

## **Základní informace o pojištění GDPR**



Nařízení o ochraně osobních údajů (GDPR) od 25. května 2018 přináší zpřísnění odpovědnosti správce dat a výrazný nárůst možných pokut. Tato legislativa související s GDPR přináší velkým i malým společnostem nemalé náklady na zabezpečení dat klientů a obchodních partnerů. I přes veškerá opatření může dojít chybou systému či jednotlivce k úniku nebo poškození spravovaných dat. Na společnost se tak mohou obrátit nejen klienti či obchodní partneři, kteří se cítí být poškozeni, ale hrozí i vysoké sankce od dozorových orgánů. Pojištění kryje škody třetích stran, náklady spojené se ztrátou dat či hackerskými útoky a obvykle i pokuty udělené dozorovými orgány.

### **Pro koho je určeno pojištění GDPR?**

- pro všechny společnosti pracující s osobními či důvěrnými údaji klientů, obchodních partnerů a zaměstnanců

### **Pojištění v oblasti GDPR poskytuje pojistnou ochranu pro případ**

- úniku (ztráta, odcizení) osobních citlivých údajů nebo firemních dat a informací z informačního systému nebo počítače pojištěného subjektu, ať již náhodného, nebo z nedbalosti
- cíleného napadení informačního systému třetími osobami („hackerské“ útoky) nebo zaměstnanci za účelem získání přístupu k datům třetích stran, jejich zneužití a způsobení škody

### **Pojištění v oblasti GDPR kryje**

- sankce uložené dozorovým orgánem např. Úřadem na ochranu osobních údajů
- skutečné/ údajné neoprávněné nakládání s osobními údaji
- skutečné/ údajné neoprávněné nakládání s důvěrnými informacemi
- neoprávněné zpřístupnění osobních či důvěrných informací zaměstnancem společnosti
- pochybení subdodavatelské firmy pracující s osobními či důvěrnými informacemi.
- zničení, zkreslení či poškození osobních dat v počítačovém systému
- fyzické odcizení IT vybavení

### **Pojištění v oblasti GDPR jsou obvykle hrazeny**

- škody třetích stran v souvislosti s únikem jejich osobních údajů a s tím spojenou odpovědností pojištěného
- náklady na IT experty (forenzní audit)
- náklady na oznámení a PR
- náklady na právní zastoupení pojištěného

- náklady spojené s jednáním s dozorovými orgány (Úřad pro ochranu osobních údajů) a jimi udělené pokuty
- výpadek sítě/přerušování provozu nebo vydírání pojištěného (ransomware)

### **Příklady konkrétních škod z praxe**

#### **Únik osobních údajů pacienta – nemocnice**

- osobnostní újma pacienta, znemožnění výkonu povolání z důvodu zveřejnění zdravotního stavu
- žaloba o finanční kompenzaci ze strany pacienta
- pokuta udělená dozorovým orgánem za zveřejnění citlivých informací

#### **Hackerský útok a následné zveřejnění 117 000 osobních údajů studentů – univerzita**

- náklady na IT experty za účelem zjištění příčiny útoku a přesného počtu zveřejněných údajů
- náklady na oznámení (informační dopis všem studentům a zřízení call centra)
- náklady na PR (zlepšení reputace a dobré pověsti) pokuta udělená dozorovým orgánem za zveřejnění citlivých informací

#### **Útok hackerů na PC síť internetového obchodu**

- následuje výpadek PC systému
- snížení zisku pojištěného v důsledku nemožnosti prodávat zboží
- náklady na IT experty za účelem zjištění příčiny výpadku systémů
- náklady na PR

### **Rozšířené krytí kybernetických rizik**

- náklady na znalce v oblasti kybernetiky při podezření na neoprávněné vniknutí do systémů společnosti
- náklady na nápravu pověsti společnosti i dobrého jména jednotlivce v případě, že dojde k porušení předpisů o ochraně osobních údajů
- náklady na obnovu elektronických dat
- zveřejnění digitálního obsahu v jehož důsledku dojde k neúmyslnému narušení autorského práva, plagiátorství, zásahu do soukromí či zásahu do pověsti právnické osoby nebo důstojnosti fyzické osoby
- ztráty vzniklé vydíráním prostřednictvím počítačové sítě
- ztráty způsobené výpadkem počítačového systému v důsledku selhání zabezpečení

Pro vypracování nabídky je nezbytné vyplnění dotazníku.