
KRAJOWE BIURO OBSŁUGI ROSZCZEŃ UBEZPIECZENIOWYCH®

# RODO

**czyli nowe prawo o ochronie danych osobowych osób fizycznych coraz bliżej ale nie dajmy się zwariować.**

## Jak się zabezpieczyć aby dalej bezpiecznie prowadzić przedsiębiorstwo.

RODO to zwyczajowa skrócona nazwa Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie **ochrony osób fizycznych** w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (...) uchwalonego 27 kwietnia 2016 roku.
Wejście w życie przepisów ustawy: **25 maja 2018 roku**.

**Kogo dotyczy:** wymogom zgodności z RODO będą podlegały wszystkie podmioty (niezależnie od formy prawnej) w tym instytucje publiczne, które w swojej działalności przetwarzają dane osobowe.

**Dane osobowe** dzięki rozwojowi technologii - zwłaszcza informatyzacja usług - przenoszą się do świata cyfrowego i stają się od niego całkowicie zależne.

> *Najważniejsze zagrożenia związane są z przetwarzaniem danych np. bezprawnym ich ujawnieniem, kradzieżą lub utratą oraz z dostępem do systemu informatycznego przez osoby nieuprawnione, w tym z cyber-wymuszeniami.*

**Dla każdej firmy źródłem tych zagrożeń mogą być:**

- osoby trzecie (np. hakerzy),
- dostawcy,
- kontrahenci,
- pracownicy.

## Konsekwencje mogą przybrać następujące oblicza:

- **Odszkodowawcze** – zarówno w zakresie odpowiedzialności cywilnej wobec osób, których dane zostały naruszone, jak też odpowiedzialności administracyjnej (np. postępowanie za naruszenie przepisów RODO),
- **Ekonomiczne** – obejmujące koszty obsługi incydentu informatycznego (informatyki śledczej, powiadomienia osób, których dane zostały naruszone, odtworzenie utraconych danych, wdrożenie właściwych zabezpieczeń itp.),
- **Reputacyjne** – oznaczające utratę zaufania klientów i kontrahentów oraz konieczność pokrycia kosztów zarządzania marką i wizerunkiem firmy.

22 256 53 00 biuro@kboru.pl www.kboru.pl

## ZIDENTYFIKOWALIŚMY więc RYZYKO, które da się ubezpieczyć !

Z naszymi partnerami tworzymy dla naszych klientów ubezpieczenie, które zabezpieczy finansowo małe, średnie i duże przedsiębiorstwo w następujących obszarach:

## I. ODPOWIEDZIALNOŚĆ CYWILNA ZA NARUSZENIE PRYWATNOŚCI:

Naruszenie prywatności jest powszechnie utożsamiane z wyciekiem danych osób fizycznych. Danych, za których ochronę odpowiada osoba lub instytucja, której je powierzono.
W rzeczywistości prawnej pojęcie to może być znacznie szersze i oznaczać naruszenie jakiejkolwiek regulacji dotyczącej ochrony prywatności. Jest to przede wszystkim Rozporządzenie Europejskie o ochronie danych osobowych (RODO), ale też wszystkie inne (lokalne) ustawy o ochronie danych osobowych.

### Odszkodowanie obejmie przede wszystkim:

- należne zadośćuczynienie i odszkodowanie dla osób fizycznych poszkodowanych przez bezprawny wyciek lub naruszenie ich danych. (Nie ma przy tym znaczenia czy dane przechowywane były w formie cyfrowej czy papierowej).
- koszty rozmaitych działań, które Ubezpieczony jest zobowiązany podjąć w celu zmniejszenia skutków wycieku lub utraty danych. Są to między innymi:
  - obowiązek pisemnego poinformowania każdej osoby, której dane zostały bezprawnie ujawnione,
  - działania podjęte w celu odtworzenia utraconych lub skompromitowanych danych,
  - usunięcie danych z miejsc w sieci, w których znalazły się bez zgody osoby, której dane dotyczą.

