GDPR tanácsadói szemüveggel

Dr. Horváth Zsolt

Összefoglalás

A személyes adatok kezelésére vonatkozó új jogszabály, a GDPR egy részletekbe menő szigorú követelményrendszer a gazdálkodó szervezetek számára. A GDPR azonban csak a követelményeket írja elő, azok megvalósításának módjára nem ad útmutatást. Ebben nyújthatnak hasznos segítséget az ISO szerinti irányítási rendszerek, hiszen azok a kívánt követelményrendszereknek a vállalati működésbe való beillesztésére adnak szabályozott keretrendszert. A cikk bemutatja, hogy a minőségirányítási és az információbiztonsági irányítási rendszerek milyen módon tudnak segítséget nyújtani a GDPR követelményeknek való megfelelésben.

Bevezetés

Minőségügyi és információbiztonsági auditori, illetve tanácsadói munkám során egyik állandó feladat annak vizsgálata, hogy az adott irányítási rendszer hogyan tart egyensúlyt az ISO szabvány általi és az egyéb külső és belső követelmények teljesítése között. A külső követelmények között első helyen szerepelnek a vonatkozó jogszabályi kötelezettségek, amelyek egyike a személyes adatok kezelésének jogi szabályozása. Ezt Európában egységesen az Európai Parlament és Tanács 2016/679. számú, a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról szóló rendelete, azaz röviden az Általános Adatvédelmi Rendelet (a GDPR[1]) határozza meg. A személyes adatok kezelését továbbá Magyarországon még a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (röviden az infotörvény) szabályozza, amelyet a 2018. július 26-i módosítással a GDPR követelményeihez igazítottak.

Személyes adatokat minden gazdasági szervezet kezel, hiszen természetes személyek végzik a tevékenységeket a szervezeten belül és kívül is, akik lehetnek maguk a tulajdonosok, a szervezet alkalmazottai, alvállalkozói, beszállítói, vevői, ügyfelei, egyéb partnerei vagy az azokat képviselő személyek. Ők mind létező személyek, akik valamilyen tevékenységet látnak el, és ez a szervezet működésében mind valamilyen módon rögzített és dokumentált.

A személyes adatok kezelésére vonatkozó követelmények így minden gazdálkodó szervezet számára egyaránt relevánsak és kötelezően betartandók. A GDPR-nak való megfelelésre felkészülési határideje az Európai Unión belül egységesen 2018. május 25-én lejárt, és a számonkérése elkezdődött. Ilyen körülmények között a gazdálkodó szervezetek számára az irányítási rendszereik során ez mindenképp a kötelezően betartandó követelmények részét képezi.

A továbbiakban a GDPR-nak való megfelelés és az irányítási rendszerek, elsősorban a minőségirányítási és infor-

[1] GDPR az Általános Adatvédelmi Rendelet angol nyelvű eredetijének, a General Data Protection Regulation-nak a rövidítése

mációbiztonsági irányítási rendszerek kapcsolatát vizsgáltam, valamint ezek kezdeti alkalmazásának eddigi gyakorlatát és tapasztalatait elemeztem.

GDPR az 'ISO követelmények'-ben

Az ISO 9001:2015 (MSZ EN ISO 9001:2015) szabvány szerinti minőségirányítási rendszer megléte azt is jelenti, hogy az azt alkalmazó vállalat képes a termékeivel és/vagy szolgáltatásaival a vevői elégedettség növelésére, valamint működésével a jogszabályi és egyéb szabályozó követelményeknek való folyamatos megfelelésre.

A minőségirányítási rendszerek kiépítésének több követelménye is szoros összefüggésbe hozható a személyes adatok kezelésének jogszabályi követelményei teljesítésével.

