Hogyan segíthet az ISO 27001 szabvány a GDPR megfelelésben

Ahogy közeledünk 2018. május 25-éhez egyre sűrűbben hallhatnunk a GDPR-ról, az EU adatvédelmi rendeletéről. Egymást érik a konferenciák a témában, cégek hirdetik technikai megoldásaikat vagy szolgáltatásaikat, mint kulcsot a megfeleléshez. De a technikai megoldások mellett szükség van egy **Rendszerre.** Cikkünkben nem szeretnénk magával az EU 2016/679 rendelettel vagy értelmezésével foglalkozni, magyar nyelven megtalálható a rendelet az interneten, csupán azokkal a kapcsolódási pontokkal, amelyek lényegesek lehetnek az ISO 27001 szabvány alkalmazása szempontjából.

Már a GDPR megjelenése elött is voltak követelmények a személyes adatok védelmére vonatkozóan (pl. 2011. évi CXII tv), némely tekintetben szigorúbbak is, mint a 2018. májusától életbe lépő szabályozás, és egyébként adatvédelmi bírság is! Kétségtelen, hogy az új limitek felébresztették a cégek vezetőit. Az is tény továbbá, hogy azoknak a vállalatoknak, amelyek nemzetközileg működnek, egységesen minden országban meg kell felniük az új rendeletnek, nem „csak” a magyar jogszabályoknak. Talán ezzel is magyarázható, hogy a GDPR kérdése folyamatosan napirenden van. Persze eddig is voltak más országokban is nemzeti jogszabályok ezen a téren, és ahol, és amely cégek komolyan vették a jogszabályi követelményeknek való megfelelést, most határozottabban előbbre tartanak a felkészültségben.

Az ok, amiért úgy döntöttünk, hogy készítünk egy útmutató leírást, egyrészt az, hogy egyre gyakrabban kérik ki véleményünket a témában, hogy mennyiben segíthet az ISO 27001. Gyakran tapasztaljuk, hogy úgy beszélnek a GDPR -ról, mint egy Rendszerről, és a megfelelés biztosításában úgy tűnik alábecsülik az ISO 27001-ben rejlő lehetőségeket is.

Mi is az ISO 27001 szabvány?

Az ISO 27001 szabvány folyamatszemléletű megközelítést alkalmaz a szervezet információbiztonság irányítási rendszerének (ISMS) kialakítására, bevezetése, működtetésére, figyelemmel kísérésére, átvizsgálására, karbantartására és fejlesztésére. Tehát nem jogszabály vagy rendelet, mint a GDPR, hanem irányítási rendszer szabvány, követelmények halmaza, amely követelményeknek a tanúsított szervezetnek meg kell felelniük a független, akkreditált tanúsító szervezetek által végrehajtott auditokon. Itt megemlíteném, hogy az EU 2016/679 rendelet 42. cikke ösztönözi az adatvédelmi tanúsítási mechanizmusokat, 43. cikke rendelkezik a tanúsító szervezetekről az EN-ISO/IEC 17065/2012 szabványnak megfelelően, amely akkreditált szervezetre utal! Tehát egy nem akkreditált tanúsítás nem biztos, hogy megvéd bennünket egy jogi procedúrában! Hasznos egyébként utána járni, mitől akkreditált egy tanúsítás. (https://www.dnvgl.hu/assurance/Management-Systems/accredited-certification.html)

De miben segíthet az ISO 27001?

A GDPR ösztönözi az olyan tanúsítási rendszereket, mint az ISO 27001, azzal a céllal, hogy bizonyítsa, hogy a szervezet a nemzetközi legjobb gyakorlatnak megfelelően aktívan kezeli adatbiztonságát. Az ISO 27001 megvalósításával szervezete egy olyan információ-biztonság irányítási rendszert vezet be, amely a képes a szervezet külső és belső környezetének változásaival összhangban biztosítani információinak bizalmasságát, sértetlenségét és rendelkezésre állását.

Az ISO 27001: 2013 szabvány 114 olyan védelmi intézkedést vázol fel, amelyek az információbiztonsági kockázatok csökkentésére használhatók, és kiválasztásuk alapja egy szisztematikus, rögzített módszertan szerint végrehajtott kockázatértékelés. A teljesség igénye nélkül ezek a kontrollok valamennyi lényeges területre kiterjednek, kedve a felső vezetés elkötelezettségével, a személyzet biztonságon, a fizikai és környezeti biztonságon, az információs rendszerek és hálózatok üzemeltetésének biztonságán át, akár a működés folytonosságig. A szabvány célja nem csak a személyes adatok védelme, hanem vállalata és érdekelt feleinek valamennyi értékes adatának, információinak védelme.

Miért több az ISO 27001?

