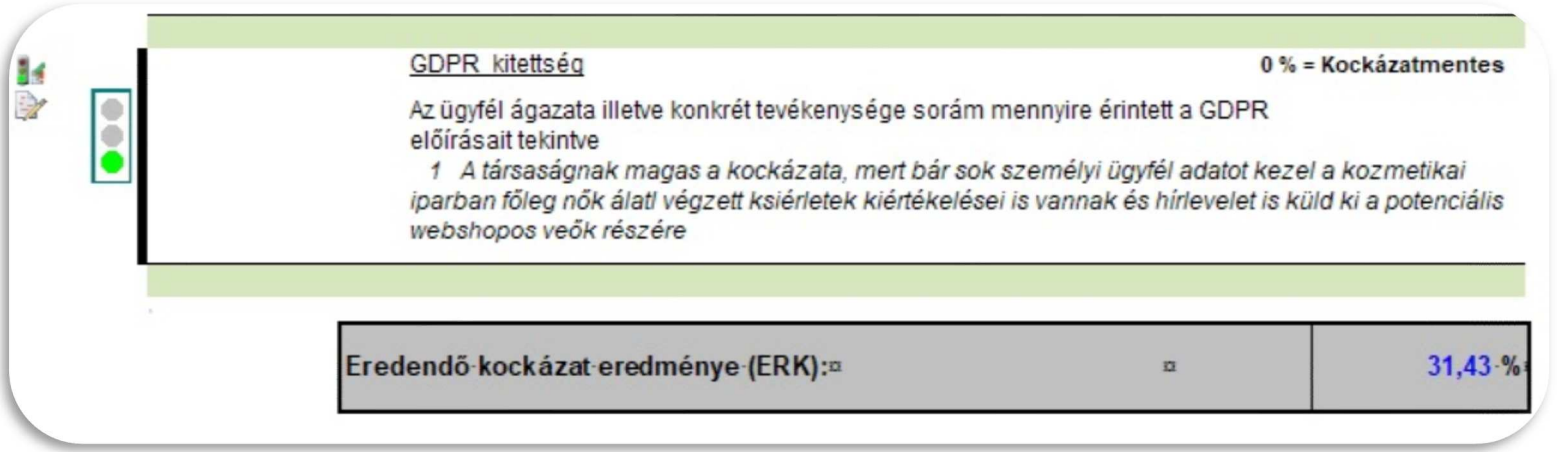
Esettanulmány I.

Egy parfümöket gyártó üzem reklámüzeneteinek küldése e-mail-hírlevélben

- Védelmi igény: közepes
  Az e-mail-címek nyilvánosságra kerülése ugyan nem lenne kívánatos az érintettek számára, de fenyegető sem. Más lenne azonban a helyzet, ha az Anonim alkoholisták csoportjának hírleveléről lenne szó.
- Incidens bekövetkezés valószínűsége: átlagosnál magasabb
  Harmadik felek részéről érdeklődés áll fenn, de ez nem rendkívül magas, várhatóan hekker támadást nem intéznek e miatt, de hírlevél adatok titkosítása elmaradt és a belsők számára történő felhasználást nem szabályozták
- Abból kell kiindulni, hogy nem kell végrehajtani hatástanulmányt

