ECOFINANCE
DORADCY FINANSOWI

Autoryzowany Partner
LEADENHALL
Coverholder at LLOYD'S

Czy moja firma potrzebuje polisy Cyber? Czy wydatek na ubezpieczenie jest zasadny?

W maju 2018 roku weszły w życie przepisy unijnego rozporządzenia ws. ochrony danych osobowych (tzw. Rozporządzenie RODO). Wprowadziło ono do polskiego systemu prawnego szereg nowych obowiązków w zakresie nie tylko ochrony danych osobowych, ale również praw osób, których dane są przetwarzane. Najważniejsze zmiany w tym zakresie to:

a) **zlikwidowano tzw. rejestr baz danych w GIODO** – oznacza to, że teraz każdy przedsiębiorca niezależnie od wielkości i formy prawnej ma obowiązek przestrzegania przepisów w zakresie ochrony danych swoich klientów i pracowników (patrz sekcja A i B polisy Cyber)
b) **administracyjne kary pieniężne do 20 mln euro lub 4% rocznego obrotu** – nowy Urząd Ochrony Danych Osobowych może kontrolować przestrzegania przepisów RODO w każdej firmie i w przypadku naruszenia zasad ochrony danych lub praw osób, których dane przetwarza przedsiębiorca, nakładać administracyjne kary pieniężne (patrz sekcja B polisy Cyber)
c) **pojawia się wymóg „rozliczalności"** – oznacza to, że teraz na przedsiębiorcy spoczywa obowiązek wykazania przed Urzędem, że wdrożone narzędzia bezpieczeństwa, jak i pisemne procedury dotyczące ochrony danych w firmie są adekwatne do zagrożeń
d) **obowiązek zgłoszenia incydentów informatycznych** - w ciągu 72h każdy przedsiębiorca ma obowiązek zgłoszenia do UODO incydentów związanych z ryzykiem wycieku, kradzieży lub zniszczenia danych osobowych wraz z opisem podjętych działań (patrz sekcja C polisy Cyber) oraz obowiązek poinformowania wszystkich osób, których dane zostały wykradzione / ujawnione.

Poza karami administracyjnymi przedsiębiorca musi liczyć się z odpowiedzialnością cywilną wobec osób, których dane lub prawa zostały naruszone oraz kosztami zarządzania incydentami informatycznymi:

a) średni koszt firmy informatyki śledczej to od 15 tyś zł opłaty zryczałtowanej za „serwer" + od 300 euro za 1h pracy informatyka śledczego
b) średni koszt agencji PR – od 20 tyś do 300 tyś zł w zależności od rozmiaru incydentu i ilości danych

Indykacja składek ubezpieczenia Cyber w Lloyd's

Wysokość składki uzależniona jest od **branży** i **przychodów** firmy za ostatnie 12 m-cy oraz tzw. **ilości rekordów**, czyli ilości osób fizycznych (klientów i pracowników), których dane przechowywane są zarówno w wersji papierowej, jak i elektronicznej. Poniższa indykacja ma charakter poglądowy i nie stanowi oferty w rozumieniu kodeksu cywilnego.

			Suma ubezpieczenia Cyber				udział własny
			500 000,00 zł	1 000 000,00 zł	2 000 000,00 zł	5 000 000,00 zł	
Ubezpieczony	Przychód	Ilość rekordów	Składka roczna	Składka roczna	Składka roczna	Składka roczna	
Kancelaria prawna A	do 10 000 000,00 zł	do 50 000	1 490,00 zł	2 012,00 zł	2 717,00 zł	4 005,00 zł	2 000,00 zł
Kancelaria prawna B	do 10 000 000,00 zł	od 51 000	1 490,00 zł	2 012,00 zł	2 717,00 zł	4 005,00 zł	3 000,00 zł

Aby otrzymać ofertę Cyber muszą być spełnione następujące minimalne warunki zabezpieczeń technicznych:

Kopie zapasowe danych tworzone są przynajmniej raz w tygodniu (np. na dyskach zewnętrznych, serwerach zapasowych, w "chmurze")	**TAK**
Ubezpieczony korzysta z oprogramowania antywirusowego i firewall	**TAK**
Oprogramowanie antywirusowe i firewall aktualizowane jest nie rzadziej niż co kwartał	**TAK**
Wdrożone są procedury kontroli dostępu i wykorzystania systemu informatycznego, w tym procedura aktualizacji oprogramowania wykorzystywanego przez Ubezpieczonego	**TAK**

Do powyższej indykacji składek przyjęto brak szkód i incydentów informatycznych (kradzież danych, zniszczenie danych, atak hakerski itp.)