- A 4.2. Az érdekelt felek szükségleteinek és elvárásainak megértése c. fejezet követelménye arról szól, hogy a gazdálkodó szervezet a minőségirányítási rendszer kiépítése (illetve működésének újratervezése) előtt határozza meg a szervezet működésével kapcsolatba hozható érdekelt feleit és azok elvárásait. Ezek után a minőségirányítási rendszer működését alakítsa ki úgy, hogy az alapján a szervezet a működése során követelményként teljesítse „a lényeges érdekelt felek lényeges elvárásait".
- A szabvány 7.5. Dokumentált információk c. fejezete követelményeket határoz meg az összes, a folyamatok működéséhez és igazolásához szükséges információ életciklusának és biztonságának a kezelésére. A szabvány a 7.5.3. A dokumentált információk felügyelete c. fejezetben a dokumentált információk használatra történő elérhetőségének és alkalmasságának, valamint a bizalmasságának, sértetlenségének és helytelen használat elkerülésének követelményeit írja elő, a dokumentált információk kezelésének teljes életciklusa alatt. Ez tulajdonképpen nem más, mint az információ biztonságának definíciója: az információ bizalmassága, sértetlensége és rendelkezésre állása.
- Fontos továbbá, hogy az ezek érdekében bevezetett intézkedések mértéke kockázatarányos legyen, azaz álljanak arányban az intézkedés bevezetésének elkerülése esetén lehetséges kár kockázatának mértékével. A szabvány 6.1. A kockázatokkal és lehetőségekkel kapcsolatos tevékenységek c. fejezete éppen erre fogalmaz meg követelményeket. Azaz a gazdálkodó szervezeteknek foglalkozniuk kell azokkal a kockázatokkal, amelyek – többek közt – „a lényeges érdekelt felek lényeges követelményeinek" teljesítése vagy nem-teljesítése következtében felmerülhetnek, vagy amelyek során a szervezet működésében nem-kívánt hatások léphetnek fel. Ezekhez meg kell tervezni és be kell vezetni a megfelelő kockázatcsökkentő intézkedéseket, értelemszerűen a kockázatok mértékével arányosan.

Hol kapcsolódnak ezen elvárások teljesítése a GDPR követelményeihez? A gazdálkodó szervezetekre vonatkozó, általános érvényű törvények és jogszabályok mindenképp „a lényeges érdekelt felek lényeges követelményeinek" minősülnek. A személyes adatok kezelésére vonatkozó EU rendelet (GDPR) és a magyar infotörvény mindenképpen teljesítendő követelmény minden gazdálkodó szervezet számára. A vállalatok folyamataiban szereplő adatok egy része a résztvevő illetve egyéb módon érintett természetes személyekre vonatkozik, tehát személyes adat. Így a folyamatok működése és igazolása során ezek mind a

dokumentált információk részét képezik, tehát kiterjednek rájuk az adatok kezelése életciklusának szabályozási valamint biztonsági követelményei. Ezeknek figyelembe kell venni a GDPR által meghatározott követelményeket, azaz a személyes adatok adatkezelési alapelveit és egyéb kritériumait, valamint a GDPR által meghatározott adatbiztonsági elvárásokat. A GDPR is előírja az adatkezelés és adatbiztonság megvalósítása során a kockázatarányos intézkedések bevezetését, ami itt a szabvány 6.1. pontjában meghatározott alapelvekkel áll összhangban.

Az ISO/IEC 27001:2013 (MSZ ISO/IEC 27001:2014) szabvány szerinti információbiztonsági irányítási rendszer célja éppen az, hogy az azt használó gazdálkodó szervezet folyamatai működésébe illessze bele az információbiztonság szemléletét. Akkor működik jól, ha a szervezet működésébe beépülő kockázatarányos intézkedésekkel minimalizálni tudja a folyamatok működése során a kezelt adatok biztonságának (azaz bizalmasságának, sértetlenségének és rendelkezésre állásának) elvesztése vagy sérülése következtében a vállalatra gyakorolt kár mértékét. Az információbiztonsági irányítási rendszer rendszerszabványa ennek kialakítására adja meg egy jól működő keretrendszer követelményeit. A szabvány az A mellékletében a technikai intézkedésekre vonatkozó biztonsági kontrollokat határoz meg, amelyek alapját a több évtizedes kialakult szakmai 'jó gyakorlatok' (best practice) képezik. Természetesen ezek a technikai biztonsági kontrollok nem minden esetben kötelezőek, és az adott körülményekre testre szabva, kockázatarányosan alkalmazandók.