GDPR előtt

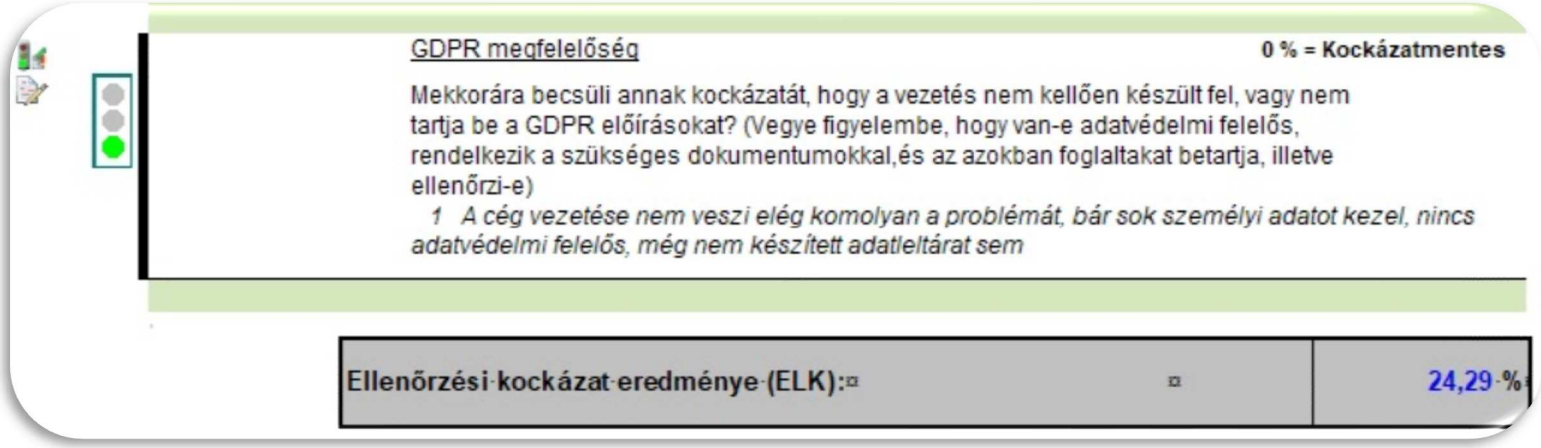


GDPR kitettség — 0 % = Kockázatmentes

Az ügyfél ágazata illetve konkrét tevékenysége sorám mennyire érintett a GDPR előírásait tekintve

1 A társaságnak magas a kockázata, mert bár sok személyi ügyfél adatot kezel a kozmetikai iparban főleg nők álatl végzett ksiérletek kiértékelései is vannak és hírlevelet is küld ki a potenciális webshopos vevők részére

Eredendő kockázat eredménye (ERK):	31,43 %



GDPR megfelelőség — 0 % = Kockázatmentes

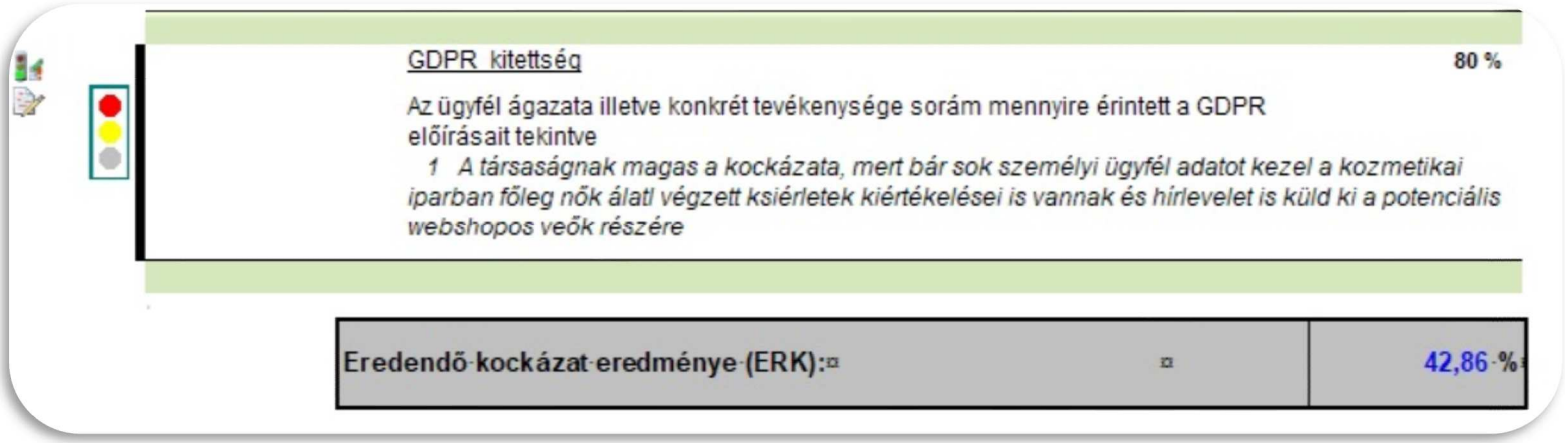
Mekkorára becsüli annak kockázatát, hogy a vezetés nem kellően készült fel, vagy nem tartja be a GDPR előírásokat? (Vegye figyelembe, hogy van-e adatvédelmi felelős, rendelkezik a szükséges dokumentumokkal,és az azokban foglaltakat betartja, illetve ellenőrzi-e)

1 A cég vezetése nem veszi elég komolyan a problémát, bár sok személyi adatot kezel, nincs adatvédelmi felelős, még nem készített adatleltárat sem

Ellenőrzési kockázat eredménye (ELK):	24,29 %

Meghatározott feltárási kockázat (DR) (Vizsgálati kockázat (AR) / Hibakockázat (IR x CR)): → → → → **AR (3,44 %)** → **DR** → = → ---------- → **x 100** → **IR (24,29 %) x CR (24,29 %)** A mostani kockázatértékeléssel az **"Eredendő kockázat"** és az **"Ellenőrzési kockázat"** területén **94,10%-os** vizsgálati biztonság biztosított az éves beszámoló esetében. A **96,56%-os vizsgálati biztonság** eléréséhez **maximum 58,34%-os feltárási kockázat** megengedett.	**58,34 %**

