WYKAZ DOKUMENTACJI RODO WRAZ Z OPISEM

Aby ułatwić zarządzanie dokumentacją RODO, została podzielona na dwie kategorie:

dokumentację wewnętrzną – przeznaczoną wyłącznie do użytku wewnątrz firmy. Nie są udostępniane klientom ani innym podmiotom. Należy je regularnie aktualizować;

dokumentację zewnętrzną - to dokumenty, które należy przekazać swoim klientom, kontrahentom lub innym podmiotom albo umożliwić do nich dostęp jakiejś grupie odbiorców, zgodnie z instrukcjami.

Dokumentacja wewnętrzna RODO – w pliku dokumenty wew. RODO

Dokumenty wewnętrzne firmy, które należy na bieżąco uzupełniać w razie zmian.

1. Polityka ochrony danych osobowych

Jest to dokument, który odnosi się do wszystkich kwestii związanych z przetwarzaniem danych osobowych w firmie w sposób ogólny – czyli gdzie dane mogą być przetwarzane, ile czasu je przechowywać, w jaki sposób je przetwarzać itd.

Dokument należy również na bieżąco uzupełniać, jeśli coś się zmieni w firmie w zakresie przetwarzania danych osobowych, np. zostaną wprowadzone inne zabezpieczenia albo np. dojdzie dodatkowe miejsce, gdzie mogą być przetwarzane dane osobowe w firmie, np. dodatkowe biuro stacjonarne. Dokument do zapoznania się i do podpisu na końcu. Dokumenty nigdzie nie publikujemy, jedynie udostępniamy do zapoznania osobom, które będą z Panią współpracują albo będą współpracować w przyszłości i otrzymają dostęp do danych osobowych użytkowników strony, czy klientów. Po zapoznaniu się z dokumentem, osoba, która się z nim zapoznała, powinna wpisać się w dokumencie ,,7. Ewidencja osób, które zapoznały się z dokumentami dot. danych osobowych.'' Mogą to być np. osoby zatrudnione na zleceniu, czy mające dostęp do danych klientów w ramach b2b.

2. Rejestr czynności przetwarzania danych osobowych

Rejestr czynności przetwarzania danych to spis wszystkich działań, jakie firma wykonuje na danych osobowych. To jak lista, która pokazuje:

- jakie dane są zbierane (np. dane klientów, użytkowników),
- w jakim celu są przetwarzane (np. zawarcie umowy, kontakt),
- komu te dane są lub mogą być przekazywane,
- jak długo dane są przechowywane.

Ten dokument należy aktualizować, jeśli zmienią się, czy dojdą kolejne zakresy przetwarzania danych osobowych. W zasadzie jest to bardziej szczegółowa polityka prywatności. Jeśli więc w firmie dane przetwarzane są jedynie w obrębie strony internetowej, zapisy są powielone, lecz bardziej rozbudowane. Jeśli natomiast dane w firmie są przetwarzane jeszcze w jakiś sposób poza stroną, wtedy należy wskazać to w rejestrze czynności przetwarzania. U Pani na razie dane stricte poza stroną, przetwarzane są na social mediach firmowych, co zostało tam uwzględnione. Tego dokumentu również nigdzie nie należy publikować, jedynie przechowywać w dokumentacji wewnętrznej i oczywiście w razie konieczności aktualizować.

3. Rejestr incydentów i naruszeń danych osobowych

Dokument wewnętrzny w dokumentacji RODO, nie należy go nigdzie publikować, lecz przechowywać w dokumentacji firmowej i w razie incydentów lub naruszeń uzupełniać.

Poniżej wyjaśnienie kiedy mamy do czynienia z incydentem, a kiedy z naruszeniem. Więcej w tym zakresie znajduje się w dokumencie ,,Polityka ochrony danych osobowych'' (pkt 1).

Incydent – to zdarzenie związane z bezpieczeństwem informacji - wewnętrzne zdarzenia losowe, awarie komputera, serwera, dysków, pomyłki informatyków, utrata danych, umyślne incydenty jak np. kradzież danych, sprzętu, czy inne jak zgubienie laptopa, pendrive'a, nieprawidłowo zaadresowana korespondencja elektroniczna, czy papierowa zawierająca dane osobowe, atak hakerski, phishing.

Naruszenie to incydent, który powoduje duże prawdopodobieństwo naruszenia praw lub wolności osób fizycznych – wtedy należy niezwłocznie zgłosić zdarzenie do organu nadzorczego oraz poinformować osoby poszkodowane.

