ADATVÉDELEM

GDPR
kisokos

+36 (70) 881-4234
info@adatvedelmiszolgaltato.hu
www.adatvedelmiszolgaltato.hu

GDPR KISOKOS

Több éven áthúzódó tárgyalássorozatot követően hatályba lépett az Európai Unió általános adatvédelmi szabályzata (EU GDPR), ami 2018 május 25-én a korábbi uniós adatvédelmi irányelvek helyébe lép.
A GDPR célja, hogy az uniós polgárok személyes adatainak védelmét szolgálja. Szabályozza az adatgyűjtés módját, feldolgozását, tárolását, törlését, adattovábbítást és felhasználását. Minden cégnek, legyen az helyi vagy nemzetközi, meg kell felelnie az új szabályozásnak, aki Európában üzleti tevékenységet folytat vagy uniós polgárok személyes adatait kezeli.
Az új szabályozás betartására irányuló felkészülési terv kidolgozása minden szervezet számára kritikus.
A bírságok mértéke az éves globális bevétel 4%-áig vagy 20.000.000 €-ig terjedhetnek, továbbá a kettő közül azt kell kifizetni, amelyik a magasabb. (Ez az összeg lényegesen magasabb, mint bármely EU tagállam adatvédelmi hatáskörben működő hatóságának büntetési díjszabása.)

De hogyan lehet megfelelni az elvárásoknak? Milyen változtatásokat kell a szervezet belső folyamataiban végrehajtania és milyen technológiákat kell alkalmaznia a személyes adatok védelmének biztosítása érdekében?
Hogyan integrálhatják az informatikai és adatbiztonsági szakemberek a "beépített adatvédelmet" a fejlesztési terveikbe?

Ez a kisokos az alábbi lépések szerint segíti Önt a GDPR megfelelésben:

1. Térképezze fel a személyes adatfeldolgozás jelenlegi állapotát a szervezeten belül
2. Állítson fel egy tervet, amelynek célja a szervezet teljes GDPR megfelelése
3. Védje az összes azonosított személyes adatot
4. Javítsa a megfelelőségi programját a folyamatos adatvédelmi ellenőrzések segítségével

GDPR ALAPFOGALMAK - DEFINÍCIÓK

Adatállomány: Az egy nyilvántartásban kezelt adatok összessége.

Adatfeldolgozás: Az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adatokon végzik. Jelen Szabályzat értelmezésében adatfeldolgozás különösen minden olyan, érdemi döntést nem igénylő technikai adatkezelési művelet, amit az adatkezelő megbízása alapján az adatfeldolgozó végez.

Adatfeldolgozó: Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely az adatkezelővel kötött szerződése alapján - beleértve a jogszabály rendelkezése alapján történő szerződéskötést is - adatok feldolgozását végzi.

Adatgazda: Egy adott szervezeti egységnél kezelt személyes adatok tekintetében a szervezeti egységet irányító vezető, aki felelős a szervezeti egysége által kezelt valamennyi személyes adat jelen szabályzatnak megfelelő kezelésért (továbbiakban: adatgazda). Amennyiben IT rendszerben kezelt személyes adattal kapcsolatos döntés meghozatala szükséges, és az érinti az Információ Biztonsági Szabályzat szerinti adatgazda felelősségét, akkor a személyes adatgazda az Információ Biztonsági Szabályzat alapján kijelölt adatgazda egyetértésével hozza meg döntését.

Adathordozó: Az adat fizikai megjelenési formája, tárolási helye, ide értve az iratokat is.

Adatigénylő: Az a természetes, vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely a személyes adatai kezelésével, helyesbítésével, törlésével vagy zárolásával kapcsolatban kérelmet nyújt be a Szervezethez.

Adatkezelés: Az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése. Jelen Szabályzat értelmezésében adatkezelés különösen az egyes adatkezelési műveletekkel kapcsolatos döntések meghozatala, utasítások kiadása.

Adatkezelő: Az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adatok kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az általa megbízott adatfeldolgozóval végrehajtatja.

Személyes adat: Az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés.