GDPR után

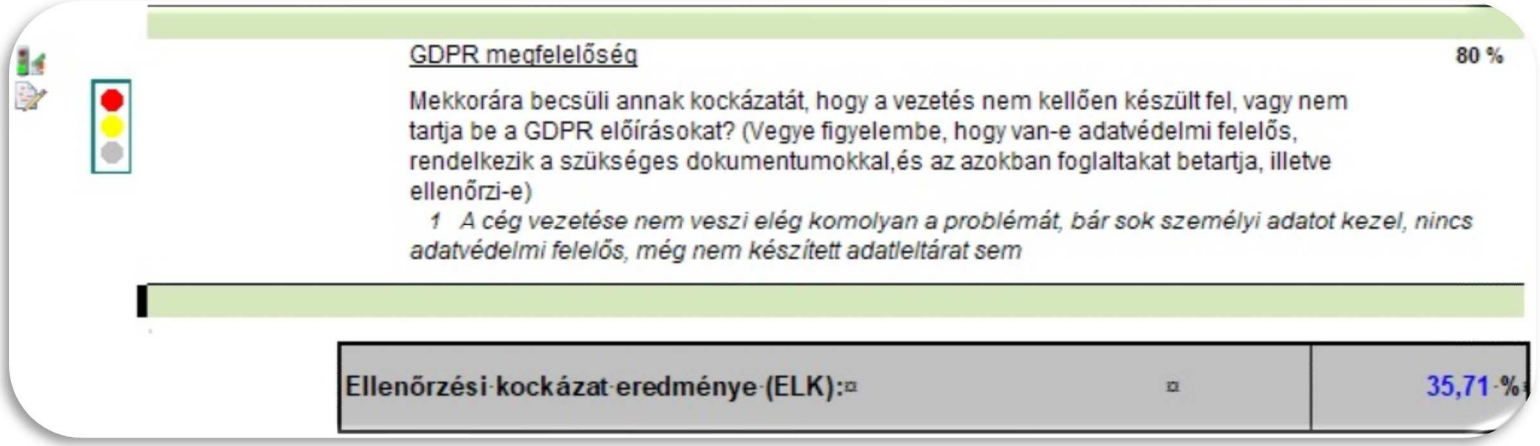


GDPR kitettség 80 %

Az ügyfél ágazata illetve konkrét tevékenysége sorám mennyire érintett a GDPR előírásait tekintve

1 A társaságnak magas a kockázata, mert bár sok személyi ügyfél adatot kezel a kozmetikai iparban főleg nők álatl végzett ksiérletek kiértékelései is vannak és hírlevelet is küld ki a potenciális webshopos veők részére

Eredendő kockázat eredménye (ERK):	42,86 %



GDPR megfelelőség 80 %

Mekkorára becsüli annak kockázatát, hogy a vezetés nem kellően készült fel, vagy nem tartja be a GDPR előírásokat? (Vegye figyelembe, hogy van-e adatvédelmi felelős, rendelkezik a szükséges dokumentumokkal,és az azokban foglaltakat betartja, illetve ellenőrzi-e)

1 A cég vezetése nem veszi elég komolyan a problémát, bár sok személyi adatot kezel, nincs adatvédelmi felelős, még nem készített adatleltárat sem

Ellenőrzési kockázat eredménye (ELK):	35,71 %

Meghatározott feltárási kockázat (DR)¶ (Vizsgálati kockázat (AR) / Hibakockázat (IR x CR)):¶ ¶ ¶ → → → → **AR (3,44 %)**¶ → **DR** → = → ---------- → **x 100**¶ → **IR (35,71 %) x CR (35,71 %)**¶ A mostani kockázatértékeléssel az **"Eredendő kockázat"** és az **"Ellenőrzési kockázat"** területén **87,25%-os** vizsgálati biztonság biztosított az éves beszámoló esetében.¶ A **96,56%-os vizsgálati biztonság** eléréséhez **maximum 26,97%-os feltárási kockázat** megengedett.	**26,97 %**

Következmény: jóval magasabb szintű rendszer és elemző vizsgálat, illetve több egyedi vizsgálat szükséges, magasabb a minta mértéke

Esettanulmány II

Példa: e-kereskedőként ügyfelei törzsadatait, elérhetőségeit, banki adatait és fizetési viselkedését tárolja.