A szabvány egyértelmű intézkedést fogalmaz meg „Minden vonatkozó jogszabályi, szabályozói, szerződéses követelményt és a szervezet megközelítését, hogy megfeleljen ezeknek a követelményeknek egyértelműen azonosítani, dokumentálni és naprakészen kell tartani minden információs rendszerre és szervezetre". Tehát nem csak a GDPR rendeletnek, hanem valamennyi vonatkozó jogszabálynak meg kell felelnie egy tanúsított szervezetnek. De ezen felül is rendelkezik a szabvány a személyes adatok védelméről, „a személyazonosításra alkalmas adatok védelmét a védelemre vonatkozó jogszabályokban és rendeletekben előírtak szerint kell biztosítani, amennyiben alkalmazandó", ez szintén biztosítja a kapcsolódást a GDPR-hoz. Ezért helytelen az a gyakran hallott vélekedés, hogy az ISO 27001 követelményei nem biztosítják a GDPR megfelelést, mivel minden vonatkozó jogszabályi követelmény egyértelműen alkalmazandó, és a megfelelés akár teljes körűen vizsgálható az auditok során. Mindenesetre még akkor is, ha a GDPR nem terjed ki a szervezetre, az ISO 27001 előbb említett iránymutatásai hivatottak biztosítani a személyes adatok védelmét.

De mit is mond a GDPR?

Idézet a 32. cikkelyből *„Az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá 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 érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, ideértve, többek között, adott esetben:*

*a) a **személyes adatok álnevesítését és titkosítását**;*

*b) a személyes adatok kezelésére használt rendszerek és szolgáltatások **folyamatos bizalmas jellegének biztosítását**, integritását, rendelkezésre állását és ellenálló képességét;*

*c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az **adatok rendelkezésre állását** kellő időben vissza lehet állítani;*

*d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának **rendszeres tesztelésére, felmérésére és értékelésére** szolgáló eljárást."*

A rendelet 33. cikkében deklarálja az adatvédelmi incidensek bejelentését, mely szerint „Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az 55. cikk alapján illetékes felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár

kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is."

Válaszok az ISO 27001 -ben

Kockázatértékelés

Az ISO 27001 megköveteli a tanúsított szervezettől, hogy módszeres kockázatelemzést végezzenek azon fenyegetések és sebezhetőségek azonosítása révén, amelyek befolyásolhatják a szervezet információs eszközeit, és lépéseket tehetnek az adatok bizalmas kezelésére, integritásának és rendelkezésre állásának megőrzésére. A GDPR szintén megköveteli a kockázatértékelést annak biztosítására, hogy a szervezet azonosítsa azokat a kockázatokat, amelyek befolyásolhatják a személyes adatokat.

A GDPR-ban meghatározott magas bírságok és a szervezetekre gyakorolt jelentős pénzügyi hatás miatt a személyes adatokkal kapcsolatos kockázatértékelés során felmerülő kockázatok túl magasak lesznek ahhoz, hogy azokat ne kezeljék. Másfelől a GDPR egyik új követelménye az adatvédelmi hatásvizsgálatok végrehajtása, ahol a vállalatoknak először meg kell vizsgálniuk a saját titkosságukat veszélyeztető kockázatokat, összhangban az ISO 27001 előírásaival. Természetesen a rendszer kialakítása során a személyes adatokat kiemelten fontosnak kell tekinteni szabvány, és az A.8.2.1 Információk osztályozása védelmi intézkedés szerint: " Az információkat a jogi előírások szerint kell besorolni, érték, kritikusság, érzékenység a jogosulatlan közzétételhez vagy módosítás alapján."

Adatok titkosítása

Az ISO 27001 szabvány is ajánlja a titkosítást, mint az egyik olyan védelmi intézkedést, amelyet egy azonosított kockázat csökkentésére alkalmazni lehet, olyan információbiztonsági célok elérésére, mint a titoktartás, integritás, letagadhatatlanság vagy hitelesítés. Mivel a szervezetek által kiválasztott intézkedéseknek a kockázatértékelés eredményein kell alapulniuk, a szervezet képes lesz azonosítani, hogy mely eszközök vannak veszélyeztetve, és melyek igényelnek titkosítást a megfelelő védelem érdekében.

Tesztelés és értékelés

Természetesen az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére számos követelményt találunk az ISMS-ben, ilyen például a 9.1 Figyelemmel kísérés, mérés, elemzés és értékelés, 9.2 belső auditok, 9.3 vezetőségi átvizsgálás, továbbá a szabvány A mellékletének intézkedései, mint például A12.4 Naplózás és monitoring, A12.6, Műszaki sebezhetőség kezelése, A12.7 Információs rendszerek audit szempontjai vagy A18.2 Információbiztonsági felülvizsgálatok, és alpontjai.