A gazdálkodó szervezetek által kezelt adatok között mindig szerepelnek személyes adatok is, így az információbiztonsági irányítási rendszer követelményei értelemszerűen azokra is kiterjednek. Az ISO 9001 szabványban fenn bemutatott követelményeket – köszönhetően az irányítási rendszerszabványok kötelezően egységes struktúrájának – az ISO/IEC 27001 szabvány is ugyanúgy tartalmazza, tehát az ott bemutatottak ugyanúgy érvények az információbiztonsági irányítási rendszerek esetén is. Azonban az információbiztonsági irányítási rendszerek esetén magának az irányítási rendszernek az alapvető célja és funkciója az adatok – köztük a személyes adatok – kezelésének és biztonságának a megfelelése, maga az egész irányítási rendszer ennek teljesítésére épül fel.

Az 'ISO rendszerek' a GDPR megfelelésben

A GDPR elvárja a gazdálkodó szervezetektől, hogy a személyes adatok kezelése során minden esetben:

- legyen meghatározva, hogy mikor kezelhető személyes adat, azaz amikor annak célja és megfelelő jogalapja azonosított, csak akkor valósuljon meg az adatkezelés;
- legyenek a GDPR-ban megfogalmazott **a**datkezelési alapelvek azonosítva és betartva, azaz követelményeket és korlátokat határoz meg az adatkezelés mértékére, módjára és terjedelmére;
- legyenek az adatkezelésben érintett természetes személyek jogai biztosítva, és az legyen számukra kommunikált is;
- működjön az „elszámoltathatóság" elve, azaz ez a működés legyen mindig, garantáltan és igazolhatóan szabályozott;
- legyen garantált a kellő mértékű adatbiztonság, azaz legyen biztosított a személyes adatok bizalmassága, sértetlensége és rendelkezésre állása megfelelő és kockázatarányos intézkedésekkel.

Ezek számos követelményt jelentenek, amelyekre azonban megvalósítási módot nem határoz meg a jogszabály. A GDPR csak a követelményeket írja elő, de sem azok adott vállalatra vagy intézményre való testre szabásának módjára, sem azok betartására vagy megvalósítására nem ad segítséget.

Másrészről az egyes ISO irányítási rendszerszabványok által meghatározott irányítási rendszerek éppen olyan keretrendszereknek a működését és szabályrendszerét írják le, amelyekkel a kívánt követelményrendszereknek való megfelelést tud az azt alkalmazó vállalat vagy intézmény elérni. Tehát ezek az ISO rendszerek épp abban tudnak segíteni, ami – jelen esetben – a GDPR-ból hiányzik, azaz segítséget tudnak nyújtani a GDPR követelményeknek való megfelelés megszervezésében, irányításában és megvalósításában.

Ha egy vállalat a GDPR követelményeknek való megfelelés biztosítására valamelyik ISO rendszer általi irányítási rendszer (pl. ISO 9001 vagy ISO/IEC 27001 szerinti rendszer) alkalmazását választja módszernek, akkor a GDPR követelményeit kell a teljesítendő célok, követelmények közé állítania. Akkor a vállalat működésébe és a folyamatszabályozásokba szabályozottan és igazolhatóan – megfelelve az elszámoltathatóság elvének – annak a teljesítése épül be, támogatva egyidejűleg a vállalat üzleti céljait és hatékony működését is.