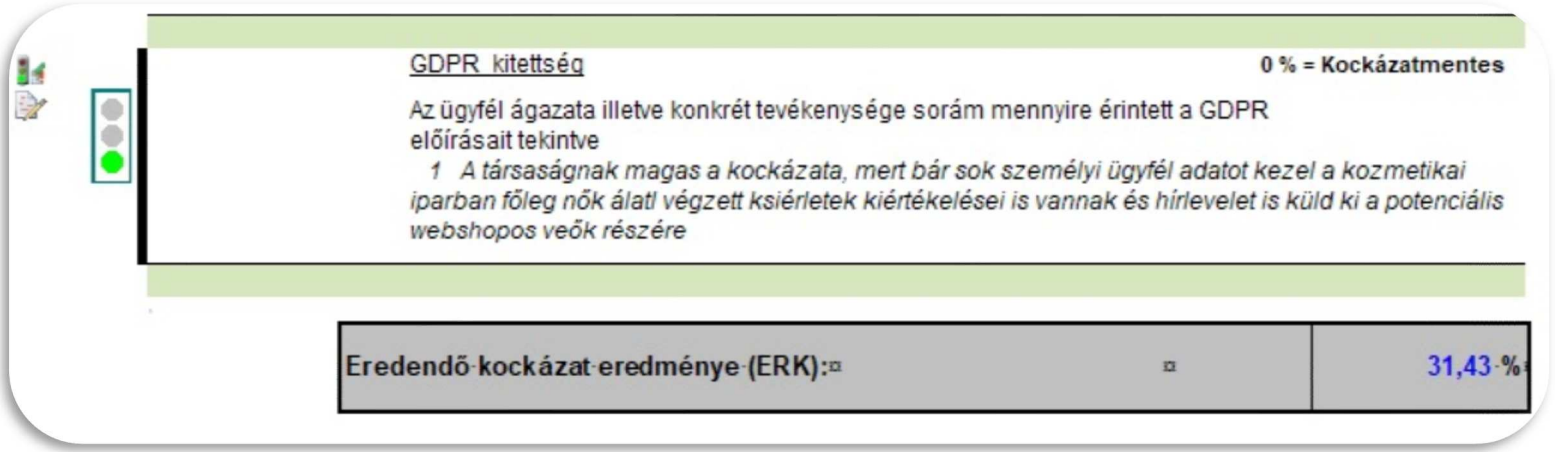
Az ügyfelek adatainál, törzsadatainál és elérhetőségeinél csekély kockázatú (B) adatokról van szó, ezért nem kell velük kapcsolatban a bővített kockázatelemzéssel foglalkozni.

Ehhez először például a következő kockázatokat kell azonosítani:

– Adatlopás idegenek által
– Adatokon keresztül lopás saját dolgozók által
– Adatvesztés a vállalaton belüli hanyag kezelés következtében
– Adatvesztés technikai hibák következtében…

E kockázatok a kiemelten jó biztonsági rendszer és a GDPR-ra kidolgozott szabályzatok és ellenőrzés miatt alacsony szinten tarthatók, ezt igazolja az elvégzett hatástanulmány is

GDPR előtt

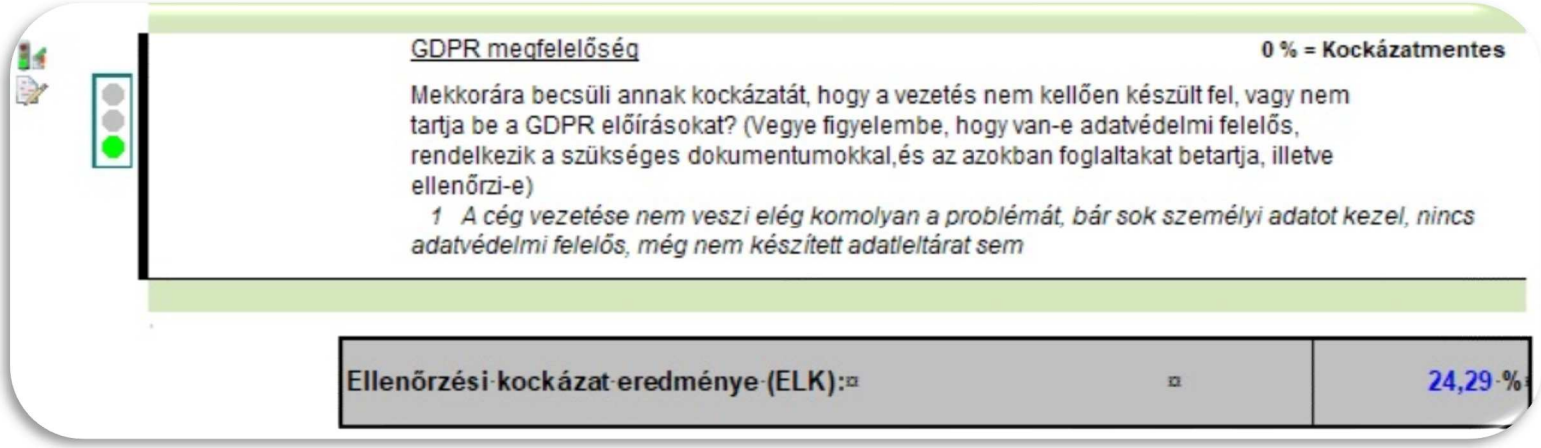


GDPR kitettség — 0 % = Kockázatmentes

Az ügyfél ágazata illetve konkrét tevékenysége sorám mennyire érintett a GDPR előírásait tekintve

