Přísnější pravidla ochrany osobních dat platí od května. Pomoci může i pojištění kybernetických rizik

Od 25. května 2018 začala pro firmy platit přísnější pravidla pro ochranu osobních dat zákazníků, tzv. GDPR. Část rizik přitom může pomoci ochránit pojištění kybernetických rizik (tzv. CYBER pojištění), na které by firmy měly aktivně myslet při analýze rizik a sjednávání svých pojistek, a to nezávisle na GDPR. Říká Michal Pilecký, specialista pojištění kybernetických rizik ze společnosti RENOMIA, největšího pojišťovacího makléře v České republice.

Firmy již pravděpodobně implementovaly všechny požadavky k GDPR. Existuje ale možnost se nějak bránit případným postihům?

Ano, věřím, že firmy, které osobní data zodpovědně zpracovávají, tak již implementovaly vše, co nové nařízení GDPR požadovalo. Navíc nařízení GDPR sice přináší řadu novinek v oblasti ochrany osobních dat, ale legislativu řešící tuto problematiku tu máme již řadu let a pro firmy to tedy není či by neměla být převratná novinka. Doporučil bych ale všem, aby se kromě nastavení IT procesů a implementace nových vnitřních pravidel, nechaly před ztrátou citlivých zákaznických dat i pojistit. RENOMIA má v této oblasti rozsáhlé domácí i mezinárodní zkušenosti a ví, co klientům doporučit.
Jak se lze proti ztrátě zákaznických dat pojistit?

Pojištění je vhodný doplněk k řízení kybernetických rizik ve firmách. Na trhu je více produktů od různých pojistitelů, specialisté RENOMIA přitom umí klientům pomoci se v nabídkách zorientovat tak, aby firmy měly co nejlepší krytí. Pojistky obvykle kryjí v případě kybernetického incidentu nejen náklady na škody a právní zastoupení v souvislosti s odpovědností vůči třetím stranám, ale například i forenzní IT audit, který nalezne zdroj a rozsah úniku dat a informací, náklady na komunikaci s veřejností a nápravu reputace postižené firmy, a dokonce i pokuty, které mohou udělit dozorové orgány.

Je možné říct, v jakém odvětví si firmy tento typ pojištění nejvíce sjednávají?

Jsou to zejména větší firmy, které spravují velké množství osobních dat (jedná se zejména o e-shopy, on-line sázkové kanceláře, společnosti z oblasti IT, společnosti z oblasti médií, telekomunikace, dodavatelé elektřiny, vody, tepla, plynu apod., finanční instituce nebo nemocnice). Rád bych zde vyzdvihl i nemocnice, které nejen že spravují citlivé osobní údaje svých pacientů, ale vloni byly i významně zasaženy škodlivým virem – ransomware Wannacry, kdy řada nemocnic na světě prakticky nemohla fungovat z důvodu zablokovaní počítačových systémů. Aktuálně zaznamenáváme zvýšený zájem i ze strany společností segmentu SME.

Jak moc se liší povědomí o této pojistce v zahraničí? Využívají pojištění proti kybernetickým hrozbám firmy v zahraničí častěji?

Samozřejmě. Ohledně pojištění firem v České republice a západní či anglo-americké tradici je obecně propojištěnost u nás nižší. Není to tedy jen případ pojištění kybernetických rizik.

Došlo už u nějaké české firmy k pojistné události a vyplacení plnění? Pokud ne, máte informace o tom, jak často k podobným událostem dochází v zahraničí?

Ano mnohokrát, váže nás však mlčenlivost vůči klientům, kdy bez jejich souhlasu nemůžeme případy komentovat. Kybernetická rizika jsou dle Allianz Risk Barometru 2. největší hrozbou na světě. Pojišťují se sice většinou velké firmy, ale ze statistik vyplývá, že ve více než 70 % případů dochází k narušení bezpečnosti či ztrátě dat zejména u malých a středních podniků do 100 zaměstnanců a k útoku malwarem dochází dle anti-malware společností přibližně každých 40 vteřin (do frekvence útoků jsou ale počítány i osobní počítače). Vzhledem k počtu útoků bych tak jako podnikatel, který nakládá s osobními daty, neváhal a pojistil se.

Příklady 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

Milan Pilecký,
specialista pojištění kybernetických rizik

RENOMIA, a.s.

Holandská 8
639 00 Brno

Tel.: +420 222 390 888
e-mail: info@renomia.cz

© EPRAVO.CZ – Sbírka zákonů, judikatura, právo | www.epravo.cz

Další články:

- Novela zákona o znalcích: krok ke stabilizaci systému, který se potýkal s provozní nepružností
- ASPI přechází na webovou verzi: výhody a budoucnost právních technologií
- Studium LLM v oboru PRÁVO & OBCHODNÍ SEKTOR: Když právo potkává byznys
- Legal Innovation Day 2025 ukáže, jak na praktické využití AI
- D.A.S. právní ochrana slaví 30 let a rozšiřuje dostupnost právních služeb
- Využijte nového AI asistenta pro právní rešerše
- Českým živnostníkům chybí právní podpora. D.A.S. přináší dostupné řešení
- ČEZ Prodej spouští inovativní službu flexibility: na dálku bude regulovat přetoky domácích fotovoltaik
- Veřejné právo jako klíčová oblast právního systému
- Za oponou vývoje: jak Wolters Kluwer vytváří AI nástroje pro efektivnější právní praxi
- Rovnováha mezi rodinou a paragrafy: Otcové z D.A.S. sdílejí své strategie