Warszawa, 12.11.2024 r.

Jak budować zaufanie klientów poprzez transparentność w zakresie ochrony danych osobowych?

Ochrona danych to nie tylko kwestia zgodności z przepisami, ale także fundament budowania zaufania i lojalności wśród klientów. W miarę jak konsumenci stają się coraz bardziej świadomi swoich praw do prywatności, organizacje muszą zdawać sobie sprawę, że skuteczna ochrona danych osobowych jest kluczowa dla zachowania wiarygodności marki i utrzymywania trwałych relacji z klientami.
Transparentna komunikacja na temat zarządzania danymi oraz wdrażanie zasady *Privacy by Design* (ochrony prywatności w fazie projektowania) są nie tylko kluczowe dla spełnienia wymogów RODO, ale także dla zapewnienia poczucia bezpieczeństwa wśród klientów i odbiorców usług, którzy udostępniają swoje dane osobowe. Ochrona danych to nie tylko wymóg prawny – to podstawowy filar relacji z klientami.

Jak wskazuje badanie „Privacy as an Enabler of Customer Trust" przeprowadzone przez CISCO[1]:

- 94% organizacji uważa, że ich klienci przestaliby robić zakupy, gdyby firma nie chroniła odpowiednio danych,
- 98% respondentów uznało, że zewnętrzne certyfikaty ochrony prywatności, takie jak ISO 27701 mają istotne znaczenie przy podejmowaniu decyzji o zakupie;
- 81% respondentów stwierdziło, że ich zdaniem sposób, w jaki firma traktuje dane osobowe, odzwierciedla poziom szacunku, jakim darzy swoich klientów. Liczba ta wzrosła o 5% w porównaniu z poprzednimi trzema badaniami, w których odnotowano stałe liczby.
- Z kolei na pytanie o najważniejszą rzecz, jaką organizacje mogą wdrożyć, aby zbudować zaufanie klientów, największa liczba (39%) wskazała na przejrzystość danych.

Są to niektóre z wyników ww. badania, które opiera się na ponad 2600 anonimowych odpowiedziach od specjalistów ds. bezpieczeństwa i prywatności w 12 regionach geograficznych.
W tym artykule przeanalizuję kluczową rolę ochrony danych w budowaniu zaufania klientów, skupiając się na przejrzystej komunikacji oraz zasadzie Privacy by Design – elementach, które nie tylko wspierają zgodność z regulacjami dotyczącymi ochrony danych, ale również wzmacniają pozycję organizacji na rynku.

Przejrzystość – fundament zaufania

Przejrzystość to jeden z kluczowych elementów ochrony danych osobowych zdefiniowanych w RODO. Jest to zasada, która stanowi podstawę budowania zaufania między przedsiębiorcami a odbiorcami ich usług. Artykuł 12 RODO wskazuje, że administratorzy

[1] Amerykańskie przedsiębiorstwo informatyczne, największe w branży sieciowej na świecie, przeprowadzające coroczne badania rynku dot. ochrony prywatności.

danych mają obowiązek dostarczyć osobom fizycznym informacje o przetwarzaniu ich danych osobowych w sposób zrozumiały, łatwy do znalezienia i w sposób przejrzysty. Obejmuje to nie tylko sposób pozyskiwania danych, ale także cel ich przetwarzania, podstawy prawne, czas przechowywania i wszelkie informacje dotyczące praw osób, których dane dotyczą, takich jak prawo do dostępu, sprostowania, usunięcia danych i prawo do sprzeciwu (art. 13 i 14 RODO).

Jak zapewnić przejrzystość w praktyce?

1. **Prosty i zrozumiały język**: Komunikaty dotyczące ochrony danych muszą być napisane w prosty, zrozumiały sposób, bez zbędnego prawniczego żargonu. Klienci powinni jasno rozumieć, w jaki sposób ich dane będą wykorzystywane.

Przykład: Zamiast skomplikowanego języka prawniczego, firma może wskazać: *„Zbieramy Twoje dane kontaktowe, aby wysłać Ci informacje o naszych promocjach. Możesz w każdej chwili zrezygnować z subskrypcji”.*

2. **Struktura informacji**: Ważne informacje muszą być wyraźnie uporządkowane i łatwe do znalezienia. Organizacja powinna zapewnić dostępność polityki prywatności i innych informacji na temat przetwarzania danych.

Przykład: Polityka prywatności może być podzielona na sekcje, takie jak „Rodzaje zbieranych danych”, „Cel przetwarzania danych” i „Twoje prawa”. Dzięki temu klienci szybko znajdą interesujące ich informacje.

3. **Dostępność informacji**: Organizacje muszą zapewnić, że klienci będą mogli łatwo uzyskać dostęp do informacji o przetwarzaniu ich danych w dowolnym momencie. Powinna być ustalona jasna ścieżka dostępu do polityki prywatności na stronie internetowej, w tym łatwe do znalezienia linki i dokumenty.

Przykład: Link do polityki prywatności powinien być widoczny na każdej stronie witryny, a także na stronie rejestracji i w procesie zakupowym, aby klienci mogli zapoznać się z zasadami przetwarzania ich danych.

4. **Wykorzystywanie pomocy wizualnych:** Stosowanie infografik, diagramów lub innych elementów graficznych to świetny sposób na uproszczenie skomplikowanych informacji.

