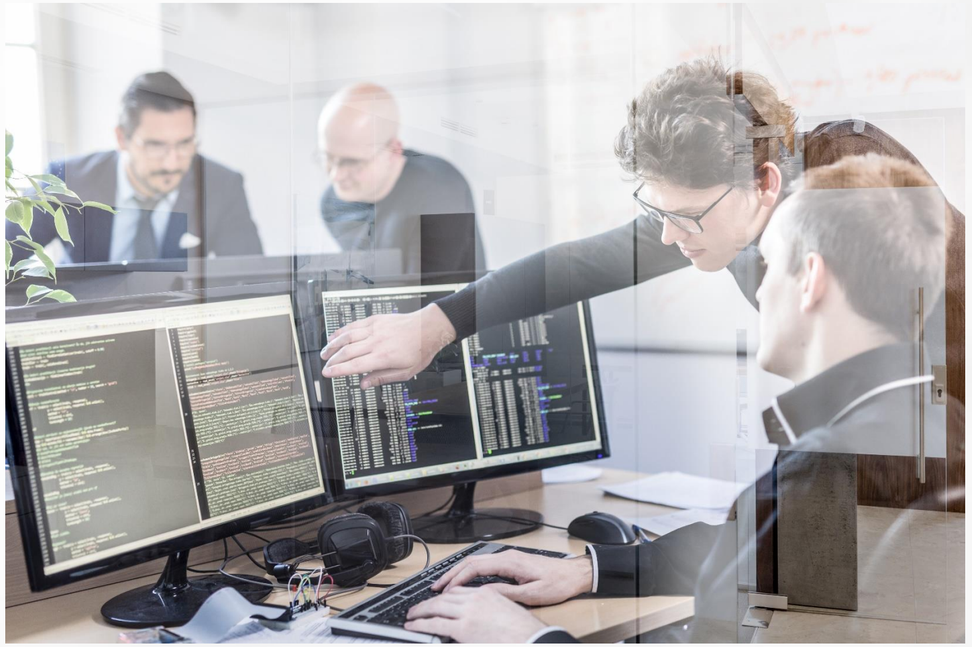
COLONNADE
A FAIRFAX COMPANY

CYBER
GDPR ADATVÉDELMI
FELELŐSSÉGBIZTOSÍTÁS

INFORMÁCIÓBIZTONSÁG

- Az információ és az információs rendszerek világában az **adatvédelmi kockázatok új kihívást jelentenek**. A vállalatok irodai eszközökön és felhőben tárolják adataikat, mobileszközökön is hozzáférnek ezekhez, interneten keresztül jutunk szolgáltatásokhoz.



- Az emberi hibákon kívül váratlan események is jelentkezhetnek, (**hackelés, vírus, mobileszközlopás** stb.) amely kapcsán nem csupán a partnereik érvényesíthetnek adatszivárgás miatt igényt, de saját cégük is komoly anyagi veszteséget szenvedhet el.

A cégek ilyen jellegű kockázataira kínáljuk innovatív biztosítási termékeinket:
GDPR és Cyber adatvédelmi felelősség biztosításunkat.

AZ ADATVÉDELMI FELELŐSSÉG - ALAPJA A GDPR

- **Személyes adataink feletti önrendelkezést** erősíti a GDPR.

- Az adat kezelője, feldolgozója, továbbítója minden esetben köteles betartani a vonatkozó jogszabályokat, az adatok **jogszerű összegyűjtésétől** kezdve egészen az **adatalanyok** adatsértéssel kapcsolatos **jogainak gyakorlásának** biztosításáig.

- Az adatalanyok **panaszt tehetnek az adatvédelmi hatóság felé**, amennyiben úgy gondolják, hogy az adataik védelemével kapcsolatos jogaik sérültek.