Ezen felül az ISO 27001 tanúsítványt választó szervezetek az akkreditált tanúsító testület által függetlenül értékeltetik és auditáltatják rendszerüket annak érdekében, hogy az irányítási rendszer megfeleljen a szabvány követelményeinek. Az akkreditált minősítés megszerzésével a tanúsított szervezet nem csak egy igazoló dokumentumot kap, hanem egy szakértői értékelést is a rendszere hatékonyságáról, és útravalót a rendszere további fejlesztéséhez.

Működés folytonosság

Az ISO 27001 foglalkozik az üzletmenet-folytonosság irányításával is, amely olyan intézkedéseket határoz meg, amelyek segítséget nyújtanak a szervezet számára az információ rendelkezésre állásának megóvásában, a redundancia biztosításában, egy nem várt esemény bekövetkezése esetén. Ezáltal az információbiztonság folyamatosan fenntartható mindhárom alap cél - bizalmasság, sértetlenség és rendelkezésre állás - tekintetében.

Incidensek kezelése

A vállalatoknak a személyes adatok megsértése után 72 órán belül értesíteniük kell az adatközlési hatóságokat. Az ISO 27001 A.16.1 „Az információbiztonsági események és fejlesztések" pontja biztosítja, hogy az incidensek jelentésre, értékelésre, a bizonyítékok begyűjtésre kerüljenek, és mindezen feladatokkal kapcsolatos felelősségek legyenek meghatározva.

Eszközkezelés

Az ISO 27001 A.8 „Eszközkezelés” kontrollok biztosítják a szervezet eszközeinek nyilvántartását, rendelkeznek elfogadható használatukról, vissza szolgáltatásukról, az információk osztályozásáról és jelöléséről, az információt tároló média kezeléséről, megsemmisítéséről, biztosítva ezáltal nem csak az üzletileg fontos információknak, de a személyes adatoknak a hatékony védelmét is. Ezen intézkedések segítik a szervezeteket, hogy megértsék, milyen személyes adatokra van szükség, hol tárolják ezeket, mennyi ideig, hol és hogyan férhetnek hozzá, amelyek mind követelményei a GDPR-nak.

Adatvédelem „by design”

A termékek és rendszerek fejlesztésében kötelezővé válik a „**Terv szerinti adatvédelem**”, egy másik GDPR követelmény. Az ISO 27001 A.14 „Információs rendszerek beszerzése, fejlesztése és karbantartása” biztosítja, hogy az információbiztonság az információs rendszerek szerves része legyen a teljes életciklusban. Találhatunk itt intézkedéseket a „biztonságos fejlesztési szabályzatoktól” kezdve a „biztonságos rendszer tervezési alapelveken”, a „kiszervezett fejlesztésen” át, a „rendszerek biztonsági teszteléséig”, csak hogy néhányat említsünk.

Szállítói kapcsolatok

A GDPR szerint, amennyiben a szervezet szolgáltató felé delegálja a személyes adatok feldolgozását és tárolását, előírja, hogy a rendelet követelményei a hivatalos megállapodások révén is teljesüljenek. Az ISO 27001 A.15.1 „Információbiztonság a beszállítói kapcsolatokban" biztosítja a szervezet azon eszközeinek, információinak védelmét, amelyek elérhetőek a beszállítók számára. Gondoskodik a szabvány arról, hogy a beszállítókkal kötendő megállapodásokban rögzítésre kerüljenek az információbiztonsági követelmények, valamint a szolgáltatás nyújtás folyamata hatékonyan figyelemmel legyen kísérve.

Összefoglalva

Nagyon sok vállalat és szervezet lehet érintett a rendeletnek való megfelelésben. Mivel az ISO 27001 egy nemzetközileg elismert és a világ minden táján alkalmazott információbiztonsági rendszer szabvány, ez lehet a legjobb lehetőség a GDPR azonnali betartásának elősegítésére. Amennyiben a vállalkozás jelenléte nemzetközi szintű, különösen nélkülözhetetlen lehet egy széleskörben, nemzetközileg elismert rendszer alkalmazása. Az ISO 27001-et már világszerte több ezer szervezet alkalmazza, és napjainkban egyike a leggyorsabban növekvő irányítási rendszer szabványoknak

Az alkalmazott technikai ellenőrzések, a strukturált dokumentáció, nyomon követés és folyamatos fejlesztés mellett az ISO 27001 bevezetése elősegíti a szervezetekben a biztonsági incidensek kezelésének kultúráját és tudatosságát. Ezen szervezetek alkalmazottai jobban tudatában vannak, és nagyobb tudással rendelkeznek a biztonsági események észleléséhez és jelentéséhez. Az információbiztonság nem csak a technológiáról szól, hanem a folyamatokról és az emberekről is.

Az ISO 27001 szabvány kitűnő keretrendszer a GDPR megfeleléshez is. Ha egy szervezet már bevezette a szabványt, legalább félúton van a személyes adatok védelmének biztosítása és az adatszivárgás kockázatának minimalizálása érdekében.