

Ogólne rozporządzenie o ochronie danych

Ogólne rozporządzenie o ochronie danych osobowych (RODO), to rozporządzenie Unii Europejskiej (UE) ustanawiające nowe przepisy dotyczące przetwarzania i ochrony danych osobowych obywateli UE.

Nakłada ono nowe obowiązki i odpowiedzialność prawną na wszystkie organizacje przetwarzające dane osobowe, a także daje osobom fizycznym nowe prawa dotyczące sposobu, w jaki ich dane są gromadzone, przetwarzane i przechowywane.

Konsekwencje RODO

Jeśli Twoją organizację obowiązują zapisy RODO, istnieje wiele kwestii, które należy dokładnie przeanalizować. Zalecamy zasięgnięcie porady prawnej w celu ustalenia, jakie kroki należy podjąć w Twojej sytuacji.

1. Wiedza na temat danych

Należyta ochrona danych oznacza zrozumienie sposobu ich traktowania w Twojej organizacji – przetwarzania, udostępniania, stosowania, archiwizowania i usuwania. Wiedza na temat danych oraz ich stosowania i przechowywania to kluczowy wymóg dotyczący budowania strategii RODO organizacji.

2. Określenie własności i rozliczalności

Ważne jest, aby zidentyfikować osobę odpowiedzialną za zgodność z przepisami dotyczącymi ochrony danych. W niektórych organizacjach wyznaczenie inspektora ochrony danych jest wymogiem. RODO wprowadziło również nową zasadę „rozliczalności”, która wymaga od organizacji przyjęcia programu zgodności z przepisami dotyczącymi ochrony danych. Organizacje mają obowiązek opracować wewnętrzne zasady ochrony danych i zapewnić szkolenie personelu w tym zakresie.

3. Zapewnienie podstawy prawnej przetwarzania

Kolejny element RODO, który firmy muszą zapewnić, to udokumentowana podstawa prawna przetwarzania różnych typów danych osobowych, z którymi mają do czynienia. Jeśli na przykład firma używa zgody jako podstawy przetwarzania, należy wówczas określić sposób jej uzyskiwania i umieć jasno wykazać sposób i czas jej wydania.

4. Rozumienie praw podmiotów danych

Aby zapewnić przestrzeganie praw w odniesieniu do danych osobowych, należy je najpierw poznać i zrozumieć. Na przykład podmioty danych osobowych mają prawo dostępu do swoich danych osobowych, a także do ich sprostowania, usunięcia lub wyeksportowania drogą elektroniczną. W pewnych okolicznościach użytkownicy mają również prawo sprzeciwić się zautomatyzowanemu podejmowaniu decyzji i profilowaniu.

5. Zapewnienie prywatności w fazie projektowania (privacy by design)

Prywatność w fazie projektowania stała się wyraźnym wymogiem, dlatego ważne, aby uwzględnić sposób wprowadzenia jej w procesy biznesowe. W niektórych okolicznościach konieczne jest również przeprowadzenie oceny wpływu na prywatność.

6. Przygotowanie do zarządzania naruszeniami

Aktualizacja i sprawdzanie zasad i procesów zarządzania naruszeniami danych mają kluczowe znaczenie w skutecznym programie ochrony danych. RODO wymaga wykrywania i terminowego zgłaszania naruszeń do właściwych organów, ponieważ za niezgłoszenie lub naruszenie grozi kara.

7. Przekazywanie istotnych informacji

Upewnienie się, że polityka prywatności organizacji i inne powiadomienia są aktualne i obejmują praktyki ochrony danych. Nowe wymagania obejmują szczegółowe określenie podstawy prawnej przetwarzania danych i powiadomienie użytkowników o organach, w których mogą wnieść skargę, jeśli wystąpi problem.

8. Współpraca z dostawcami

Spełnienie zobowiązań w zakresie RODO wykracza poza wewnętrzne zasady organizacji. Wszystkie osoby trzecie przetwarzające dane osobowe w imieniu firmy muszą również przestrzegać niezbędnych standardów ochrony danych. Niektóre pytania, które można zadać swoim dostawcom:

- Czy stosują skuteczne zasady w zakresie bezpieczeństwa sieci i informacji, prywatności oraz ochrony danych?
- Czy przestrzegają międzynarodowych norm i weryfikują zgodność z nimi?
- W jaki sposób mogą udowodnić, że posiadają głęboko zakorzenioną kulturę zaufania i bezpieczeństwa? Jakie mechanizmy kontrolne stosują, aby pomóc Twojej firmie zarządzać danymi i spełnić swoje obowiązki w roli administratora?



Dropbox: Ochrona Twoich danych

Zaufanie jest podstawą naszych relacji z milionami ludzi i firm na całym świecie.

Cenimy sobie fakt, że nam ufasz, i poważnie traktujemy odpowiedzialność za ochronę Twoich informacji. Aby zasłużyć na Twoje zaufanie, zbudowaliśmy i będziemy nadal rozwijać Dropbox z naciskiem na bezpieczeństwo, zgodność i prywatność.