1 A társaságnak magas a kockázata, mert bár sok személyi ügyfél adatot kezel a kozmetikai iparban főleg nők álatl végzett ksiérletek kiértékelései is vannak és hírlevelet is küld ki a potenciális webshopos vevők részére

Eredendő kockázat eredménye (ERK):	31,43 %



GDPR megfelelőség — 0 % = Kockázatmentes

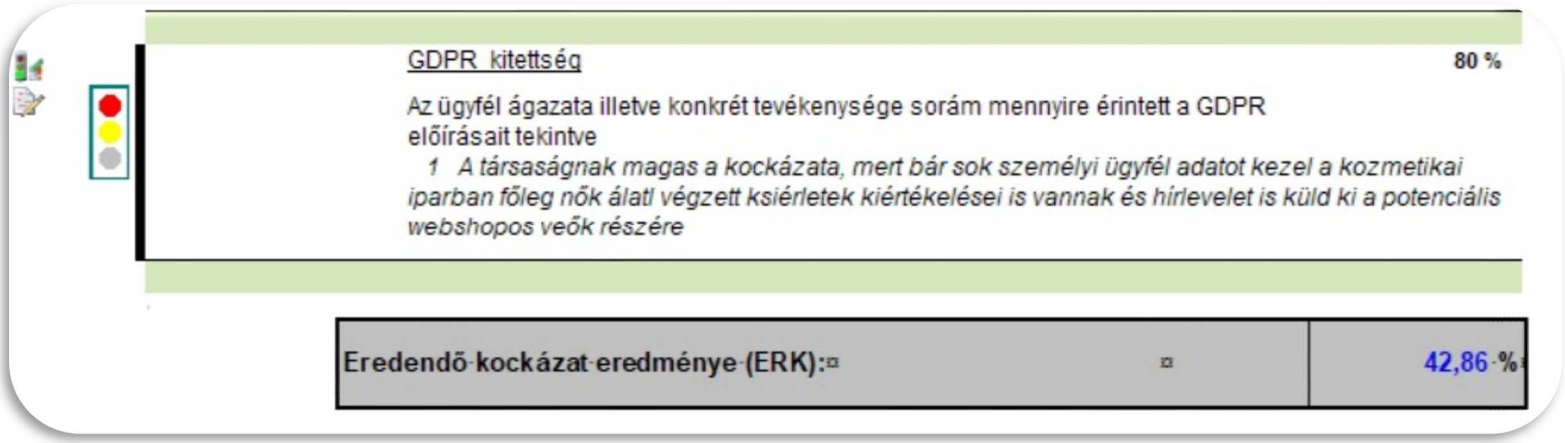
Mekkorára becsüli annak kockázatát, hogy a vezetés nem kellően készült fel, vagy nem tartja be a GDPR előírásokat? (Vegye figyelembe, hogy van-e adatvédelmi felelős, rendelkezik a szükséges dokumentumokkal,és az azokban foglaltakat betartja, illetve ellenőrzi-e)

1 A cég vezetése nem veszi elég komolyan a problémát, bár sok személyi adatot kezel, nincs adatvédelmi felelős, még nem készített adatleltárat sem

Ellenőrzési kockázat eredménye (ELK):	24,29 %

Meghatározott feltárási kockázat (DR) (Vizsgálati kockázat (AR) / Hibakockázat (IR x CR)): $DR = \frac{AR\ (3{,}44\ \%)}{IR\ (24{,}29\ \%)\ x\ CR\ (24{,}29\ \%)} \rightarrow x\ 100$ A mostani kockázatértékeléssel az **"Eredendő kockázat"** és az **"Ellenőrzési kockázat"** területén **94,10%-os** vizsgálati biztonság biztosított az éves beszámoló esetében. A **96,56%-os vizsgálati biztonság** eléréséhez **maximum 58,34%-os feltárási kockázat** megengedett.	**58,34 %**