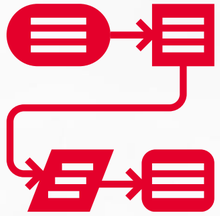
- **Kárigénnyel** léphetnek fel a felelőssel szemben (vagyoni kár, sérelemdíj)

- A cégeket ezeken túl a törvényben vagy szerződésben meghatározott **titoktartási kötelezettség** is terhelheti, amelyek megsértésével szintén jelentős károkat okozhatnak üzleti partnereiknek.

ADATVÉDELMI ÉS KIBERKOCKÁZATOK

COLONNADE
A FAIRFAX COMPANY

DÖNTÉSI HIBÁK
vezetők, szakértők, adatvédelmi tisztviselők, alkalmazottak által hozott rossz döntések



FOLYAMATHIBÁK
a céges rendszer használata során: a védelem, jelszavak, e-mailek, hozzáférések, adatok szabályellenes továbbítása

TECHNIKAI PROBLÉMÁK
személyes adatok, bizalmasan kezelendő információk közzététele

EMBERI HIBÁK
dolgozói hanyagság, outsourcing tevékenység, (volt) munkatárs bosszúja

MULASZTÁSOK
incidensek bejelentésének és az ilyenkor szükséges további intézkedések elmulasztása

HACKELÉS, MOBILESZKÖZ-LOPÁS
szolgáltatás megtagadási támadás, szoftver, kód vírus általi módosítása, blokkolása, az adatokhoz történő jogosulatlan hozzáférés

KIKNEK AJÁNLJUK A BIZTOSÍTÁST?

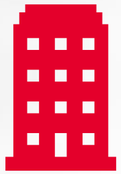
COLONNADE
A FAIRFAX COMPANY

Szektorálisan és tevékenységtől függetlenül bármely kis, közepes és nagyvállalatnak:

- ahol **személyes és/vagy vállalati adatokat kezelnek a cég GDPR szerinti felelőssége felmerül**. (még akkor is javasolt, ha adatvédelmi tisztviselő és IT biztonsági szakember működik közre) A munkavállalói adatok kezelése is ide tartozik!
- amelyek **működését az informatikai háttér** határozza meg – pl. irodai működés, termelést, irányítás, ügyfélforgalom, bármely szolgáltatás, rendelkezésre-állás- illetve ahol a külső/belső adatok és információk az IT biztonsági rendszer sérülékenységéből adódóan nyilvánosságra kerülhetnek
- amelyekre az adatvesztés/ helyreállítás, incidens felszámolása, egy esetleges bírság **komoly anyagi terhet ró,** vagy náluk reputáció-csökkenés, ügyfélvesztés következhet be
- ahol az adatbázisok, online platformok elérhetetlensége a működést vezérlő informatika működésképtelensége miatt az **üzletmenet megszakad** és a kialakult helyzet gyors orvoslásán a vállalat hosszútávú életben maradása múlik

Bármely működés veszélyeztetett!

KIKNEK AJÁNLJUK A BIZTOSÍTÁST?



KISEBB CÉGEK

- Mivel egy incidens esetén nem tudnak mozgósítani azonnal szakembereket, a folyamataik nincsenek a krízishelyzetre felkészítve.
- Az anyagi következmények felemészthetik a cég tartalékait.

NAGYOBB CÉGEK

- Mivel a cégcsoport összefüggő IT rendszereit, közös tárhelyét ért támadás azonos időben állítja a céget/cégcsoportot/nemzetközi hálózatot egy váratlan krízishelyzet elé.
- Az állapot felszámolása, a rendszer és adatok visszaállítása idő és költségigényes.

GDPR ADATVÉDELMI FELELŐSSÉGBIZTOSÍTÁS ELEMEI I.