Przykład: Firma ubezpieczeniowa może używać ikon do przedstawiania różnych typów zbieranych danych osobowych, takich jak ikona domu dla zbierania danych do ubezpieczenia dot. nieruchomości lub ikona samochodu dla danych zbieranych w celu ubezpieczenia pojazdu. Taka reprezentacja wizualna zwiększa zrozumienie i zapewnia przejrzystość.

Przejrzystość odgrywa kluczową rolę w budowaniu relacji opartych na zaufaniu między firmą a klientem. Kiedy klienci mają jasność co do sposobu przetwarzania ich danych i wiedzą, że

organizacja działa odpowiedzialnie i zgodnie z prawem, są bardziej skłonni korzystać z jej usług oraz dzielić się swoimi danymi. Transparentność w zarządzaniu danymi zapewnia poczucie bezpieczeństwa i kontroli nad danymi osobowymi.

Privacy by Design

Zasada Privacy by Design jest jednym z kluczowych wymogów wynikających z RODO. Oznacza to, że prywatność powinna być integralną częścią procesów biznesowych, uwzględnianą od samego początku w projektowaniu produktów, usług i systemów, a nie dodawaną jako późniejsza poprawka.
Zgodnie z badaniem „Privacy as an Enabler of Customer Trust", 80% organizacji zauważyło znaczną poprawę w zaufaniu klientów dzięki inwestycjom w ochronę prywatności oraz wdrażaniu zasady Privacy by Design.

Na co zwrócić uwagę podczas projektowaniu procesu z perspektywy odbiorcy usługi?

Nie ma uniwersalnego przepisu, którego organizacje muszą się trzymać, aby wdrożyć zasadę *Privacy by Design*, ponieważ zależy to od rodzaju przetwarzanych danych oraz specyfiki działalności firmy. Niemniej jednak oto kilka kluczowych kwestii, które warto wziąć pod uwagę:

- **minimalizacja danych** - ogranicz gromadzenia danych osobowych do zakresu niezbędnego do realizacji określonego celu,
- **dopasowane informacje o przetwarzaniu danych osobowych** – zaplanuj sposób realizacji obowiązków informacyjnych w momencie gromadzenia danych i pamiętaj o sposobach zwiększania przejrzystości wskazanych w tym artykule,
- **pseudonimizacja –** stosuj pseudonimizację danych (zastąpienie danych umożliwiających identyfikację osoby pseudonimami) w celu minimalizacji ryzyk,
- **automatyczne usuwanie danych** – wprowadź procesy automatycznego usuwania danych osobowych po określonym czasie przechowywania,
- **szczegółowe zgody** – umożliw użytkownikom zarządzanie poszczególnymi uprawnieniami dotyczącymi zbierania ich danych – np. śledzenie lokalizacji, personalizacja reklam,
- **bezpieczeństwo danych osobowych** – zidentyfikuj obszary obarczone ryzykiem przetwarzania i na tej podstawie dobierz odpowiednie środki bezpieczeństwa,
- **obsługa żądań osób** – zaprojektuj sprawny proces obsługi żądań zgłaszanych przez klientów, zadbaj o dobry kanał komunikacyjny oraz kompetentne osoby, które będą obsługiwały takie zgłoszenia,
- **podmioty trzecie** – zweryfikuj potencjalnych dostawców usług, jeśli dostęp do danych osobowych mają mieć też inne firmy (dostawcy usług) i zawrzyj umowy powierzenia przetwarzania danych.

Świadomość klientów

Coraz więcej klientów, oprócz wybierania zaufanych dostawców usług, podejmuje także własne działania w celu ochrony swoich danych osobowych. Incydenty związane z naruszeniami ochrony danych oraz powszechne przekonanie, że środowisko technologiczne

nie szanuje prywatności użytkowników ani nie zapewnia odpowiedniej przejrzystości w zakresie danych, przyczyniają się do wzrostu świadomości wśród konsumentów.
Ww. raport Cisco wykazał, że:

- 58% osób dokładnie czyta i upewnia się, że rozumie informacje o prywatności przed ich zaakceptowaniem;
- 53% respondentów aktywnie zarządza swoimi preferencjami dotyczącymi plików cookie online;
- 46% osób posiadających mikrofony na swoich urządzeniach wycisza je, gdy nie są używane.

Te aktywności wskazują, że konsumenci o wyższej świadomości technologicznej, podejmują działania w celu zabezpieczenia swoich danych, a w konsekwencji tego korzystają również tylko z zaufanych stron/sklepów/serwisów/aplikacji.

Podsumowanie

Ochrona danych to nie tylko obowiązek wynikający z przepisów, lecz także kluczowy element w budowaniu zaufania i lojalności klientów. W dobie rosnącej świadomości klientów organizacje muszą zdawać sobie sprawę, że ochrona danych osobowych jest kluczowa dla utrzymania wiarygodności marki i nawiązywania trwałych relacji z klientami.
Przejrzysta komunikacja w zakresie zarządzania danymi oraz wdrażanie zasady Privacy by Design są niezbędne nie tylko do spełnienia wymagań RODO, ale także do zapewnienia klientom poczucia bezpieczeństwa przy udostępnianiu swoich danych przedsiębiorstwom.

Nina Zacharska - specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.