## II. ODPOWIEDZIALNOŚĆ ADMINISTRACYJNA ZA NARUSZENIE PRYWATNOŚCI:

Wyciek danych osobowych lub inne naruszenia prywatności osób fizycznych, mogą spowodować wszczęcie postępowania regulacyjnego. Do ich ochrony powoływane są organy państwowe.(Urząd Ochrony Danych Osobowych oraz Prokuratura).
Konsekwencją postępowania może być wydanie decyzji zobowiązującej winnego do konkretnego działania i/lub nałożenie na niego finansowej kary administracyjnej.

**Kary przewidziane w Europejskim Rozporządzeniu** o ochronie danych osobowych (w skrócie RODO) mogą być ogromne: do 4% łącznego przychodu Ubezpieczonego lub 20mln EUR w zależności, która z tych kwot jest większa!
Ubezpieczyciel pokrywa koszty obrony w tego typu postępowaniach regulacyjnych. Może objąć także refundację nałożonych kar administracyjnych.

## III. KOSZTY OBSŁUGI INCYDENTU INFORMATYCZNEGO:

Incydent informatyczny to pojęcie znacznie szersze od wycieku danych. Może nim być każdy atak hakerski lub wręcz proste stwierdzenie faktu, iż nieuprawniona osoba miała dostęp do systemu informatycznego firmy i jej danych.

**Polisa pokrywa koszty** usług niezbędnych do odpowiedniego zarządzenia obsługą takiego incydentu. Ubezpieczyciel nie tylko zrefunduje te koszty, lecz co ważniejsze - na życzenie Ubezpieczonego - zapewni odpowiednie usługi.

22 256 53 00 biuro@kboru.pl www.kboru.pl

**Dobrym przykładem jest tzw. informatyka śledcza. - współpraca z zewnętrznymi specjalistami jest absolutnie niezbędna i obejmuje:**

- identyfikację skompromitowanych stacji roboczych, serwerów i innych urządzeń sieciowych oraz zabezpieczenie śladów włamań,
- określenie najlepszej metody zabezpieczenia danych oraz samo ich zabezpieczanie,
- analizę zebranych danych (pamięci RAM i dysków) w celu ustalenia źródeł, skutków i metody ataku,
- odzyskanie plików konfiguracyjnych i innych istotnych informacji na temat intruza,
- odtworzenie historii działań atakującego i ofiary ataku (np. dla ustalenia sposobu zainfekowania),
- analizę dzienników zdarzeń z tych systemów zewnętrznych, które także mogły zarejestrować aktywność intruza.

**Inne obszary obsługi incydentu, których koszty refunduje Ubezpieczyciel, mogą być zlecone:**

- kancelariom prawnym zdolnym sprawnie obsłużyć pozwy (także zbiorowe),
- agencjom Public Relations.

## IV. ODPOWIEDZIALNOŚĆ CYWILNA ZA NARUSZENIE BEZPIECZEŃSTWA INFORMACJI U OSÓB TRZECICH:

Obszar ten zapewnia ubezpieczonemu ochronę, gdy niewłaściwe działanie jego systemu informatycznego lub nienależyte korzystanie przez niego z systemu zewnętrznego wyrządzi szkodę osobom trzecim.

Skutkiem może być powstały u osoby trzeciej wyciek danych lub inne jego straty. Szkodą mogą być omawiane już usługi informatyków śledczych, ale traktowane nie jako szkoda własna ubezpieczonego, ale jako szkoda osoby trzeciej.

Inne roszczenia mogą dotyczyć pokrycia kosztów agencji PR lub kancelarii prawnej, które osoba trzecia w związku z wyciekiem musi ponieść.

Polisa pokryje takie roszczenie, za które odpowiedzialność na zasadach ogólnych można przypisać ubezpieczonemu, czyli kiedy jest on właścicielem lub operatorem systemu informatycznego, którego wadliwość lub niewystarczające zabezpieczenia doprowadziły do wycieku. Ubezpieczenie obejmie także koszty obrony przed nieuzasadnionymi roszczeniami.