Ha az adott vállalatnál már működik egy ISO rendszer (pl. ISO 9001 vagy ISO/IEC 27001 szerinti rendszer), akkor az a GDPR bevezetése következő tevékenységeinek végzésénél nagymértékben segítséget nyújt:

- A GDPR bevezetésének első lépése az adatkezelési tevékenységek felmérése a működő folyamatok mentén.
  → A szabályozottan működő ISO rendszerek esetén vannak dokumentáltan szabályozott folyamatok, és azok tevékenységei már ismertek, dokumentáltan szabályozottak.
- A GDPR adatkezelések során felmérni, azonosítani kell a kezelt személyes adatokat.
  → ISO 9001 szerinti minőségirányítási rendszerek esetén a folyamatokban kezelt dokumentált információk már azonosítottak, kezelésük szabályozott, és ez jó kiindulási alap a személyes adatok részletes azonosítására.
  → ISO/IEC 27001 szerinti információbiztonsági irányítási rendszerek esetén azonosítottak a kezelt adatok (köztük személyes adatok is), így ott az adatvagyon részletes felmérése (és sokszor az osztályozása is) már adott.
- A GDPR adatkezelésekhez meg kell határozni az adatok adatvédelmi kockázatait is, hogy azok alapján meghatározhatóak legyenek a szükséges bevezetendő adatvédelmi intézkedések.
  → ISO 9001 szerinti minőségirányítási rendszerek esetén kötelező elvárás a kockázatalapú szemlélet bevezetése, aminek következtében alkalmazni kell valamilyen, jellemzően folyamatalapú kockázat-felmérési módszert. Ez általában könnyen kiterjeszthető a személyes adatkezelések adatvédelmi kockázatainak meghatározására is.
  → ISO/IEC 27001 szerinti információbiztonsági irányítási rendszerek esetén általában speciális szakmai módszerrel meghatározottak a felmért adatvagyon információbiztonsági kockázatai, amelyek kiterjednek a köztük lévő személyes adatokra is.

- A felmért kockázatok alapján meg kell határozni a szükséges adatvédelmi intézkedéseket.
  → ISO 9001 szerinti minőségirányítási rendszerek esetén kötelező elvárás a kockázatalapú szemlélet bevezetése, aminek következtében kötelező a feltárt nagy kockázatok esetén megfelelő kockázatkezelési intézkedések alkalmazása. Ez könnyen kiterjeszthető az adatvédelmi kockázatok esetére is.
  → ISO/IEC 27001 szerinti információbiztonsági irányítási rendszerek esetén az adatvagyon felmért információbiztonsági kockázatai alapján bevezettek és felügyeltek számos információbiztonsági kontrollintézkedést, amelyek kiválasztására a szabvány A melléklete és maga az információbiztonsági szakma jó gyakorlata számos segítséget ad. Ezek kiterjednek a köztük lévő személyes adatok adatvédelmi kockázataira is.

- A kockázatalapon meghatározott adatvédelmi intézkedéseket egy adatvédelmi menedzsment keretrendszer segítségével kell felügyelni, karbantartani és működtetni.
  → Tulajdonképpen ezt a feladatot látja el maga az ISO/IEC 27001 szerinti információbiztonsági irányítási rendszer.

Ebből látható, hogy egy meglévő és működő irányítási rendszer nagy segítséget tud nyújtani a GDPR követelményeknek való megfelelés kialakításában, elsősorban a felmérésekben és szabályozások kialakításában, illetve ISO 27001 alkalmazása esetén az adatbiztonsági követelmények magas szintű szakmai teljesítésében.

GDPR bevezetés tapasztalatai, problémái az ISO-val rendelkező szervezeteknél

A GDPR-szerű működés kialakítása, annak lépései különböző jellegű feladatokat és azzal kapcsolatban különböző jellegű szakmai ismereteket és képességeket kíván.

- A személyes adatkezelési tevékenységeket és a kezelt személyes adatokat a működő folyamatok mentén fel kell mérni, és nyilvántartást kell róluk készíteni.
  → Ehhez elsősorban folyamatmenedzsment ismeretekre, rendszerszemléletre és rendszerező képességre van szükség.

