástér
- 1. kategória gyakorlatilag nem létezik,
  5. kategória gyakorlatilag nem teljesíthető
- Meghatározott határidők a megfelelés kialakítására, ami függ a szervezetet felügyelő központi szervtől (minisztériumtól) is, ugyanakkor többéves cselekvési tervet kell létrehozni
- Új létesítések esetén nincs türelmi idő, azonnali megfelelés kell
- Sok az ügyfele a hatóságnak, nem megy helyszínre, nincsenek állásfoglalásai
- A hatály nem egyértelmű (államigazgatási szervek -> költségvetési szervek)

GDPR alapok

Jogi környezet

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.)

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

(General Data Protection Regulation / GDPR / Általános Adatvédelmi Rendelet)

(EGT-vonatkozású szöveg)

Jogi környezet

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.)

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)

2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól (E-ügyintézési tv.)

Alapelvek

„A belső piac megfelelő működése érdekében a személyes adatok Unión belüli szabad áramlását a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmével összefüggő okokból nem szabad korlátozni vagy megtiltani.”

= Piac elsődlegessége a személy érdekeivel szemben

„…e rendelet alkalmazása során az uniós intézményeket és szerveket, és a tagállamokat és azok felügyeleti hatóságait ösztönözni kell, hogy vegyék figyelembe a mikro-, kis-és középvállalkozások sajátos szükségleteit.”

= Jogalkalmazókra bízza a KKV-k problémáját

Alapelvek …

Európában legyenek egységes adatvédelmi szabályok, de hagyjunk helyet a nemzeti sajátosságoknak is!

„Ha e rendelet úgy rendelkezik, hogy a benne foglalt szabályokat tagállami jog által pontosítani, illetve korlátozni lehet, a tagállamok e rendelet egyes elemeit beépíthetik a nemzeti jogukba, …”

„… a rendelet nem zárja ki olyan tagállami jog elfogadását, amely meghatározza a különleges adatkezelési helyzetek körülményeit, ezen belül pontosabban megállapítja, hogy milyen feltételek mellett jogszerű a személyes adatok kezelése.”

Alapelvek …

Európában legyenek egységes adatvédelmi szabályok, de hagyjunk méltányos helyet a nemzeti sajátosságoknak is!

Uniós jog hatályán kívül eső területek:

- Nemzetbiztonság, külügy
- Igazságszolgáltatás, egyházak adatkezelése mint sajátos kivétel
- Anonimizált adatok: statisztika, kutatás
- Természetes személy által kizárólag személyes vagy otthoni tevékenység keretében végzett adatkezelés (nem üzleti célok)
- Elhunyt személyek adatai

Alapelvek …

Tagállamok további korlátozási lehetőségei!

- Honvédelem, közbiztonság
- Közérdekű célkitűzések: monetáris, költségvetési, adózási okok, népegészségügy, szociális biztonság
- Különleges adatok
- Dolgozókkal szembeni etikai eljárások
- Érintett személy vagy mások szabadságainak védelme
- Polgári jogi követelések érvényesítése

Érintett jogai

Természetes személy, mint érintett jogai:

- Átlátható tájékoztatáshoz való jog
- Adathozzáférés joga
- Helyesbítéshez, törléshez való jog
- Az adatkezelés korlátozásához való jog
- Az értesülés joga az előbbiekhez
- Adathordozhatósághoz való jog
- Tiltakozás joga

Adatkezelő feladatai (24. cikk)

(1) Az adatkezelő az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével **megfelelő technikai és szervezési intézkedéseket hajt végre annak biztosítása és BIZONYÍTÁSA céljából,**

hogy a személyes adatok kezelése e rendelettel összhangban történik. Ezeket az intézkedéseket az adatkezelő felülvizsgálja és szükség esetén naprakésszé teszi.

Adatkezelő feladatai

Az adatkezelő tevékenységének része különösen:

- Adatok nyilvántartása
- Adat kezelés biztonságának kialakítása
- Adatvédelmi incidens bejelentése hatósághoz
- Érintettek értesítése incidens esetén
- Hatásvizsgálat
- Előzetes konzultáció hatósággal

Adatkezelési nyilvántartás

Elkészítése:

- Ahány céllal történik adatkezelés, annyi nyilatkozat/tétel/bejegyzés kell...
- Példa: honlapnál fel kell mérni az adatkezelési eseteket, amik előfordulhatnak, úgymint:
  - regisztráció, megrendelés, hírlevél feliratkozás
  - kapcsolatfelvétel (akár űrlapon, akár e-mailben), bármely marketing popup, ahol személyes adatot gyűjtünk (pl. e-mail címért kupon felajánlása, stb.)
  - működési és/vagy marketing sütik telepítése (IP-cím megjegyzése) az oldal látogatásakor
  - nyereményjáték
  - garanciális panaszok, fogyasztóvédelmi panaszok kezelése

… és a tartalom

A nyilvántartásnak tartalmaznia kell:

- A vállalkozás nevét és elérhetőségi adatait
- Az adatfeldolgozás indoklását és az adatkezelés célját
- Az adatalany- és személyesadat-kategóriák ismertetését, tehát az érintettek és a kezelt adatok körét
- Annak tényét, ha történik profilalkotás az érintett kapcsán
- Az adatokat megkapó szervezetek típusait
- Az esetleges adattovábbításra vonatkozó információkat, beleértve a nemzetközi adattovábbításra vonatkozó információkat is
- Felelős személy
- Az adatkezelési műveletek jogalapjait
- Az adatok tárolási/elérési helye
- A kezelt személyes adatok időtartama és/vagy törlésének időpontját, amennyiben az ismert
- Érintett folyamatok, szabályzatok
- Továbbítás harmadik félnek
- Védelmi kontrollok

Jogalapok …

Az adatkezelés jogszerűségéhez - a GDPR 6. cikke alapján - legalább az alábbi jogalapok egyikének fennállása szükséges:

a) érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;

b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;

c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;

d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;

e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;

f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Jogalapok …

Az adatkezelés jogszerűségéhez - a GDPR 6. cikke alapján - legalább az alábbi jogalapok egyikének fennállása szükséges:

a) érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;

b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;

c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;

d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;

e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;

f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.