Zakres ubezpieczenia Cyber przyjęty do indykacji

Sekcja A	**naruszenie prywatności - koszty postępowań i odszkodowań cywilnoprawnych**
Kiedy zadziała?	*Gdyby doszło do naruszenia danych osobowych klientów lub pracowników (zarówno w wersji papierowej, jak i elektronicznej) np. wyciek lub kradzież danych lub naruszenia praw w zakresie ochrony danych osobowych mogą oni wystąpić do firmy przetwarzającej ich dane o zadośćuczynienie za naruszenie dóbr osobistych oraz naprawienie szkody majątkowej wynikłej z tego naruszenia.*
Sekcja B	**naruszenie prywatności - koszty postępowań regulacyjnych i kar nakładanych w trybie administracyjnym**
Kiedy zadziała?	*Gdyby doszło do naruszenia danych osobowych klientów lub pracowników (zarówno w wersji papierowej, jak i elektronicznej) np. wyciek lub kradzież danych lub naruszenia praw w zakresie ochrony danych osobowych mogą oni złożyć skargę do organu nadzoru, skutkującą wszczęciem przez organ kontroli w zakresie ochrony danych osobowych. W przypadku stwierdzenia naruszeń Urząd Ochrony Danych Osobowych może nałożyć na firmę przetwarzającą te dane administracyjną karę pieniężną w max. wysokości do 20 mln euro lub 4% rocznego obrotu.*
Sekcja C	**naruszenie bezpieczeństwa informacji - koszty zarządzania kryzysowego po incydencie informatycznym**
Kiedy zadziała?	*Gdyby doszło do ryzyka naruszenia danych osobowych klientów lub pracowników (zarówno w wersji papierowej, jak i elektronicznej) np. naruszenie bezpieczeństwa systemów informatycznych, wyciek, kradzież danych lub do ataku hakerskiego blokującego dostęp do systemów wykorzystywanych przez firmę w swojej działalności wymagane jest niezwłoczne wdrożenie procedur bezpieczeństwa:* *- Koszty informatyki śledczej – audyt systemów informatycznych, zidentyfikowanie luk bezpieczeństwa, zabezpieczenie krypto-śladów, wydanie raportu z rekomendacjami* *- Koszty agencji PR – wdrożenie planu zarządzania wizerunkiem i zminimalizowania utraty reputacji*
Sekcja D	**naruszenie bezpieczeństwa informacji - koszty postępowań i odszkodowań cywilnoprawnych**
Kiedy zadziała?	*Gdyby do w związku z naruszeniem bezpieczeństwa systemów informatycznych, które wyprodukował lub udostępnił swoim kontrahentom Ubezpieczony, zostali oni narażenie na szkody w swojej działalności (np. ubezpieczony udostępnia system do rozliczeń i zamówień i system ten został zablokowany w wyniku ataku hakerskiego) mogą oni wystąpić z roszczeniem o odszkodowanie w związku z brakiem możliwości prowadzenia swojej działalności.*

Sekcja E	odpowiedzialność multimedialna - koszty postepowań i odszkodowań cywilnoprawnych
Kiedy zadziała?	*Gdyby doszło do naruszenia czyichś praw do wizerunku, wypowiedzi lub praw autorskich poprzez działalność firmy z wykorzystaniem social media (np. profil firmowy na Facebook), stron WWW (np. strona firmy) lub służbowej poczty elektronicznej (np. mailing do klientów itp.) wówczas osoby poszkodowane takim działaniem mogą zgłosić do firmy roszczenie o naprawienie szkody lub zadośćuczynienie za naruszenie dóbr osobistych.*
Sekcja F	cyber wymuszenie - koszty „okupu" po ataku hakerskim
Kiedy zadziała?	*Gdyby doszło do ataku hakerskiego typu „ransomware" blokującego dostęp do systemów wykorzystywanych przez firmę w swojej działalności lub mającego na celu kradzież danych klientów, a następnie żądanie od firmy zapłaty określonej sumy pieniędzy za odblokowanie dostępu do danych lub za nieujawnianie tych danych wówczas za zgodą Ubezpieczyciela koszty takiego „cyber wymuszenia" mogą zostać pokryte z polisy.*