- A személyes adatkezelési tevékenységek célját, jogalapját és jogi megfelelési jellemzőit azonosítani kell, szükség esetén javaslatokat kell tenni az adatkezelési tevékenységek módosítására vagy beszüntetésére.
  → Ehhez adatvédelmi jogi ismeretek szükségesek.

- A személyes adatkezelési tevékenységek adatbiztonsági kockázatait fel kell mérni, és javaslatokat kell tenni a szükséges biztonsági intézkedésekre.

  → Ehhez információbiztonsági ismeretek szükségesek, mind az IT biztonság, mind a nem IT-alapú információbiztonság, mind a biztonságszervezés területein.

- A személyes adatkezelési tevékenységek megfelelő működtetésének elszámoltathatósága érdekében annak dokumentált és igazolható szabályozási rendszerét kell kialakítani, amely folyamatosan felügyelt és szükség esetén folyamatos továbbfejlesztése biztosított. Mindemellett ezt úgy kell megvalósítani, hogy az adatkezelési tevékenységek megfelelő szabályozottsága mellett a vállalat rugalmas és hatékony üzleti működése is fennmaradjon és fenntartható legyen.

→ Ehhez folyamatmenedzsment, vezetési és ISO rendszerekre vonatkozó ismeretek és képességek szükségesek.

Ebből látható, hogy egy GDPR-nak való megfelelés kialakítása számos különböző szakmai ismeretet kíván meg. A probléma az, hogy jellemzően alig van olyan szakértő, aki egyszerre rendelkezik ezekkel az ismeretekkel és képességekkel. Sokszor még olyan szakértői csapatot is nehéz találni, ahol ezek a kompetenciák egyszerre jelen lennének. A szervezetek vezetői a GDPR-nak való megfelelés kialakítását sokszor egy munkatársnak, esetleg egy külső szakértőnek adják oda, akik a fenti szakmai ismeretek közül jellemzően csak az egyikkel rendelkeznek. Ekkor mind a felmérés, mind a kialakított szabályozás szakmai szempontból könnyen hiányossá válik, és a kialakított működési rendszer valamelyik komponense hiányos vagy gyengén működő lesz.

Tapasztalat szerint az ISO irányítási rendszerrel rendelkező cégek esetében is a GDPR-nak való megfelelés kialakítása számos buktatóval jár, és sok esetben nehezen és lassan halad. Az eddigi tapasztalatok alapján a következő jellemző csoportosítás figyelhető meg:

- Számos cég még semmit sem tett a GDPR-nak való megfelelés kialakítására. Ezek nagy része a KKV szektorba tartozik. Itt a vezetők részéről a kivárás taktikája a jellemző, arra gondolnak, hogy „úgysem minket fognak először ellenőrizni”.
- A cégek egy másik csoportjára jellemző, hogy megszerzett (pl. ingyen van nagyon kevés pénzért internetről letöltött) valamilyen Adatvédelmi szabályzat mintát, arra ráírta a cége nevét és ezt gondolja a GDPR megfelelésnek. Itt a cél nyilvánvalóan a kötelezettség gyors és formális kipipálása. 2018 nyarán Magyarországon kihirdetve lett, hogy a KKV szektorban az első esetben nincs büntetés csak figyelmeztetés. Így ezzel a formális megoldással a cégvezető a ’jó szándékot’ már bemutatni véli, és ezzel a megoldással az első büntetést elkerülni gondolja.
- Sok esetben, különösen közepes vagy nagyobb vállalatoknál, ahol volt már régebben is Adatvédelmi szabályzat, ott azt aktualizálták. Ez alapvetően jó megoldásnak számít. Az aktualizált szabályzat megfelelősége és teljessége természetesen az aktualizálást végző szakértők tudásának és ráfordítási idejének a függvénye.
- Sok esetben külső tanácsadót bíztak meg a GDPR-nak való megfelelés és a kapcsolódó szabályzatok kialakításával. Itt az elkészült eredmény szakmai színvonala nagyon különböző, egészen a használhatatlantól a nagyon kiválóig terjed. Ez a tanácsadó (vagy tanácsadói csapat) szakmai hozzáállásának, tudásának és munkamennyiség ráfordításának a függvénye. Természetesen itt is nagy szerepet játszik, hogy a GDPR kialakításához szükséges kompetenciák közül melyek vannak meg vagy melyek hiányoznak a munka során.