Adatkezelési incidens: 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 GDPR 7 ALAPELVÉNEK MEGISMERÉSE

A digitális fejlődés átalakítja a munkavégzést. A modern üzleti életben az alkalmazottak és az általuk használt eszközökben a személyes adatokhoz való hozzáférés, bárhol lehetséges. A marketingesek egyre inkább arra ösztönzik az embereket, hogy csatlakozzanak a közösségi oldalakhoz, használjanak mobil alkalmazásokat, webes felületeket és hírlevelekre iratkozzanak fel. Mivel a személyes adatokat feldolgozó üzleti alkalmazásokban jelenlévő személyes adatok többnyire felhőben tárolódnak és az emberek egyre több információt osztanak meg az új digitális csatornákon keresztül, ez exponenciálisan növeli a személyes adatok kezelésének kockázatát.
Az EU GDPR alapvetően a kockázat csökkentésére a rendelet 99. cikkelyében meghatározza, hogy milyen személyes adatok gyűjthetők össze, mikor lehet összegyűjteni, és hogyan kell ezeket az adatokat feldolgozni és biztosítani.
Mielőtt bármilyen intézkedést megtenne az EU GDPR megfelelés érdekében javasoljuk, hogy előbb teljes mértékben legyen tisztába a követelményekkel.

A GDPR hét kulcsfontosságú alapelvből áll, ezek az alábbiak:

CÉLHOZ KÖTÖTTSÉG

Személyes adatok gyűjtése csak meghatározott, egyértelmű és jogszerű célból történjen, és azokat ne kezeljék ezekkel a célokkal össze nem egyeztethető módon; a 89. cikk (1) bekezdésének megfelelően nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés.

Személyes adatot felvenni és felhasználni általában csak az érintett beleegyezésével szabad. Mindenki számára követhetővé és ellenőrizhetővé kell tenni az adatfeldolgozás egész útját vagyis mindenkinek joga van tudni, hogy hol, mikor és milyen célra használja fel az ő személyes adatait.

Az adatkezelés minden szakaszában meg kell felelnie az adatkezelés céljának, ez azt jelenti, hogy nem csak az adatkezelő és más személyek közötti adatátadás, hanem az adatkezelés minden olyan szakasza, amelyet az adatkezelő kizárólag a szervezetén belül végez.

Az adatkezelőnek olyan belső eljárásrendet kell kidolgoznia, amely biztosítja, hogy az adatkezelés folyamata ne lépjen ki az adatkezelési cél által meghatározott keretekből.

A cél változása minden esetben új adatkezelést eredményez. Cél nélküli adatkezelés az adatalany hozzájárulása esetén sem végezhető.

Szükséges idő figyelembe vétele: A célhoz kötöttségbe ütköző lehet az adatkezelés akkor, ha az adatok kezelése nem a szükséges időre korlátozódik, tekintettel arra, hogy a felvett adatok minősége, időszerűsége az idő múlásával változik, romlik. Az "időbeni korlátozás nélkül" kifejezés ellentétes az adatvédelem elveivel.

A célhoz kötöttség elve nem érvényesül a közérdekű adatok kezelése esetén.

TISZTESSÉGES ÉS TÖRVÉNYES ADATKEZELÉS

Az adatkezelést jogszerűen és tisztességesen, valamint az érintett számára átlátható módon kell végezni.
A tisztességes adatkezelés követelménye akkor kerül a vizsgálat fókuszába, amikor az adatkezelésnek van ugyan látszólag célja is és jogalapja is, mégis valami "nincs rendben".

Az adatkezelés tisztességes volta az emberi méltóság védelmével áll szoros kapcsolatban.

A pontos, teljes és naprakész adatok kezelésének követelménye: Személyes adatok felvételénél a pontos adatrögzítésre kell kiemelt figyelmet fordítani. Az elírás, adatbeviteli hiba sokszor az adminisztrátor gondatlanságára vezethető vissza, ennek következménye viszont súlyos lehet.