GDPR után

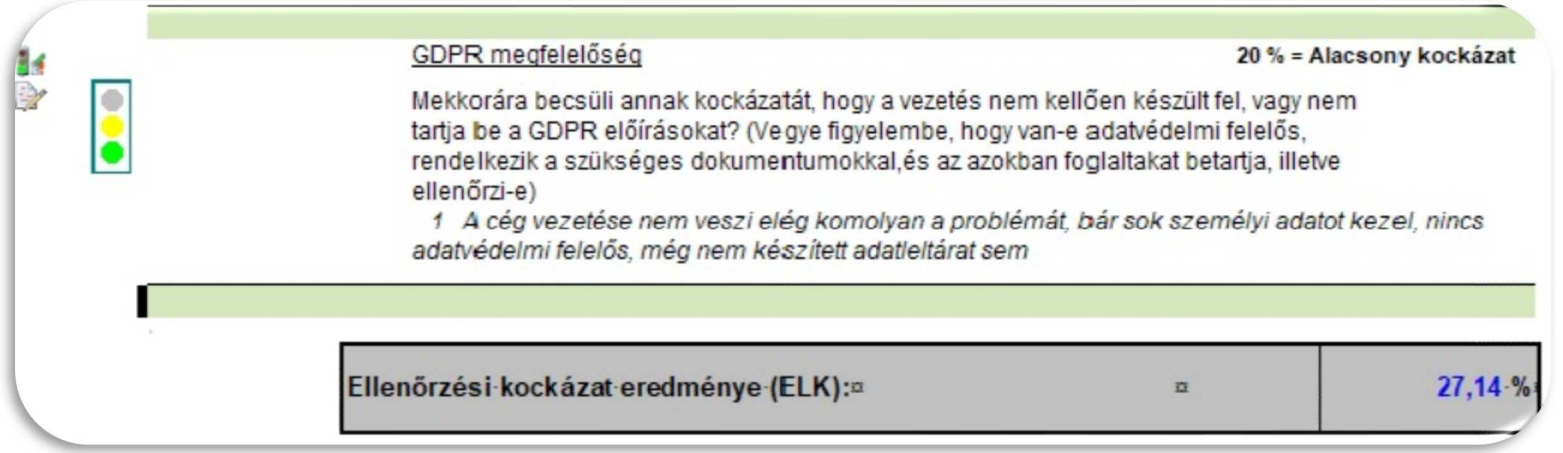


GDPR kitettség 80 %

Az ügyfél ágazata illetve konkrét tevékenysége sorám mennyire érintett a GDPR előírásait tekintve

1 A társaságnak magas a kockázata, mert bár sok személyi ügyfél adatot kezel a kozmetikai iparban főleg nők álatl végzett ksiérletek kiértékelései is vannak és hírlevelet is küld ki a potenciális webshopos veők részére

Eredendő kockázat eredménye (ERK):	42,86 %

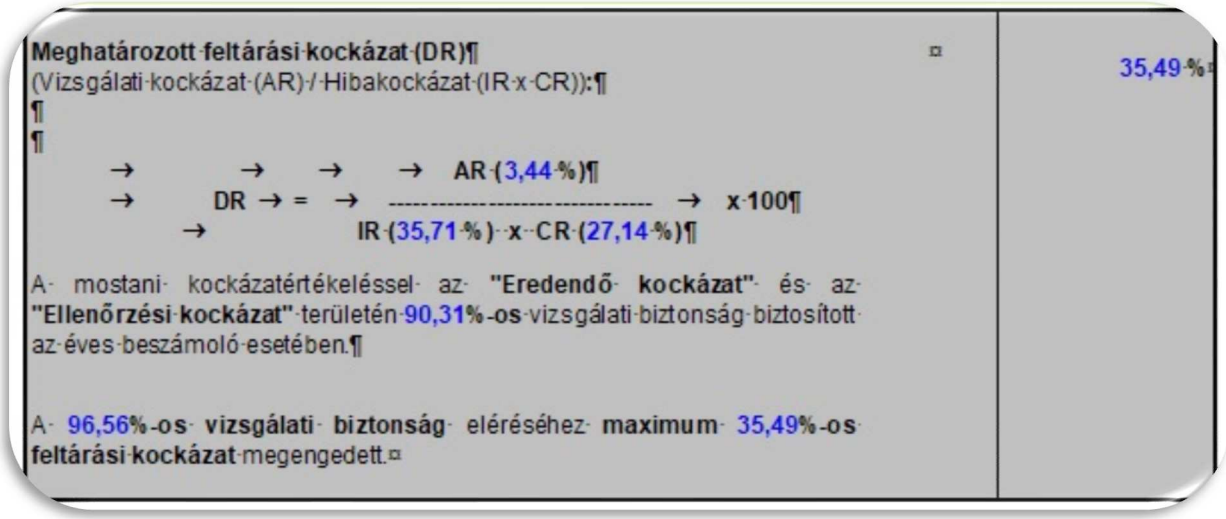


GDPR megfelelőség 20 % = Alacsony kockázat

Mekkorára becsüli annak kockázatát, hogy a vezetés nem kellően készült fel, vagy nem tartja be a GDPR előírásokat? (Vegye figyelembe, hogy van-e adatvédelmi felelős, rendelkezik a szükséges dokumentumokkal,és az azokban foglaltakat betartja, illetve ellenőrzi-e)

1 A cég vezetése nem veszi elég komolyan a problémát, bár sok személyi adatot kezel, nincs adatvédelmi felelős, még nem készített adatleltárat sem