A GDPR-nak való megfelelés kialakításának fő problémái röviden a következőkben foglalhatók össze:

Hatósági (külső elvárási) oldalról:

- GDPR követelményei túl általánosak – néhol belső ellentmondások is vannak benne.
- Az Infotörvény és maga a GDPR néhány helyen ellentmondanak egymásnak.

- Nincsenek még meg a szükséges ágazati jogszabályok, illesztések.
- Nincs (kevés) a használható hatósági állásfoglalás, útmutató.

Szervezeti, vállalati (megfelelési) oldalról:

- Nagyon sok szervezet még semmit sem csinált.
- Sokan csak formális szabályozást készítettek valódi működés nélkül.
- GDPR kiépítést (szabályozást) sokszor csak egy területnek adják oda (egyféle szaktudás).
- A jogászok sokszor csak külön 'sziget-megoldást' készítenek, ami nem integrált a vállalati szabályozási rendszerbe.
- Valódi, életszerű problémákra kevés a jó megoldás.

Összefoglalás

A személyes adatok kezelésére vonatkozó új jogszabály, az EU általános adatvédelmi rendelete (a GDPR) egy új, részletekbe menő szigorú követelményrendszer a gazdálkodó szervezetek számára. Noha ez a jogszabály 2016 áprilisában lépett életbe, a számonkérés határidejére csak 2018. május 25. volt. Ezért az erre való felkészülésre két teljes év állt a rendelkezésre, mégis csak az utolsó félévben kezdtek el ezzel foglalkozni a vállalatok. Az első vállalatoknak külön nehézséget jelentett, hogy ebben nem volt még senkinek gyakorlata, nem volt erre ismert példa.

Maga a jogszabály is csak követelményeket határoz meg, de sem annak értelmezésére, sem a testre szabásra, sem a megvalósítás módjára kezdetben semmilyen segítség vagy hatósági állásfoglalás, ajánlás nem volt.

A vállalatok számára a végrehajtásra hasznos segítséget nyújthatnak az ISO szerinti irányítási rendszerek, hiszen azok a tetszőlegesen kívánt követelményrendszerek, mint szempontrendszerek vállalati működésbe való beillesztésére adnak szabályozott keretrendszert.

Ha a GDPR által meghatározott követelményeket szétbontjuk jogi megfelelési és technikai (adatbiztonsági) megfelelési követelményekké, akkor egy meglévő minőségirányítási rendszer képes a felmérésben és a szabályozások kialakításában strukturált segítséget nyújtani. Ugyanakkor az információbiztonsági irányítási rendszer például ezen túlmenően a technikai adatbiztonsági követelmények magas szintű megvalósításában is segít, illetve lehet, hogy egy már meglévő információbiztonsági irányítási rendszer esetén ez megvalósított és működő is.

Szerző
Dr. Horváth Zsolt
Az INFOBIZ Informatikai, Információbiztonsági és Vezetési Tanácsadó Kft. társtulajdonosa és ügyvezetője 2006 óta. EOQ MNB által regisztrált minőségirányítási és információbiztonsági rendszermenedzser és auditor. Tíz évig látta el a SIEMENS magyarországi szoftverházának, a SIEMENS PSE Kft-nek 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 és társszerzője. A Budapesti Metropolitan Egyetem Információbiztonsági Menedzser c. posztgraduális szakirányú továbbképzésének a szakfelelőse és oktatója.