I. FELELŐSSÉGI FEDEZET
(MÁSNAK OKOZOTT KÁROK)

- **Adatfelelősség:** valamely cselekmény, tévedés, mulasztás a Személyes és Vállalati adatok nem megfelelő kezelése kapcán
- **Kiszervezett tevékenységre vonatkozó fedezet:** amennyiben az adatkezelő kiszervezi az adatfeldolgozást (pl. archiválás, call center, ügyfélszolgálat, adatrögzítés, adattárolás stb)
- **Hálózatbiztonsági fedezet:** a kár abból származik, hogy a Biztosított tévedése, vagy mulasztása miatt
  - az informatikai rendszert támadás éri (kód, vírus, módosító szoftver által) és ez a szoftverekben, adatokban sérülést okoz;
  - az adatok hozzáférhetetlenné válnak a jogosult részére;
  - hozzáférési kódhoz jut illetéktelen személy; módosulnak, megsemmisülnek, törlődnek az adatok;
  - az adattároló eszközt ellopják vagy elveszítik; az adatok nyilvánosságra kerülnek

A biztosító fizeti a károsult (adatalany, vagy üzleti partner) ténylegesen felmerülő vagyoni kárát, sérelemdíjat, az ügy vizsgálatához szükséges szakértői költséget, jogi védekezés költségét.

GDPR ADATVÉDELMI FELELŐSSÉGBIZTOSÍTÁS ELEMEI II.

II. EGYÉB KÖLTSÉGEK, BÍRSÁG

- **Adatkezeléssel kapcsolatos vizsgálatok**

  Hivatalos vizsgálatnál felmerülő jogi tanácsadás költségei és jogi képviselettel kapcsolatos szakértői díjak

- **Adatkezeléssel kapcsolatos bírságok**

  Biztosítónk kifizeti az adatvédelmi jogszabályok megsértése miatt indult hivatalos vizsgálat eredményeként kiszabott bírságot

- **Értesítési költségek**

  A Biztosító a biztosított részére vagy nevében kifizet minden olyan szakértői díjat, amely az adatalanyok és/vagy bármely illetékes szabályozó hatóság kötelező értesítéséhez kapcsolódik az adatvédelmi jogszabályok tényleges vagy állítólagos megsértése miatt.

CYBER ADATVÉDELMI FELELŐSSÉGBIZTOSÍTÁS ELEMEI I.

COLONNADE
A FAIRFAX COMPANY

I. TELJES GDPR FEDEZET (AZ ELŐZŐEKBEN ISMERTETETT SZERINT)

II. EGYÉB SZAKÉRTŐI DÍJAK

- **Proaktív szakértői** szolgáltatások
- A **Társaság és Magánszemély jó hírnevének védelme**: független PR tanácsadó által
- **Elektronikus adatok (helyreállítás)** Az elveszett elektronikus adatok helyreállításával, ismetelt összegyűjtésével vagy újraelőállításának lehetőségeivel kapcsolatos - szakértői vizsgalatok és azok helyreállításával, újraelőállításával kapcsolatos költségek

III. OPCIONÁLIS KITERJESZTÉSEK

- **Multimédia felelősség** (digitális médiatartalmak): Fedezi a harmadik fél szellemi tulajdonával kapcsolatos jogok megsértéséből, vagy valamely elektronikus tartalommal kapcsolatos gondatlanságból eredő karteritest, es az ezekkel kapcsolatos jogi védekezés költséget.
- **Zsarolás:** Az adatbiztonsági fenyegetés megszüntetése érdekében a zsaroló részére kifizetett váltságdíj és szakértői költségek
- **Hálózatkiesés:** A rendszerbe történő illetéktelen behatolás miatt jelentkező rendszerkiesésből eredő üzemszüneti vesztességek (akár egy hacker, vírus vagy Denial of Service támadás okozta)

CYBER ADATVÉDELMI FELELŐSSÉGBIZTOSÍTÁS ELEMEI II.