ADATTAKARÉKOSSÁG ELVE

Az adatkezelési rendszerek tervezésekor, illetve működésük során biztosítani kell azt, hogy minimális mértékben kerüljön sor személyes adatok kezelésére. (beépített adatvédelem)

Az adattakarékosság elve azt jelenti, hogy már az adatkezelés megkezdése előtt vizsgálni kell, hogy szükséges-e egyáltalán a személyes adatok kezelése. Ahogy a cél megvalósult, a személyes adatokat azonnal törölni kell- feltéve, hogy az adattárolást egyéb jogszabály nem írja elő.

PONTOSSÁG ELVE

Pontosnak és szükség esetén naprakésznek kell lenniük a kezelt személyes adatoknak. Minden ésszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés célja szempontjából pontatlan személyes adatok haladéktalanul törlésre kerüljenek.

KORLÁTOZOTT TÁROLHATÓSÁG ELVE

A kezelt adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelési céljainak eléréséhez szükséges ideig teszi lehetővé, a személyes adatok ennél hosszabb ideig történő tárolására csak akkor kerülhet sor, amennyiben a személyes adatok kezelésére a 89. cikk (1) bekezdésének megfelelően közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból kerül majd sor.

INTEGRITÁS ÉS BIZALMAS JELLEG

A személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve. (Informatikai biztonság jelentőségét ismeri el a rendelet)

ELSZÁMOLTATHATÓSÁG

Az adatkezelő felelős az adatkezelési folyamatának törvényben leírtak szerinti megfeleléséért, továbbá képesnek kell lennie e megfelelés igazolására. Az Uniós polgárok személyes adatait feldolgozó valamennyi szervezetnek képesnek kell lennie arra, hogy bizonyítékot szolgáltasson arra vonatkozóan, hogy fentiekben felsorolt elveket betartja adatkezelési eljárásaiban. Minden szervezetnek ki kell alakítania és működtetni kell egy adatrögzítési értesítési rendszert, amelybe be kell rögzíteni az összes ismert sérelmet. A közepes és magas kockázatú adatvédelmi incidenseket 72 órán be kell jelenteni a felügyeleti hatóságnak, valamint megfelelő kárenyhítési és érintettek tájékoztatására irányuló lépést meg kell tenni.

A rendelet értelmében az adatkezelők felelősek a magánélet védelméért és a személyes adatok titkosságáért, továbbá biztosítaniuk kell a megfelelő technikai és szervezeti működést érintő ellenőrzéseket a személyes adatok védelme érdekében. A kezelt személyes adatokat kizárólag az adatkezelő és az érintett között létrejött szerződés/elfogadott adatkezelési tájékoztató alapján kell kezelni.

MIÉRT FONTOS FOGLALKOZNI A GDPR-RAL?

A szervezetnek el kell tudni számolni a hatóság előtt a GDPR megfeleléssel kapcsolatosan. Ez a kötelezettség figyelmet követel a szervezetek vezetőitől, mivel nagy kockázattal járnak a GDPR óriási bírságai. Nagyon szigorú szankciókat határoz meg a megállapított elvek be nem tartása miatt. Legfeljebb 20.000.000 euró, vagy a teljes árbevétel 4% -a (a kettő közül a magasabb), az első öt alapelv megsértésére (jogszerűség, méltányosság és az átláthatóság; a pontosság és a cél korlátozása; az adatok minimalizálása és tárolás korlátozása).
A hatodik és a hetedig alapelv megsértéséért legfeljebb 10 000 000 euró, vagy az összes árbevételének 2% -a szabható ki, (integritás, bizalmasság és elszámoltathatóság). Ez a büntetés minden olyan jogsértésre vonatkozik, amelyben a vállalat nem hajtotta végre megfelelő biztonsági ellenőrzéseket, vagy az előírt 72 órán belül nem jelentette és nem járt el megfelelő módon az adatvédelmi incidenst illetően.
A GDPR szerint azok a szervezetek, amelyekről tudomásunk szerint szándékosan nem hajtották végre az ellenőrzéseket és a hét elv betartását a legmagasabb bírságot kell kiszabni, ami nem csak anyagi, hanem a vállalati hírnévben is tartós károkat okozhat. Továbbá közvetlen bírságokra is érdemes odafigyelni, amik a nem megfelelőség kapcsán merülhetnek fel, ugyanis a GDPR lehetővé teszi a magánszemélyek számára, hogy bepereljenek minden olyan szervezetet, amely károkat okozhat számára személyes adatainak megsértése miatt.

