CHUBB®

Ogólne rozporządzenie o ochronie danych (RODO)

Co trzeba wiedzieć o RODO?

W jaki sposób Chubb może pomóc ograniczyć cyberryzyko?

CHUBB®

Co trzeba wiedzieć o RODO?

Nowe rozporządzenie RODO wprowadza ujednolicone zasady postępowania w całej Unii Europejskiej. Harmonizuje krajowe przepisy dotyczące ochrony danych osobowych i obowiązuje bezwzględnie. Jest odpowiedzią na zmiany technologiczne, jakie zaszły w społeczeństwie przez ostatnie dwadzieścia lat.

Nowe zasady opracowano tak, aby podmioty przechowujące dane osobowe były odpowiedzialne za informacje w ich posiadaniu.

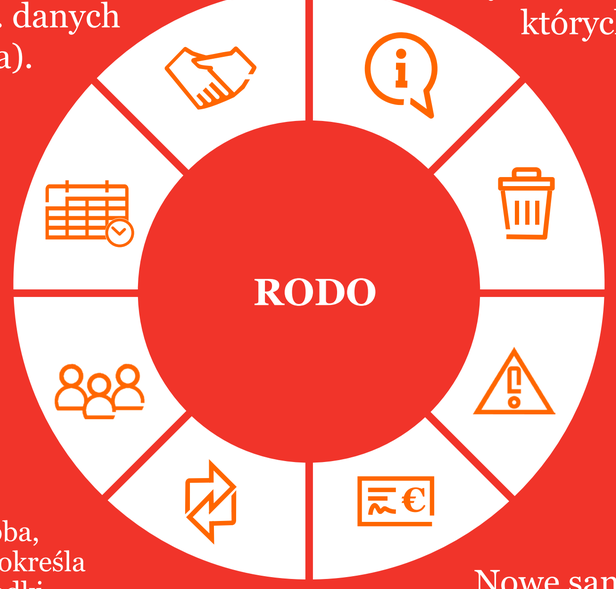
Rozporządzenie reguluje między innymi następujące kwestie:

Wyrażenie zgody na przetwarzanie danych osobowych oraz wyraźne dopuszczenie przetwarzania ich określonych kategorii (np. danych dotyczących stanu zdrowia).

Data wejścia w życie: **25 maja 2018 r.**

Zwiększenie zakresu odpowiedzialności **podmiotów przetwarzających** w porównaniu z administratorami.

- Administrator: zdefiniowany ogólnie jako osoba, podmiot lub jednostka, która określa cel przetwarzania danych i środki, jakimi są przetwarzane.
- Podmiot przetwarzający: zdefiniowany ogólnie jako osoba, podmiot lub jednostka, która przetwarza dane osobowe w imieniu administratora.



Niezwłoczne powiadamianie o incydentach organów ochrony danych osobowych oraz osób, których dane dotyczą.

Prawo do **„usunięcia”** danych i **„zostania zapomnianym”**.

Potrzeba wprowadzenia mechanizmów **oceny skutków** w przypadku operacji przetwarzania powodujących wysokie ryzyko.

Prawo do **przenoszenia danych**

Nowe sankcje, w tym **grzywny** do wysokości 20 mln euro lub 4% globalnego obrotu, **ostrzeżenia** ze strony organów ochrony danych oraz **postępowania regulacyjne**.

> W jaki sposób Chubb może pomóc ograniczyć cyberryzyko?

Co trzeba wiedzieć o RODO?

Artykuł 32: Bezpieczeństwo przetwarzania – najważniejsze założenie Rozporządzenia

W rozporządzeniu nie warunkuje się nałożenia kary faktyczną utratą lub ujawnieniem danych. Karać można w przypadku niespełnienia wymogów określonych w Rozporządzeniu, co stwierdza się w trakcie dochodzenia wszczynanego wówczas, gdy podejrzewa się włamanie lub w ramach postępowania regulacyjnego prowadzonego przez organ ochrony danych, np. Prezesa UODO (Urzędu Ochrony Danych Osobowych).

Wymogi sformułowane w Rozporządzeniu opierają się na ryzyku i nie mają charakteru preskryptywnego.

Po stronie administratorów i podmiotów przetwarzających leży obowiązek wdrożenia „odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku". Poza odpowiedzialnością obu stron warto wspomnieć również o pozostałych środkach o charakterze organizacyjnym (politykach, procedurach, szkoleniach, itp.) oraz o zabezpieczeniach technicznych.

Niektóre postanowienia artykułu 32 precyzują wymagania odnośnie do „środków" mających na celu ograniczenie ryzyka:

1. Szyfrowanie

Treść ustępu sugeruje, że odpowiedzialność za zapewnienie bezpieczeństwa na poziomie adekwatnym do ryzyka leży zarówno po stronie administratora, jak i podmiotu przetwarzającego, obejmując również szyfrowanie danych.
W przypadku operacji przetwarzania powodujących wysokie ryzyko, administratorzy muszą dokonać oceny ryzyka, obejmującą również analizę mechanizmów zabezpieczających, takich jak szyfrowanie.