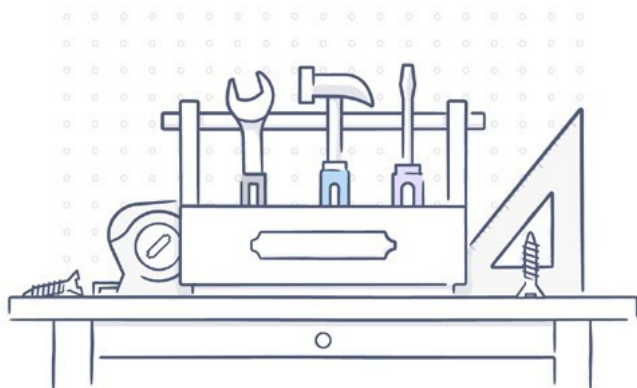
Bezpieczeństwo: ochrona i kontrola

Ochrona: Architektura i bezpieczeństwo informacji

Usługa Dropbox została zaprojektowana w oparciu o bezpieczną, rozproszoną infrastrukturą z wieloma warstwami ochrony, w tym z bezpiecznym transferem danych, szyfrowaniem, konfiguracją sieci i kontrolą na poziomie aplikacji, rozproszonymi w skalowalnej i bezpiecznej infrastrukturze. Skuteczna struktura zarządzania bezpieczeństwem informacji ma na celu ocenę ryzyka i budowanie kultury bezpieczeństwa w usłudze Dropbox. Regularnie sprawdzamy i aktualizujemy zasady bezpieczeństwa, zapewniamy naszym pracownikom szkolenia w zakresie bezpieczeństwa, przeprowadzamy testy bezpieczeństwa aplikacji i sieci (w tym testy penetracyjne), przeprowadzamy oceny ryzyka i monitorujemy zgodność z zasadami bezpieczeństwa. Szczegółowe informacje na ten temat można znaleźć w [Dropbox Business Security White Paper](#).

Kontrola: wspieranie administratorów IT

Dropbox zapewnia funkcje kontroli i widoczności wymagane przez administratorów IT, ułatwiając łatwiejsze zarządzanie obowiązkami w zakresie zgodności. Nasz panel administratora umożliwia monitorowanie aktywności zespołu, przeglądanie podłączonych urządzeń i sprawdzanie informacji dotyczących audytu. Aby łatwo zarządzać dostępem członków zespołu do określonych folderów, można tworzyć grupy – wtedy menedżer folderu zespołu zapewnia widoczność i kontrolę nad folderami, w tym zarządzanie synchronizacją. Funkcja zgody na link oznacza możliwość zabezpieczenia hasłem udostępnionych linków, ustawić daty wygaśnięcia, aby udzielić tymczasowego dostępu i ograniczyć dostęp do linków stosowanych w Twojej organizacji. Nasze narzędzie do transferu między kontami umożliwia łatwe przenoszenie plików między użytkownikami, gdy ich obowiązki ulegną zmianie. Zdalne czyszczenie umożliwia usuwanie plików z zagubionych lub skradzionych urządzeń.



Zgodność: zaufanie i weryfikacja

Procedura zgodności to skuteczny sposób sprawdzania wiarygodności usługi. Zachęcamy Cię do tego i oczekujemy, że zweryfikujesz zgodność naszej praktyki bezpieczeństwa z najpopularniejszymi normami i przepisami, np. ISO 27001, 27017, 27018 i SOC 1, 2, i 3. Nasi niezależni audytorzy zewnętrzni sprawdzają nasze kontrole i dostarczają raporty i opinie, które w miarę możliwości udostępniamy użytkownikom. Szczegółowe informacje na temat stosowanych standardów i sposobu weryfikacji praktyk bezpieczeństwa są dostępne na naszej stronie [complianceweb](#).

Prywatność: nasze zaangażowanie

Jesteś właścicielem swoich danych i niezależnie od tego, czy są to Twoje dane prywatne, czy informacje służbowe, poważnie traktujemy zaufanie naszych użytkowników i ciężko pracujemy, aby zapewnić ochronę wszystkich danych w naszych systemach. Nasza Polityka prywatności jasno opisuje, jak obchodzimy się z Twoimi informacjami i jak je chronimy. Publikujemy Raport przejrzystości, a nasze zasady dotyczące rządowych żądań udzielenia informacji wymagają udostępniania informacji na temat tego, jak często otrzymujemy, analizujemy i odpowiadamy na takie żądania. Staramy się również zmieniać przepisy w taki sposób, aby skuteczniej chroniły Twoje dane.

Wspólne działanie w celu zapewnienia bezpieczeństwa danych

Dropbox współpracuje z klientami biznesowymi, aby chronić ich dane. Podejmujemy kompleksowe działania w celu ochrony naszej infrastruktury, sieci i aplikacji, szkolimy pracowników w zakresie praktyk bezpieczeństwa i prywatności, budujemy kulturę, w której zaufanie jest najwyższym priorytetem; poddajemy nasze systemy i praktyki rygorystycznym testom i audytom przeprowadzanym przez zewnętrzne firmy. Klienci odgrywają również kluczową rolę w zapewnieniu ochrony swoich zespołów i danych. Dropbox umożliwia konfigurację, używanie i monitorowanie konta w sposób zgodny z wymogami bezpieczeństwa, prywatności i zgodności z przepisami organizacji. Nasze instrukcje dotyczące wspólnej odpowiedzialności mogą pomóc Ci lepiej zrozumieć działania, jakie podejmujemy, aby Twoje konto było bezpieczne i działania, które możesz podjąć, aby zachować widoczność i kontrolę nad danymi swojego zespołu.

Treść instrukcji służy ułatwieniu dostępu do informacji i nie stanowi porady prawnej. W razie potrzeby odbiorcy powinni zasięgnąć porady prawnej na własną rękę.