A GDPR vállalkozásokra gyakorolt hatása kétség kívül jelentős. De miért van szükség ezekre a nagy bírságokra és kiemelt odafigyelésre?
Az elmúlt években rohamosan megnőttek a személyes adatokkal való visszaélések, adatkiszivárgások és hacker támadások esetei, valamint az ezekkel okozott károk és probléma mértéke is.
A PWC szervezet kimutatásai szerint, akik 664 brit nagyvállalatot vizsgálva kimutatták, hogy 2015-ben 81%-kal nőtt az információ-biztonsági incidensek száma a 2014-es évhez viszonyítva.

Az USA Identity Theft Resource Center bejelentése szerint 2016-ban 1093 nagy információ-biztonsági incidens történt 40%-al több mint az előző évben, továbbá ezen incidensek együttvéve.
Ezen személyes adatok sérelmét okozó támadásokat, eljárásbeli és informatikai biztonsági problémák okozták, amik megakadályozhatóak lettek volna megfelelő felkészüléssel és odafigyeléssel.
A GDPR azt akarja elérni, hogy a szervezetek tudatosan figyeljenek oda a személyes adatkezeléseikre és alakítsanak ki információ biztonság szempontjából biztonságos rendszereket és folyamatokat.

Útmutató a megfeleléshez: A biztonságos adatkezelés szemléletét be kell ágyazni a folyamatokba és a munkatársak tudatosan kell, hogy figyeljenek erre a munkájuk során.

HOGYAN TUDJA BETARTANI A GDPR ELVEIT?

A rendelet útmutatást ad, és bizonyos esetekben konkrét az emberekről, folyamatokról és technológiákról szóló ajánlásokat a szervezetnek kell végrehajtania ahhoz, hogy megfeleljen a hét alapelvnek.

Ezek közé tartoznak a következők:

- Személyes adatok titkosítása
- A személyes adatokhoz és a feldolgozáshoz felhasznált berendezésekhez való jogosulatlan hozzáférés vagy használat megakadályozása
- A feldolgozó rendszerek és szolgáltatások folyamatos titkosságának és integritásának biztosítása
- A személyes adatokhoz való hozzáférés és a személyes adatokhoz való hozzáférés időben történő helyreállításának lehetősége
- Rendszeres adatvédelmi hatásvizsgálatok, az adatok eredetének, természetének, részletességének és súlyosságának értékelésére
- Adatvédelmi incidensek
- A technikai és szervezeti intézkedések hatékonyságának rendszeres tesztelésére, értékelésére és értékelésére szolgáló folyamat valamint annak biztosítására, hogy az adatfeldolgozás biztonságos legyen.

A teljes szabályozási dokumentum több mint 50 alkalommal említi a "biztonság" szót, a biztonság és a védelem egyértelműen a GDPR fő üzenete. De mielőtt elkezdené a biztonsági ellenőrzések végrehajtását, először fel kell mérnie a szervezetét, annak jelenlegi állapotát. Hogyan kezelik jelenleg a személyes adatokat a vállalkozáson belül? Milyen ellenőrzések vannak érvényben? Milyenek a hiányosságok a jelenlegi állapot és a GDPR teljes körű betartása között?

Az alábbiakban kiemeljük a négy fő lépést amit egymást követően kell végrehajtania:

Az EU GDPR-nek való megfeleléshez szükséges lépések.