2. Systemy i usługi przetwarzania

Obowiązki wykraczają obecnie poza samą ochronę danych i obejmują również infrastrukturę.
Podmioty przetwarzające muszą zagwarantować administratorom zastosowanie odpowiednich środków technicznych i organizacyjnych.
Innymi słowy, podmioty przetwarzające muszą zapewnić dostępność odpowiedniej infrastruktury i sprzętu oraz zagwarantować właściwy przepływ informacji. Ich usługi muszą być też stale dostępne.
Ataki DDoS czy ataki przy pomocy oprogramowania typu ransomware mogą spowodować przerwy w świadczeniu usług.
Brak dostępu do danych osobowych uznaje się obecnie za naruszenie bezpieczeństwa, które może skutkować sankcjami analogicznymi do sytuacji, gdy następuje ich utrata lub nieuprawnione ujawnienie.
Podmioty przetwarzające muszą zapewnić odpowiednio wysoki poziom bezpieczeństwa, aby ochronić się przed tego rodzaju zagrożeniami, a ważną rolę w procesie odgrywa również właściwa ocena ryzyka i analiza funkcjonujących mechanizmów.

3. Jak najszybsze przywracanie dostępu do usług w przypadku wystąpienia incydentu fizycznego lub technicznego

Kluczowymi hasłami w tej części Rozporządzenia są: Przywracanie – wprowadza się potrzebę zapewnienia odpowiedniej elastyczności systemu oraz możliwości uruchomienia środowiska zapasowego, aby zagwarantować ciągłość świadczenia usług.
Pojawiające się określenie „niezwłocznie" sugeruje, że administrator musi z góry przewidzieć wszelkie możliwe konsekwencje włamania. Należy wziąć pod uwagę wpływ na inne osoby oraz rozważyć ewentualne potrzeby konsumentów i osób fizycznych w zakresie dostępu do danych, a nie kierować się wyłącznie interesem biznesowym.
Rozróżnienie incydentów fizycznych i technicznych rozszerza zakres odpowiedzialności – z samych cyberataków na pożary, powodzie, awarie oraz inne, typowe zagrożenia. Prowadzone analizy należy również rozszerzyć na podwykonawców.

4. Testowanie i ocena środków technicznych i rozwiązań organizacyjnych

Treść tej części Rozporządzenia sugeruje, że ocena ryzyka jest niezbędna to tego, aby ustalić, jakie środki będą odpowiednie. Prowadząc testy, można również ocenić ich skuteczność.

> W jaki sposób Chubb może pomóc ograniczyć cyberryzyko?

Co trzeba wiedzieć o RODO?

Podsumowanie

Wymogi określone w RODO wykraczają poza ochronę danych osobowych:

- dokonywanie oceny ryzyka, wykraczającej zakresem poza ocenę skutków dla ochrony danych,
- zapewnienie bezpieczeństwa na poziomie adekwatnym do ryzyka, co obejmuje również szyfrowanie danych,
- zapewnienie redundancji/odpowiedniej elastyczności systemów,
- wdrożenie planu odzyskiwania po awarii, uwzględniającego wymóg „niezwłoczności” reakcji,
- testowanie i ciągłe monitorowanie wszelkich zabezpieczeń – zarówno o charakterze organizacyjnym, jak i technicznym.

Kontakt

Zapraszamy do kontaktu z Chubb.

Chubb European Group SE Spółka Europejska
Oddział w Polsce
ul. Królewska 16
00-103 Warszawa
Tel.: 22 452 39 99
e-mail: poland.office@chubb.com

> W jaki sposób Chubb może pomóc ograniczyć cyberryzyko?

W jaki sposób Chubb może pomóc ograniczyć cyberryzyko?

W jaki sposób Chubb może pomóc ograniczyć cyberryzyko?

Kogo chronimy?

Polisa Cyber Enterprise Risk Management chroni organizacje każdej wielkości przed zagrożeniami takimi jak: brak dostępności, naruszenie danych, uszkodzenie danych, oprogramowanie typu ransomware, incydenty cybernetyczne w zakresie odpowiedzialności względem osób trzecich, jak i szkód własnych poniesionych w wyniku działań podejmowanych w złej wierze lub zaniedbań.

Polisa zawiera w sobie szeroki zakres usług analizy cyberryzyka, zarządzania kryzysowego po wystąpieniu zdarzenia oraz umożliwia transfer części ryzyka na ubezpieczyciela. Naszym celem jest ograniczenie coraz większego ryzyka ponoszonego przez podmioty, związanego z funkcjonowaniem w cyberprzestrzeni oraz z ochroną danych osobowych.

Jaki jest zakres ochrony?

Reagowanie na incydenty: Nawiązaliśmy współpracę z liderem rynku usług zarządzania kryzysowego, dzięki czemu możemy zaoferować naszym klientom usługi reagowania na incydenty w skali globalnej. Nasze usługi dostępne są 24 godziny na dobę za pośrednictwem jednego punktu kontaktowego.