Ellenőrzési kockázat eredménye (ELK):	27,14 %



Következmény: jóval magasabb szintű rendszer vizsgálat kell, illetve csak valamivel kell több egyedi vizsgálat

[Lessons learned.pdf]

Adatáramlások kockázatalapú értékelése az adatvédelemre gyakorolt hatásokat értékelő, jól megtervezett folyamat (PIA = Protection Impact Assessment) azaz hatástanulmány alapján

Adatáramlások	Adatáramlás kockázatértékelése	A kockázat romboló hatásának meghatározása	Adatáramlások rangsorolása	Hatástanulmány végrehajtása	Intézkedések meghatározása
A titoktartási és megfelelőségi kockázatok teljes körű értékeléséhez tudni kell, hogyan használják fel a (vevői és dolgozói) adatokat. Ezért az adatvédelemre gyakorolt hatásokat értékelő saját folyamatunk egyrészt az adatáramlások listájának elkészítéséből áll, mely lista teljes áttekintést ad az adatokat tároló adatforrásokról (rendszerekről és fájlokról), hogyan történik az adatok feldolgozása, kikkel osztjuk meg, és meddig őrizzük meg őket. Az adatforrások leltárba vétele a belső vezetők részvételével megtartott (+/- kétórás) workshop keretében	Az adatvédelemre gyakorolt hatásokat értékelő folyamat második lépésében az adatforrásokat a kapcsolódó kockázatok szerint kategóriákba (magas, közepes, alacsony) soroljuk. Az ilyen kockázatértékelés – ami egy (rövid) kérdőívből áll – segíti a szervezeteket adatáramlásaik rangsorolásában, és annak megállapításában, hogy a GDPR alapján kötelező-e a hatásértékelés, és erre vonatkozóan létrehozza a vizsgálati keretet. A kockázatértékelés tárgyát többek között az alábbiak képezik: - személyes adatok	Az adatáramlásokról összegyűjtött információk alapján a GDPR miatt várt módosítások alátámasztására meg kell határozni a kockázat romboló hatását, rangsorolni kell az adatáramlásokat, és meg kell határozni az intézkedéseket. Külső tanácsadó támogatást nyújt (1) a titoktartási kockázatot tartalmazó minőségi jelentés elkészítésében és (2) a mérhető romboló hatásra vonatkozó, egyúttal a vállalati stratégiába illeszkedő jelentés összeállításában, valamint (3) a saját titoktartási kockázatot kontrolláló keretrendszerből levezetett mé-	A kockázat szervezetre gyakorolt, meghatározott mértéke és az egyes adatáramlásokra megállapított kockázat(ok) alapján kijelöljük, hogy mely adatáramlásokra kell a hatástanulmányt elkészíteni, valamint hogy az értékeléseket milyen sorrendben célszerű végrehajtani. Legelőször azokra az adatáramlásokra hajtjuk végre, amelyek leginkább befolyásolják a szervezetet – az adott kockázat romboló hatása alapján.	Külső tanácsadó kidolgozott egy részletes Excel-táblát az adatáramlásoknak az érintett természetes személyekre gyakorolt hatásának értékeléséhez szükséges kérdőív alapján. Ez a kérdőív lefedi a GDPR legtöbb elemét (a kockázatértékelésnél átfogóbb), és főleg zárt végű kérdéseket (igen/nem, több lehetséges válasz, értékelő skála stb.) tartalmaz, és így felhasználóbarát eszközzé teszi a PIA-értékelést a vállalkozás számára. Igény esetén a PIA-kérdőív módosítható vagy integrálható meglévő kockázatértékelésekkel (pl. BIA vagy ISRA).	A PIA-értékelés végrehajtásán túl meghatározzuk a PIA-értékelés során megaállapított természetes személyekre gyakorolt kockázatok mérsékléséhez szükséges intézkedéseket is. Ezután ezt az intézkedési listát felosztjuk a kockázatok szervezetre gyakorolt romboló hatása alapján, és először a legmagasabb kockázatokat mérsékeljük.

történik. Adatáramlási eszközeink segítségével érvényesíthetők a workshop eredményei.	- speciális adatok - adatvolumen - a folyamat érzékenysége	rőszámok meghatározásában, ami tájékoztat a kockázat vállalatra gyakorolt romboló hatásáról, és ahol lehet, illeszkedik a stratégiai célokhoz.			

[the_accountatnts_gdpr_toolkit.pdf 6-7. oldal]

A könyvelő GDPR intézkedési terve

Mit tehet most a felkészülés érdekében

- **Elindulás**: Szervezetének mostanra már el kellett kezdenie a GDPR irányelvnek való megfeleléssel kapcsolatos munkát. Kezdjen neki a lehető leghamarabb, mert a megfelelőség eléréséig az út sok időt vesz igénybe.