**Przykładem tego może być:**

- naruszenie lub wyciek - z winy Ubezpieczonego - danych przechowywanych w systemie osoby trzeciej, np.: wyciek danych z systemu PESEL, do którego dostęp ma urząd gminy, wyciek z bazy NFZ, z której korzysta placówka medyczna.

## V. ODPOWIEDZIALNOŚĆ MULTIMEDIALNA:

Obejmuje roszczenia z tytułu czynów popełnionych przez Ubezpieczonego w wyniku publikacji za pomocą środków elektronicznych, a więc na stronach internetowych, w mediach społecznościowych lub w intranecie.

**Odpowiedzialność taka obejmuje ochroną czyny polegające na:**

- Zniesławieniu, znieważeniu i pomówieniu,
- Naruszeniu prawa do prywatności,
- Naruszeniu praw autorskich,
- Naruszeniu prawa do domeny lub znaku towarowego,
- Dopuszczenie się plagiatu.

## VI. KOSZTY CYBER-WYMUSZENIA.

**Cyber-wymuszenie polega na:**

- wprowadzeniu - lub wiarygodnej groźbie wprowadzenia - złośliwego oprogramowania lub zakłócenia pracy systemu informatycznego ubezpieczonego,
- rozpowszechnieniu - lub wiarygodnej groźbie rozpowszechniania - danych osób, za których bezpieczeństwo odpowiada Ubezpieczony.

Następnie cyber-przestępca - w zamian za zaprzestanie dalszych działań lub za przywrócenie dostępu do systemu lub danych tam przechowywanych - żąda zapłacenia określonej kwoty wyrażonej w kryptowalucie. Tak wymuszona płatność stanowi szkodę własną Ubezpieczonego. **Ten zakres jest fakultatywny.** Kwota wymuszonej na Ubezpieczonym płatności zostanie zrefundowana, tylko wtedy, gdy Ubezpieczyciel wyraził uprzednio na to zgodę. Decyzja o udzieleniu takiej zgody podejmowana jest w oparciu o szczegółową analizę sytuacji oraz opinię ekspertów z zakresu informatyki śledczej.

## VII. KOSZTY ODTWORZENIA DANYCH I UTRACONY ZYSK.

Koszty odtworzenia danych i koszty przestoju bywają przedmiotem odrębnego ubezpieczenia majątkowego – jednak tylko wtedy, gdy są skutkiem fizycznej utraty lub uszkodzenia mienia (komputerów, nośników).
Objęcie ich ochroną także wówczas, gdy przyczyna ma charakter „software'owy" a nie „sprzętowy" jest dla wielu przedsiębiorców nie mniej istotne.
W tym obszarze ubezpieczyciel pokryje przede wszystkim szkodę własną Ubezpieczonego polegającą na koszcie odtworzenia jego własnych, utraconych danych. Obejmie też, wymieniony w warunkach katalog kosztów, które Ubezpieczony zmuszony będzie ponosić mimo przestoju przedsiębiorstwa i związany z tym brak przychodów. Zakres ten będzie szczególnie interesujący dla tych przedsiębiorstw, w których charakter działalności przesądza o tym, że to naruszenie bezpieczeństwa ich systemów, a nie pożar czy zalanie komputerów może spowodować długotrwały przestój.

## Co nam potrzeba od firmy aby przygotować ofertę:

- pełnomocnictwo brokerskie
- kwoty przychodu ubezpieczonego za ostatnie 12 miesięcy,
- szacunkowej liczby posiadanych rekordów danych osobowych (rekord = 1 osoba fizyczna),
- rodzaju branży, w której prowadzi firma działalność.

## Skontaktuj się z nami:

**Krajowe Biuro Obsługi Roszczeń Ubezpieczeniowych Sp. z o.o.**
ul. Powązkowska 15, 01-797 Warszawa

22 256 53 00

biuro@kboru.pl , agnieszka.derylo@kboru.pl , grzegorz.waszkiewicz@kboru.pl

Wejdź na naszą stronę: **www.kboru.pl** i prześlij nam swoje dane kontaktowe.