COLONNADE
A FAIRFAX COMPANY

	B2) Adatkezeléssel kapcsolatos bírságok:	*a kártérítési limit 25%-a*
	C1) Proaktív szakértői szolgáltatások	*a kártérítési limit 25%-a*
	C2) A társaság jó hírnevének védelme	*a kártérítési limit 25%-a*
	C3) Magánszemély jó hírnevének védelme	*a kártérítési limit 25%-a*
	C4) Adatalanyok értesítése	*a kártérítési limit 25%-a*
	C5) Elektronikus adatok	*a kártérítési limit 25%-a*
6. Opcionális kiterjesztések:	**D) Multimédia felelősség** / az éves díj 10%-a	*nincs fedezetben / a kártérítési limit 25%-a*
	E) Zsarolás / az éves díj 15%-a	*nincs fedezetben / a kártérítési limit 25%-a*
	F) Hálózatkiesés / az éves díj 25%-a	*nincs fedezetben / a kártérítési limit 25%-a*

Figyelem! A feltüntetett éves díj az opcionális kiterjesztés pótdíjait még nem tartalmazza!

7. Általános önrészesedés:	10%, min.	2.500.000 Ft	/ káresemény
	20 %, min. 5.000.000 Ft / káresemény az "E) Zsarolás" fedezet vonatkozásában		
Hálózatkiesés:	várakozási idő 12 óra, min. 5.000.000 Ft / káresemény		
8. Éves díj:	**1. opció**	**2.995.849 Ft**	
	2. opció	**4.185.995 Ft**	
	3. opció	**5.512.786 Ft**	
Díjfizetés:	**Éves díjfizetés**		
9. Visszamenőleges hatály:	A kockázatviselés kezdete		
10. Függelék:	„Log4j" vagy „Log4shell" (CVE-2021-44228) kizárás		

A GDPR ÉS CYBER ADATVÉDELMI BIZTOSÍTÁS VÁLLALÁSA

COLONNADE
A FAIRFAX COMPANY

- A biztosítás nem helyettesíti a GDPR megfelelést, az csak a felkészülés után fennálló maradékkockázatok kezelésére szolgál! Csak ***tudatosan felkészült*** cégeke köthető a biztosítás- szerződéskötéskor nyilatkozatot kérünk a dokumentált GDPR elvárás teljesítéséről, jelen állapotáról.
- **Díjindikációt** adunk a **cég alapadatai**, tevékenysége, árbevétele alapján. A díjazás még függ a kezelt adatok volumenétől, érzékenységétől, területi hatálytól, kiszervezett tevékenységtől.
- ***Kérdőív kitöltése szükséges:*** felhőszolgáltatás, média, pénzintézetek, egészségügy, közművek, állami, önkormányzati szervek esetén, 10 mrd. Ft árbevétel és 500 mió Ft limit felett
- A cégek nagyságrendjéhez igazított **kártérítési limiteket** adunk, a bírság összegét szublimitáljuk
- Már folyamatban levő ügyekre nem lehet biztosítást kötni, a **kárelőzményről** nyilatkozni kell, de nem kizárt!
- Szakmai + Cyber/adatvédelmi fb. **kombinált** szerződés: közös limit, kedvező díj.
- **Cégcsoportra együttesen** is köthető szerződés, a cégeknek külön kell megfelelniük!
- **„Virtuális Védőháló”** termék: mini Cyber, alacsony limitekkel, instant ajánlattal. Teljes dokumentáció (marketinggel) rendelkezésre áll!
- **Colonnade vagyonbiztosításhoz kiegészítő Cyber fedezet** köthető

„VIRTUÁLIS VÉDŐHÁLÓ” CYBER ÉS ADATVÉDELMI FELELŐSSÉGBIZTOSÍTÁS

COLONNADE
A FAIRFAX COMPANY

- A járványügyi helyzetre, a távoli munkavégzésre való tekintettel kialakított termék, amely rugalmasabb biztosítási megoldást kínál kisebb vállalatok részére

- Kérdőív kitöltése nélkül, egyszerűsített ajánlati lap kitöltésével megköthető

- Egyszerűsített követelményrendszer (de a GDPR által támasztott alapvető elvárásoknak való megfelelés itt is feltétel)