- **Adatvédelmi felelős** (DPO = Data Protection Officer) **kiválasztása**: Az adatvédelmi felelős kijelölése jogszabály által előírt kötelezettség. Gondosan mérlegelni kell, hogy melyik dolgozót nevezik ki erre a feladatra és annak végrehajtására, ill. végrehajtatásra. Például az összes dolgozónak tudnia kell, kinek jelezze első körben az adatokhoz kapcsolódó szabályszegéseket.

- **Vállalati adatok szétválasztása**: Nagy mennyiségű adatot kezelő szervezetként a könyvelőirodáknak ismerniük kell a birtokukban lévő és általuk kezelt adatokat. Ennek keretében különbséget kell tenniük a személyes adatok, az ügyféladatok és a dolgozói adatok között, valamint ezek megszerzési módjai között. Ennek egyik lehetséges módszere, hogy teljes körűen dokumentálja az iroda a vállalkozás birtokában lévő információkat, megadja, ezek honnan származnak, hol és hogyan történik a tárolásuk, hogyan dolgozza fel őket, és kikkel osztja meg azokat például. Olyan adatok tartoznak ide, mint az elérhetőségek vagy az üzleti bankszámlával kapcsolatos információk.

- **Vállalati adatok kezelése**: a vállalkozásoknak megfelelően kell kezelni adataikat, ami azt jelenti, hogy legyenek könnyen törölhetők az adatok teljes mértékben az összes rendszerből és biztonsági mentésből az elfelejtéshez való jognak megfelelően, kérésre adatokat kell tudni szolgáltatni a vállalkozás birtokában lévő adatokról, tudni kell, hogyan használják fel ezeket az adatokat, és ismerni kell a magánszemélyek saját adataikra vonatkozó jogait.

- **Vállalati eljárások aktualizálása**: a vállalkozásoknak aktualizálni kell a ’mondj el mindent, mondd gyorsan és mondd az igazat’ elv megsértésének feltárására és jelentésére vonatkozó eljárásaikat. Ezen kívül felszólíthatják a vállalkozást az adatvédelemre gyakorolt hatások értékelésére (DPIA = Data Privacy Impact Assessment). A legjobb gyakorlat szerint teljes körű DPIA hajtandó végre a magas kockázatú feldolgozási tevékenységekre vonatkozóan. Ilyen például, ha a feldolgozó tevékenység az ügyféladatok védelmére vonatkozó szabály megsértésének magas kockázatát eredményezheti.

- **Adatok vizsgálata**: a vállalkozás személyes adatok kezelésére vonatkozó jelenlegi gyakorlatának alapos felülvizsgálata jó módszer arra, hogy megértsük, mit kell tenni a GDPR érdekében. Ez magában foglalja a DPIA-értékelés végrehajtását, a titoktartással kapcsolatos feljegyzések és levelezés áttekintését, annak ellenőrzését, hogy a személyes adatokat védő meglévő folyamatok biztonságosak-e, és hogy vállalkozásunk teljesíti-e a magánszemélyek jogait. Ez azt jelenti, hogy az adatok formátuma biztosítja a más adatfeldolgozónak való könnyű továbbíthatóságot (adatok hordozhatóságát). A cégeknek azt is át

kell tekinteniük, hogyan keresik meg a magánszemélyeket, hogy megszerezzék hozzájárulásukat adataik felhasználásához, és hogyan kezelik ezeket a hozzájárulásokat.

- **A vállalati kiber-tér védelmének áttekintése:** értékelni kell a jelenlegi kiber-biztonsági módszereket, mert előfordulhat, hogy ezek is tökéletesítésre szorulnak.

- **Meglévő standardok vizsgálata**: a GDPR-ra való felkészülés nem feltétlenül jelenti azt, hogy ezt nulláról kell kezdeni, értékelheti a már meglévő biztonsági előírásokat, hogy némi előnyre tegyen szert, mielőtt a megfelelőség egyéb részletei ismertté válnak. A biztonsági előírások jelenthetnek ISO-szabványokat, például a személyes azonosításra alkalmas adatokra vonatkozó 27018-as szabvány vagy az információbiztonság kezelésére vonatkozó 27001-es szabvány.

- **Teljes vállalkozásra kiterjedő megközelítés**: fontos, hogy az előírásokat a vállalat egészében alkalmazni kell, mert az ügyfelek érdeklődhetnek olyan részletek felől, hogy mit tesznek önök a megfelelés érdekében. Felkészültségével a vállalkozás azt közvetíti ügyfelei felé, hogy komolyan veszi a GDPR-ra való felkészülést, és ezzel a vállalat professzionalizmusát tudja demonstrálni. Az ügyfeleket tájékoztatni kell arról, illetve emlékeztetni kell arra, hogy nekik is vannak a GDPR-hoz kapcsolódó kötelezettségeik.