1. LÉPÉS: FEDEZZE FEL ÉS OSZTÁLYOZZA AZ ÖSSZES SZEMÉLYES ADATOT

Nem védheti azt, amit nem lát. A megfelelés első lépése az összes személyes adat azonosítása és osztályozása, amit a szervezet összegyűjt, feldolgoz és tárol. Ezt könnyebb mondani, mint végrehajtani. A mai üzleti tevékenység rendkívül szerteágazó csatornákat használ az adatkezelésekben. (Személyes adatok megtalálhatóak e-mailben, a közösségi hálózatokon keresztül a felhőben stb.) Kezdjük a jelenlegi állapot értékelésével, az adatvagyon leltárral. Azonosítani kell az adatkezelési formákat, az egyes adatkezelési formákon belül számba venni, hogy milyen személyes adatok rögzítődnek, milyen eszközökön és adatbázisokban tárolódnak, mennyi ideig, kik férnek hozzá ezekhez az adatokhoz, kiknek kerül esetlegesen továbbításra további feldolgozás céljából.
Az azonosítást és osztályozást követően térképezze fel az adatgyűjtési és-használati folyamatokat. A csapatnak szükséges meghatároznia, hogyan áramolnak a személyes adatok az üzleten és az ellátási láncon keresztül. Meg kell határoznia és azonosítania kell, hogy kik azok a partnerek (harmadik felek) akik a személyes adatokat feldolgozzák a szervezete nevében.

Az adatok láthatósága és ellenőrzése kulcsfontosságú kérdés az adatvédelmi szakemberek számára.
Tegyük fel, hogy a szervezetében már be lett vezetve az ISO 27001 vagy valamilyen egyéb szabvány, ebben az esetben már lehet, hogy rendelkezik egy adatosztályozási rendszerrel és egy személyazonosító és hozzáférés-kezelő programmal. Ez nagy előnyt jelent a szervezet számára, mivel az ilyen bevezetett rendszerek bizonyítékként szolgálhatnak arra, hogy bemutatják a GDPR elszámoltathatóság elvének megfelelően, hogy a szervezet tisztában van az adatok kezelésével járó felelősséggel és rendszert alakítottak ki ennek érdekében. Vegye figyelembe, hogy a biztonsági keretek betartása (ISO27001 bevezetése) önmagában nem terjed ki az összes GDPR követelményre.

2. LÉPÉS: HOZZON LÉTRE EGY "TERVET" AZ ÖSSZES AZONOSÍTOTT VÉDELMI SZABÁLYOZÁSI HIÁNY MEGSZÜNTETÉSÉHEZ

Miután meghatározta a szervezet adatvédelmi adatainak jelenlegi állapotát, térképezze fel eredményeit a GDPR követelményeivel szemben, hogy meg lehessen határozni a nagy kockázatú hiányosságokat, amelyeket azonnal biztosítani kell.
Ebben a fázisban a szervezetnek meg kell valósítania azt, hogy az összes GDPR követelményt összeveti az első lépésben feltérképezett adatokkal és egy GAP elemzésben összesíti a hiányosságokat.
A hiányosságok összefoglalása után pedig egy cselekvési akciótervet kell kialakítani.
Ebben a lépésben több szempont van. A szervezeti adatkezelési politika létrehozása viselkedésbeli változásokat hajt végre. A terv részeként az Ön vállalkozásának létre kell hoznia egy sor adatvédelmi és irányítási irányelvet, amelyek megfelelnek a GDPR követelményeinek. A szervezet részeire vonatkozó szabályozásoknak világosan meg kell határoznia a személyes adatokhoz való hozzáférés módját, kezelni, feldolgozni, biztosítani és tárolni a szervezeten belül. Ezeket a szabályzatokat felül kell vizsgálni és jóvá kell hagyni azoknak az üzleti egységeknek, amelyeket érintenek.
Incidens-reagálási tervek: A GDPR világos iránymutatást ad arra vonatkozóan, hogy mit kell végrehajtani adatszegés esetén. Ha a vállalkozás tisztában van a személyes adatok megsértésével, értesítenie kell az érintetteket, az egyéneket és a felügyeleti hatóságot a jogsértésről.

Minden szervezetnek ki kell alakítania egy dokumentumot, ami az incidensek kezelésére vonatkozik, amely képes azonosítani és reagálni a személyes adatok megsértése esetén.
Az adatsértés észlelését követően a szervezetnek azon kell dolgoznia, hogy visszaállítsa az adatkezelés biztonságát a normális szintre. Az incidens-válasz tervnek tartalmaznia kell az adatok törlését és a jogsértési értesítési folyamatot annak biztosítására, hogy a jogsértésről a szervezet jelentést tehessen az illetékes felügyeletnek 72 órán belül.
Ahhoz, hogy sikeres legyen az incidenskezelés, biztosítani kell, hogy a helyreállítási tervek szorosan illeszkedjenek az üzleti folyamatokhoz.