- A GDPR adatvédelmi felelősségbiztosításunkból már ismert fedezetek:
  - **Adatfelelősség**: személyes adatok és vállalati információk nem megfelelő kezelése, hálózatbiztonság
  - **Egyéb szakértői díjak**: proaktív szakértői szolgáltatások, a társaság jó hírnevének védelme, adatalanyok értesítése, elektronikus adatok helyreállítása
  - **Adatkezeléssel kapcsolatos bírságok**

- **Alacsonyabb limitek** (10/20/30 millió Ft), **kedvező díjak** (35.000-150.000 Ft)

- 500 millió Ft-ot nem meghaladó árbevételű cégek részére köthető

CYBER KITERJESZTÉS VAGYONBIZTOSÍTÁSOKHOZ

- A biztosított által egy kibertámadás következtében elszenvedett **saját károk** fedezetére szolgál

- Kizárólag **vagyonbiztosítással együtt** köthető (már meglévő, vagy újonnan megkötött szerződés mellé)

- Fedezetek:
  Hálózatkiesés
  Adathelyreállítás
  „**Bricking**”: elektronikus eszközök működésképtelenné válása
  Zsarolás
  IT szakértői költségek

- A teljes Cyber biztosításhoz képest alacsonyabb követelményrendszer, kérdőív kitöltése nem szükséges

- **Limitopciók: 10/25/50 millió Ft**

- 5 milliárd Ft-ot nem meghaladó árbevételű cégek részére köthető

ADATVÉDELMI BÍRSÁG

NAIH bírság a Sziget Zrt. által szervezett rendezvényeken folytatott, beléptetéssel összefüggő adatkezelések (NAIH 2019/55)

A NAIH megállapította a 2016. június 1. napjától 2018. május 24. napjáig terjedő időszakban szervezett rendezvényeken alkalmazott beléptetési gyakorlat során megvalósított adatkezelés jogellenességét abban a tekintetben, hogy a Kötelezett által a vizsgált időszakban folytatott adatkezelés

a) nem megfelelő jogalap alapján történt,
b) nem felelt meg a célhoz kötöttség elvének,
c) az érintettek nem kaptak megfelelő előzetes tájékoztatást.

Ez a gyakorlatban annyit jelentett, hogy a személy azonosító okmányokat lemásolták és megőrizték beléptetéskor.

A bírság összege 30.000.000 Ft volt.

KÁRPÉLDÁK - CYBER

HÁLÓZATBIZTONSÁG

Egy alkalmazott véletlenül kártékony számítógépes vírust töltött le a társaság hálózatán keresztül, amely kiterjedt adatvesztéssel járt, és vírus egy ügyfél számítógépes hálózatára történő továbbítását eredményezte. Az ügyfél beperelte a társaságot, azzal érvelve, hogy meg kellett volna akadályoznia a vírus továbbítását. Az elveszett adatok és a hálózatbiztonsági rendszer sérelme által okozott gazdasági veszteségek meghaladták a 220 millió forintot.

→ *Hálózat biztonság fedezet*

ZSARÓLÓVÍRUS

Egy társaság zsarolóvírus áldozata lett, amely a vállalat hálózati rendszerein belül terjedt, ezzel számos személyi számítógépet és szervert megfertőzve. A társaság felvette a kapcsolatot egy IT céggel, akik megállapították, hogy a számítógépek és szerverek pótlása kisebb költséggel jár, mint a rendszerek törlése, meghajtók formattálása és újjáépítése – teljes költség 4,8 millió forint.

→ *Zsarolás fedezet, IT szakértői tanácsadás*

HÁLÓZATKIESÉS

Egy termelő üzem számítógépes rendszerébe történő illetéktelen behatolás következtében a vállalatnak le kellett állítania gyártósorait, amíg a biztonsági hibát el nem hárítják. Az érintett adatok felmérése és elkülönítése, valamint a biztonsági hiba azonosítása 3 napot vett igénybe. Az üzemleállás több mint 150 millió forintos bevételkiesést okozott a társaságnak.

→ *Hálózatkiesés fedezet*

Köszönöm a figyelmet!