Infotv. módosítása

- Nemzeti hatóság kijelölése
- GDPR által nem szabályozott kérdésekben nemzeti intézkedés meghozatala
- GDPR tartalmában engedélyezett nemzeti pontosítások, szigorítások, korlátozások
- Bűnügyi irányelv kötelező jogharmonizációja
- GDPR hatálya alá nem tartozó kérdések szabályozása az uniós rendelet irányvonala mentén

Mai problémák

- Elmúlt 2018. május 25.
- Eltérő értelmezések vannak köztudatban.
- Elfogadták Infotv. módosítását, vannak értelmezési problémák.
- Hiányoznak egyes hatósági listák, állásfoglalások, értelmezések (EU és tagállami szinten is).
- Tanúsító szervek, metódusok, magatartási kódexek, velük kapcsolatos követelmények sem léteznek.
- Nem lehet megmondani a tutit, így nincs tévedhetetlen szakember a területen.

Hatósági feladatok

GDPR szerinti nemzeti hatóságként lép fel a NAIH

- Alkalmazza az Európai Adatvédelmi Testület állásfoglalásait, iránymutatásait, saját hatáskörben állásfoglalásokat, iránymutatásokat tesz közzé.
- Tanúsítással és magatartási kódexekkel kapcsolatos követelményeket dolgozz ki.
- Konzultációs lehetőséget biztosít.
- Incidens-és panaszbejelentéseket fogad.
- Hatósági ellenőrzést, vizsgálatot végez.

Hatósági feladatok

Infotv. szerinti hatóságként tevékenykedik

- Az Infotv-ben beépített Bűnügyi Irányelv előírásainak betartását felügyeli.
- Felügyeli a nemzeti hatáskörbe utalt rendeleti előírások megvalósulását.
- Felügyeli az ágazati törvények által szabályozott, a személyes adatok kezelésére vonatkozó előírások megvalósulását.
- Továbbra is ellátja az Infotv-ben rögzített egyéb feladatait.

NAIH aktusok

Hatósági vizsgálatban

- Tájékoztatást kér
- Adatvédelmi auditot folytat
- Tanúsítványokat felülvizsgál
- Minden érintett helyiséghez, eszközhöz, adathoz hozzáfér
- Feltételezett jogsértésekről tájékoztatja az adatkezelőt/adatfeldolgozót

NAIH aktusok

Korrekciós hatáskörben

- Figyelmeztet, elmarasztal, utasít
- Elrendel helyreigazítást, tájékoztatást
- Adatkezelést korlátoz, megtilt, adatáramlást
- megakadályoz
- Tanúsítványt visszavon/visszavonat
- Közigazgatási bírságot szab ki

NAIH aktusok

Engedélyezés, tanácsadás hatáskörben

- Konzultál és tanácsot ad az adatkezelőnek
- Véleményt alkot és nyilvánosságra hoz
- Adatkezelést engedélyez, ha szükséges
- Tanúsítványt visszavon/visszavonat
- Tanúsítási rendszert, magatartási kódexet hagy jóvá
- Részt vesz tanúsító akkreditálásában

<https://naih.hu>

Adatkezelő feladatai

Cél: jogszerűség + információbiztonság + folyamatalapú működés együttes biztosítása

- Komplex helyzetfelmérés
- Adatkezelések tisztítása
- Folyamatok definiálása, hiányzó funkciók és kontrollok meghatározása, beépítése (fejlesztés)
- Szabályzatok, nyilvántartások összeállítása,
- módosítása, szerződések pontosítása
- Oktatás, érintettek tájékoztatása

Elegendő biztonság

- Bizalmasság, sértetlenség, rendelkezésre állás, ellenálló képesség biztosítása
- Követhetőség, elszámoltathatóság az adatkezelési folyamatokban (pl. törlés, zárolás)
- Rendszeres, dokumentált belső ellenőrzés/audit/kockázatkezelés
- Személyes adatok álnevesítése, titkosítása
- Intézkedések, korlátozások egyes adatkezelési eseményekre
- Megfelelés igazolásához felhasználható:
  - magatartási kódexhez való csatlakozás (nem közhatalmi szervek esetén), ha lesz ilyen
  - tanúsítási mechanizmushoz történt csatlakozás, ha lesz

Megoldás, alapszint

Fizikai hozzáférés-védelem
Adminisztratív szabályok (szabályzat)
Logikai védelem

- Felhasználóazonosítás, jogosultságkezelés
- Titkosítás
- Anonimizálás
- Adatszivárgás megelőzése
- DRP/Mentés
- Incidenskezelés
- Adatkezelési aktusok támogatása
- Naplózás

Sokat segíthet

2013. évi L. tv. (Ibtv.) szerinti megfelelés

Minőségirányítási rendszerek, információbiztonsági szabványok bevezetése, elsősorban ISO 2700x, ISO 29100, NIST 800-53, ISO 9001

SAP vállalati folyamatirányítás

A dokumentumkészletet lefedő iratkezelési rendszer

Irányítási rendszer, azon belül a Compliance működése

Jó kapcsolat tanácsadó cégekkel, mint partnerekkel

Olvasnivalók

Célszerű a hivatkozott honlapokon körülnézni és a dokumentumokba belenézni.