**CKD**

# VEZETŐ TISZTSÉGVISELŐK ÉS FELÜGYELŐBIZOTTSÁGI TAGOK FELELŐSSÉGBIZTOSÍTÁSA
## Cyber esemény kizárás (CKD)

A jelen záradék alapján a felek tudomásul veszik és elfogadják, hogy:
A jelen (viszont)biztosítási szerződés nem nyújt fedezetet a **Cyber esemény**ből eredő, azon alapuló, illetve annak tulajdonítható veszteségek, károk, díjak, költségek, kiadások és/vagy felelősség tekintetében.

A jelen záradék alkalmazásában:
**Cyber esemény** minden tényleges, állítólagos vagy feltételezett alábbi esemény:
a) az adatok károsodása, elvesztése, megsemmisülése, megsérülése, ellopása, illetve az adatok feletti operatív ellenőrzés elvesztése, valamint az adatok jogosulatlan vagy gondatlan kezelése, gyűjtése, rögzítése, visszakeresése, közzététele, terjesztése vagy az adatokkal való jogosulatlan vagy gondatlan rendelkezés a biztosított, illetve a biztosított **Társaság** független vállalkozója vagy külső szolgáltatója által; és/vagy

b) a személyes adatokhoz vagy bizalmas információkhoz való jogosulatlan hozzáférés, illetve azok jogosulatlan felhasználása (kivéve azt az információt, amely a nagyközönség számára jogszerűen és nyilvánosan elérhető, ide nem értve azt az esetet, amikor az adott nyilvánosan elérhető információ adatgyűjtés és/vagy -kezelés révén egyedileg azonosíthatóvá vált), amíg az érintett adatok a biztosított, illetve a biztosított **Társaság** független vállalkozója vagy külső szolgáltatója birtokában, őrzésében vagy ellenőrzése alatt találhatók; és/vagy

c) a **Társaság Számítógépes Rendszeré**nek nem fizikai, illetve technológiai meghibásodása vagy az adatok védelmére irányuló bármely technológiai biztonsági intézkedés meghibásodása. Ez magában foglalja többek között a biztosított **Társaság** üzleti tevékenységének az említett esemény(ek)ből eredő megszakítását is; és/vagy

d) a hálózati forgalom rosszindulatú irányítása, rosszindulatú számítógépes kód bejuttatása, valamint egyéb rosszindulatú támadás a **Társaság Számítógépes Rendszere** ellen, azon belül vagy annak felhasználásával. Ez magában foglalja többek között a biztosított társaság üzleti tevékenységének az említett esemény(ek)ből eredő megszakítását is; és/vagy

e) a biztosított **Társaság** üzleti tevékenységének megszakítása a biztosított által a **Társaság Számítógépes Rendszer**ének üzemeltetésével vagy karbantartásával kapcsolatban megvalósított véletlen, nem szándékos vagy gondatlan cselekményből, hibából vagy mulasztásból eredően, melynek következtében a **Társaság Számítógépes Rendszere** részben vagy egészben elérhetetlenné válik; és/vagy

f) az adatvédelemre vonatkozó jogszabályok és egyéb szabályok megsértése a fenti a)-e) pontból eredően;
g) zsarolóvírus támadás (ramsomware attack).

A **Cyber esemény** fogalommeghatározásában szereplő a) és c) pont alkalmazásában az adatok magukban foglalják többek között a személyes adatokat és/vagy a bizalmas információkat is (kivéve azt az információt, amely a nagyközönség számára jogszerűen és nyilvánosan elérhető, ide nem értve azt az esetet, amikor az adott nyilvánosan elérhető információ adatgyűjtés és/vagy -kezelés révén egyedileg azonosíthatóvá vált), függetlenül azok formájától.
A **Társaság Számítógépes Rendszere**: a biztosított Társaság által bérelt, a tulajdonában lévő vagy általa üzemeltetett, illetve a biztosított társaság vagy annak külső szolgáltatója (szolgáltatói) rendelkezésére bocsátott vagy számukra hozzáférhetővé tett számítógépes rendszer (ideértve többek között a hardvereket, a szoftvereket és/vagy a számítógépes programokat is), amely a biztosított **Társaság** elektronikus adatainak vagy szoftvereinek tárolására és kezelésére szolgál.

A jelen biztosítási szerződésben foglalt egyéb feltételek, rendelkezések, kizárások és korlátozások egyebekben továbbra is változatlanul fennállnak.

Allianz Hungária Zrt.