A jól összehangolt tervek biztosítják, hogy folyamatos felügyelet alatt legyenek azok a folyamatok, amelyekben személyes adatokat kezelnek.

3. LÉPÉS: ADATVÉDELMI INTÉZKEDÉSEK VÉGREHAJTÁSÁNAK FOLYAMATA ÉS ELLENŐRZÉSE

A megfelelő emberek bevonása az adatvédelmi folyamatok és a technológia irányítására a legjobb megoldás a biztonságos szervezet elérése érdekében, megelőzve a véletlen vagy rosszindulatú adatsértést.
A GDPR akcióterv végrehajtásával és az összes személyes adat titkosításával és védelmével megszüntethető vagy minimálisra csökkenthető a szervezetben az adatvédelmi incidens valószínűsége, így a magas bírságok kockázata is csökkenthető.
Kezdje a megvalósítást azokkal az üzleti folyamatokkal, amik magas kockázatúak, amelyek alapvetően befolyásolhatják az uniós polgárok magánélethez való jogát.
Az alábbiakban néhány ajánlás található az olyan ellenőrzésekre vonatkozóan, amelyeket belsőleg lehet végrehajtani a szervezet által feldolgozott személyes adatokkal kapcsolatosan.

Adatvédelmi tisztviselő kinevezése: Ha jelentős mennyiségű személyes adatot rendszeresen dolgoz fel az Ön vállalkozása, akkor Önnek ki kell neveznie egy adatvédelmi tisztviselőt (akár egy belső személy vagy egy külső szolgáltatás formájában). Ez a szerep meghatározó annak érdekében, hogy tanácsot adjon minden olyan kérdésben, amely a GDPR rendeletnek való megfeleléssel kapcsolatos.

Az emberek és a szervezet elkötelezettsége a sikerhez vezető út: Támogatás nélkül nem valósulhat meg semmi. Ezért a sikeres GDPR megfelelés kulcsfontosságú tényezője a felső vezetés bevonása és a megfelelő csapat kialakítása. A GDPR egyedülálló lehetőséget kínál arra, hogy a biztonsági ellenőrzések szükségességét az igazgatótanács szintjén hozzák meg.
A központi megfelelőségi csoportnak folyamatosan felül kell vizsgálnia a GDPR programot, hogy mérje a haladást a megfelelés felé vezető úton. Ez a csapat jogi-, HR-, PR-, üzleti egység vezetőkből, adatvédelmi tisztviselőből, informatikus szakemberekből áll. Gyakorlatokat kell tartani annak ellenőrzésére, hogy a bevezetett szabályozások megfelelően kerüljenek végrehajtásra.

A munkatársak képzési programjába be kell illeszteni a GDPR és adatkezelési folyamatokkal kapcsolatos ismeretanyagot. A hangsúlyt a munkatársak viselkedésének és adatkezelés fontosságának és biztonságának szemléletformálására kell fordítani. A belső felhasználókat oktatni kell az egyes műveletekhez kapcsolódó adatbiztonsági kockázatokra.
Javasolt egy adatvédelmi és információ biztonsági szabályzat kialakítása a szervezeten belül, annak érdekében, hogy a GDPR-szabályok betartását és a személyes adatok feldolgozásának védelmét szolgálják. A szervezetnek biztosítania kell, hogy az ellenőrzések a fejlesztés teljes életciklusán keresztül megvalósuljanak minden folyamat tekintetében, amelyek érintik a személyes adatokat. A szervezeten belüli osztályoknak és vezetőknek együtt kell működniük annak biztosítása érdekében, hogy az adatvédelem minden fontos üzleti projekt középpontjába kerüljön.
A folyamatazonosítás és a hozzáférés kezelés fenntartja az irányítást: Olyan folyamatot kell kialakítani, amely csak a meghatározott felhasználók számára biztosít hozzáférést az olyan kritikus rendszerekhez (beleértve a felhőalapú szolgáltatásokat is), amelyek tárolják és feldolgozzák az uniós polgárok adatait.