Wspieramy klientów na każdym etapie procesu ochrony, korzystając ze wsparcia licznego grona ekspertów specjalizujących się w informatyce śledczej, zapobieganiu atakom DDoS, wymuszeniach komputerowych (extortion), kwestiach prawnych, obowiązkach informacyjnych oraz public relations. Nasze usługi są dostępne 24 godziny na dobę przez 365 dni w roku.

Sekcje związane z odpowiedzialnością względem osób trzecich chronią przed odpowiedzialnością z tytułu utraty danych osób fizycznych lub poufnych danych korporacyjnych.

Ochrona obejmuje między innymi:

- prywatność – nieskuteczną ochronę dokumentów i danych w postaci fizycznej lub cyfrowej,
- bezpieczeństwo sieci – udział w rozprzestrzenieniu cyberataku,
- treść – naruszenie praw własności intelektualnej poprzez nieprawidłowe zarządzanie danymi i nośnikami lub zaniedbania w tym zakresie,
- ograniczony dostęp – ograniczenie klientom dostępu do systemów komputerowych ubezpieczonego, np. do stron internetowych, w efekcie ataku na system,
- reputacja – zniesławienie lub naruszenie prywatności w wyniku działań w cyberprzestrzeni.

Sekcje związane z kosztami i szkodami własnymi zaprojektowano tak, aby zminimalizować skutki incydentów związanych z cyberprzestrzenią.

Ochrona obejmuje między innymi:

- koszty informowania o naruszeniach prywatności,
- utratę zysku w wyniku zakłócenia działalności,
- koszty odzyskania i odtworzenia danych, w tym podwyższone koszty robocizny i sprzętu,
- kwotę okupu oraz inne koszty związane z wymuszeniem komputerowym,
- koszty zarządzania kryzysowego po wystąpieniu incydentu.

W zakresie dopuszczonym przez prawo zapewniamy również ochronę przed sankcjami nakładanymi przez organy nadzoru w przypadku naruszeń prywatności. Powyższe obejmuje koszty obrony, kary administracyjne oraz odszkodowania wypłacane konsumentom.

Jaki jest limit?
Maksymalny limit odpowiedzialności to łącznie 25 mln euro.

Dlaczego Chubb?

Specjalistyczna wiedza o cyberzagrożeniach.
Jesteśmy światowym liderem w zakresie ubezpieczeń ryzyk cybernetycznych od 2001 r.

Globalny zasięg
Nasze polisy zapewniają ochronę ubezpieczeniową, która pozwala sprostać stale rosnącym i zmieniającym się wymaganiom regulatorów. Dysponujemy lokalnymi zespołami likwidatorów szkód oraz specjalistów ds. reagowania na incydenty w 54 państwach, w tym również wyspecjalizowanymi zespołami ds. ryzyka cybernetycznego na kluczowych dla nas rynkach na całym świecie. Pozwala nam to świadczyć w sposób spójny najwyższej jakości usługi na całym świecie.

Ubezpieczenie ryzyka cybernetycznego w przedsiębiorstwie (Cyber ERM).
Dzięki naszemu holistycznemu podejściu do ochrony ubezpieczeniowej poza szeroką ochroną w ramach polisy oferujemy również usługi oceny ryzyka cybernetycznego, zarządzania kryzysowego po wystapieniu incydentu oraz możliwość transferu części ryzyka na ubezpieczyciela.

Niniejsza karta informacyjna jest przeznaczona do użytku wyłącznie przez brokerów ubezpieczeniowych. Ma charakter informacyjny. W dokumentach polisowych przedstawiono wszystkie warunki świadczenia usług oraz mające zastosowanie wyłączenia.

> Co trzeba wiedzieć o RODO?

Kontakt

Aby dowiedzieć się więcej o naszych usługach ERM związanych z cyberryzykiem, zachęcamy do odwiedzenia strony internetowej Chubb www.chubb.com.pl lub do kontaktu z naszymi przedstawicielami.

Chubb. Insured.℠

Zawartość tego materiału służy wyłącznie celom informacyjnym i nie stanowi osobistej porady ani zalecenia związanego z produktem lub usługą dla żadnej osoby lub firmy. Zapoznaj się z dokumentacją dotyczącą polisy wydaną w celu uzyskania pełnych Ogólnych Warunków Ubezpieczenia.

Chubb European Group SE Spółka Europejska Oddział w Polsce, z siedzibą w Warszawie, adres: ul. Królewska 16 00-103 Warszawa, wpisany do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego, prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000233686, NIP 1080001001, REGON 140121695, notyfikowany Komisji Nadzoru Finansowego. Chubb European Group SE jest zakładem ubezpieczeń podlegającym przepisom francuskiego kodeksu ubezpieczeń, zarejestrowanym w Rejestrze Działalności Gospodarczej i Rejestrze Spółek (Registres du Commerce et des Sociétés – RCS) w Nanterre pod numerem 450 327 374, z siedzibą we Francji, adres: La Tour Carpe Diem, 31 Place des Corolles, Esplanade Nord, 92400 Courbevoie, Francja. Chubb European Group SE posiada kapitał zakładowy w wysokości 896,176,662 EUR, opłacony w całości.

MPAGDPR201807231445