Nyomon kell tudni követni és ellenőrizni az adatokhoz való hozzáférést, és ha szükséges, korlátozza ezt a hozzáférést az adatszegés kockázatának csökkentése érdekében.

Adatrögzítési értesítési nyilvántartás: Az adatvédelmi tevékenységre kiterjedő belső nyilvántartásra van szükség, amely kiemelten nyilvántartja az adatkezelési incidenseket és adatkezeléssel kapcsolatos kérelmeket az érintettek részéről.

Adattitkosítás: A GDPR egyértelműen támogatja a személyes adatok titkosítását, így az adatszegés esetén, a publikussá vált információ olvashatatlan így nem okoz kárt az érintettek számára. Ráadásul a GDPR megállapítja, hogy titkosított adatok adatvédelmi incidense kapcsán az érintetteket nem kell tájékoztatni, mivel a kikerült adataik gyakorlatilag használhatatlanok.
A tárolt adatok és a mozgásban lévő adatok titkosítási eljárásairól gondoskodni kell. Erősen javasolt az automatikus titkosítási eljárások használata.
A titkosítás végrehajtása elengedhetetlen, de ez csak a kezdet. A végső cél a teljes adatállomány biztosítása.

Technológia a az eszközök és hozzáférések menedzselésére:
Személyes adatok és eszközök felügyelete és védelme. Szegmentálja és korlátozza a hálózatának azon részeire vonatkozó hozzáférést, amelyek tárolják és feldolgozzák a rendkívül érzékeny személyes adatokat. A hálózati sebezhetőségek és külső fenyegetések felismerése és elemzése, amelyek célja az adatlopás vagy adatmegsemmisítés. Csak a vállalati hálózat folyamatos figyelemmel kísérése és védelme lehet a megoldás annak érdekében, hogy a személyes adatok ellopását célzó fenyegetések ellen hatékonyan fellépjen.

Technológia az e-mail üzenetek menedzselésére:
Az összes adatszegés több mint 90%-a e-mailben kezdődik. Az üzleti vállalkozásoknak olyan megoldásokat kell bevezetni, amelyek védik az adathalászatra irányuló támadásokat. Ezeknek a védelmi eljárásoknak képesnek kell lenniük a rosszindulatú tartalom szűrésére és a belső felhasználók megakadályozására, akik kapcsolatban állnak azokkal a hackerekkel, akik az uniós polgárok személyes adataihoz kívánnak hozzáférni.

Technológia-archívum menedzsmentre:
Automatikus megőrzési időtartamok beállítása adatbázisok és archívumok között. Az archívumkezelés kapcsán biztosítani kell az automatikus adat-visszakeresés és törlés jogát, hogy a magánszemélyek élhessenek az adattörlési kérelmükkel, vagy biztosítható legyen az adatkezelés lejárati idejének betartása.

4. LÉPÉS: BIZTONSÁGI ELLENŐRZÉSEK A HATÉKONYSÁG FOKOZÁSA ÉRDEKÉBEN

Rendszeres ellenőrzések. Miután megszervezte az ellenőrzéseket a hiányosságok feltárására, rendszeresen értékelnie kell ezek hatékonyságát. Rendszeresen értékelje az adatvédelmi kockázatokat. Tesztelje az incidensekre végbement válaszintézkedéseket. Értékelje az információs rendszerek rugalmasságát az azonosított kockázatokkal szembeni védekezéshez és mérje meg a bevezetett biztonsági ellenőrzések hatékonyságát az adatszegések megelőzésében.

Partnerek adatfeldolgozása kapcsán kockázatbecslés:
A szervezetnek felelőssége, hogy minden harmadik fél biztonsági ellenőrzését szem előtt tartsa, akik személyes adatokat dolgoznak fel a szervezet nevében. Értékelje a beszállítók (feldolgozók) biztonsági szintjét és kössön megfelelő szerződéseket a beszállítókkal annak megállapítása érdekében, hogy megfelelnek-e a GDPR feldolgozási követelményeinek.
Ha erre nem hajlandó a partner, akkor meg kell tárgyalnia egy új adatfeldolgozási megállapodást a követelmények teljesítése érdekében. Folyamatosan értékelje partnereivel közös adatkezelési folyamatainak biztonsági szintjét és megfelelőségét!

ADATVÉDELEM

A GDPR MEGFELELŐSÉGI ELLENŐRZŐLISTA

Itt van egy gyors ellenőrző lista, amely megvizsgálja, hogy készen áll-e a GDPR megfelelésre

Fedezze fel és osztályozza az összes személyes adatot. (adatvagyonleltár)

- ▢ Szervezetünk tudja (és dokumentálta), hogy milyen folyamatokban, milyen személyes adatokat kezel jelenleg
- ▢ Szervezetünk tudja, hogy az összes személyes adatot számba vettük
- ▢ Szervezetünk tudja, hol tárolódnak, milyen folyamatokban jelennek meg a személyes adatok
- ▢ Szervezetünk ismeri az összes olyan harmadik felet, amely a személyes adatokat dolgoz fel a szervezet nevében.

Hozzon létre egy "tervet" az összes azonosított védelmi szabályozási hiány megszüntetéséhez.

- ▢ Szervezetünk létrehozta és átadta az adatvédelmi és információbiztonsági szabályzatot
- ▢ Szervezetünknél van egy terv, amely felderíti, reagál, és jelentést tesz a személyes adatokkal kapcsolatos kérelmek és incidensek kezelésére.

Adatvédelem intézkedések végrehajtásának folyamata és ellenőrzése

- ▢ Szervezetünk adatvédelmi tisztviselőt nevezett ki
- ▢ A vezetőség tudatában van a GDPR programban való részvételnek
- ▢ Szervezetünk az adatvédelemre vonatkozó felhasználói tudatossági programot vezetett be
- ▢ Szervezetünk az EU személyes adatait az egyéni hozzájárulások alapján vagy egyéb megfelelő jogállás szerint rögzíti
- ▢ Szervezetünk minden nagyobb üzleti projekt adatvédelmi ellenőrzését végrehajtotta

- Szervezetünk felhasználói hozzáférési szinteket állított fel olyan rendszerek számára, amelyek személyes adatokat dolgoznak fel
- A szervezet titkosítja az összes személyes adatot
- Szervezetünk fejlett biztonsági megoldásokat alkalmazott az adatszegések megelőzése érdekében

Az eljárások hatékonyságának növelése, rendszeres ellenőrzésekkel

- Szervezetünknek van egy folyamata az adatvédelmi ellenőrzések hatékonyságának tesztelésére (a mi szervezetünkben és azon harmadik felek között, amelyek a nevünkben feldolgozzák az adatokat)
- Szervezetünk adatvédelmi hatásvizsgálatot végez minden új folyamat esetében amik kockázatosak lehetnek a személyes adatokra nézve.

KÖVETKEZTETÉSEK ÉS AJÁNLÁSOK

Az adatszegésekre kiemelt figyelem irányul, így eljött az ideje, hogy a szervezetek azonosítsák és védjék az összes személyes adatot, és a GDPR-nak való megfelelés irányába lépéseket tegyenek - ennek elmulasztása jelentős üzleti kockázatokat eredményez. Mi több, a megfelelésre és a szabványokra épülő keretek betartása végső soron segítheti a szervezetet, hogy vonzóbb és biztonságosabb színben tűnjön fel ügyfelei szemében.

A GDPR esetében a megfelelést a szervezetnek kell bizonyítania, hogy megtette a megfelelő intézkedéseket a rendelet elveinek és elvárásainak követése tekintetében.
A szervezetnek gondoskodnia kell az általa és adatfeldolgozó partnerei által kezelt személyes adatok biztonságáról.

Mi az alábbi 4 lépcsős megközelítést javasoljuk a GDPR megfelelőssége érdekében elvégezni:

1. Fedezze fel és osztályozza az összes személyes adatot. (adatvagyonleltár)
2. Hozzon létre egy "tervet" az összes azonosított védelmi szabályozási hiány megszüntetéséhez.
3. "Minden adat" védelme a megfelelő biztonsági ellenőrzések kidolgozása és végrehajtása révén.
4. "Biztonsági ellenőrzések növelése"