4. Ewidencja umów powierzenia przetwarzania danych osobowych

Dokument należy każdorazowo uzupełniać, poprzez wskazywanie podmiotów, z którymi firma ma zawarte umowy powierzenia przetwarzania danych osobowych. Dokument wewnętrzny w dokumentacji RODO, nie należy go nigdzie publikować, lecz przechowywać w dokumentacji firmowej.

5. Ewidencja wniosków dotyczących danych osobowych

Teoretycznie każda osoba, której dane osobowe firma przetwarza, ma prawa względem swoich danych osobowych, np. prawo do ich sprostowania, czy usunięcia.

Ewidencja wniosków jest to dokument wewnętrzny firmy i jeśli ktoś złożyłby wniosek dot. swoich danych osobowych, należy uzupełnić tabelę w ewidencji. W praktyce rzadko się to zdarza. Dotyczy raczej sytuacji, gdy dane są przetwarzane w celach marketingu, który jest prowadzony bez podstawy prawnej. Dokument wewnętrzny w dokumentacji RODO, nie należy go nigdzie publikować, lecz przechowywać w dokumentacji firmowej i w razie potrzeby uzupełniać.

6. Ewidencja osób upoważnionych do przetwarzania danych osobowych

Dokument wewnętrzny – nie należy go nigdzie publikować, lecz należy uzupełniać, o każdą osobę, która została upoważniona do przetwarzania danych osobowych, na podstawie wzoru upoważnienia, o którym mowa w pkt 5 poniżej - dokumentacji zewnętrznej.

7. Ewidencja osób, które zapoznały się z dokumentami dot. ochrony danych

Każda osoba upoważniona do danych firmy, czyli pracownik, współpracownik, osoba na b2b, powinna zostać zapoznana z ,,Polityką ochrony danych'' i z ,,Instrukcją zarządzania systemem informatycznym''. Po zapoznaniu najlepiej to udokumentować, w taki sposób, aby ta osoba wpisała się do tej właśnie ewidencji. Dokument wewnętrzny – nie należy go nigdzie publikować, lecz należy uzupełniać, o każdą osobę, która została upoważniona do przetwarzania danych osobowych i zapoznana z dokumentami, o których mowa w zdaniu poprzednim.

8. Instrukcja zarządzania systemem informatycznym

To dokument odnoszący się do zabezpieczeń stosowanych w systemach informatycznych. Można go stosować również jako źródło wiedzy w zakresie tego w jaki sposób dane przetwarzać i jak je zabezpieczać, czy przechowywać, np. jak zabezpieczać laptopa służbowego hasłem itp.

Dokument wewnętrzny – nie należy go nigdzie publikować, lecz należy aktualizować, jeśli coś się zmieni (np. pojawi się nowe zabezpieczenie) oraz okazać osobom upoważnionym do przetwarzania danych (osobom, które będą z Panią współpracować w przyszłości i uzyskają dostęp do danych klientów, użytkowników strony (np. do programów, do laptopów, czy telefonów służbowych).

9. Zapewnienie ciągłości komunikacji i formularz – test równowagi

Test równowagi to dokument, który sprawdza, czy interes firmy (administratora) w przetwarzaniu danych jest ważniejszy niż ewentualna niewygoda lub naruszenie prywatności osoby, której dane dotyczą.

Pomaga ocenić, czy firma może legalnie przetwarzać dane na podstawie tzw. prawnie uzasadnionego interesu. Sprawdza, czy dane są niezbędne do celu, czy nie można osiągnąć tego celu w mniej inwazyjny sposób oraz czy prawa i wolności osób nie są nadmiernie naruszane.

To wewnętrzny dokument – nie przekazuje się go klientom, lecz przechowuje w dokumentach firmowych na wypadek kontroli. Dokument przesłany w dokumentacji dotyczy przetwarzania danych w celach kontaktowych i wskazanych w formularzu kontaktowym na stronie.

10. Działania marketingowe social media – test równowagi

11. Prezentowanie opinii – test równowagi

Jak powyżej, w pkt 9, z tą różnicą, że dotyczy prowadzenia kont na social mediach i prezentowania opinii.

Jeśli w przyszłości będzie Pani chciała przetwarzać dane w inny sposób na podstawie prawnie uzasadnionego interesu administratora, należy najpierw również przeprowadzić test równowagi, na wzór przesłanych dokumentów.

Dokumentacja zewnętrzna RODO – w pliku dokumenty zew. RODO

Zewnętrzna w tym kontekście nie oznacza, że dokumenty publikujemy gdzieś, np. na stronie, tylko przekazujemy np. do podpisu, czy do zapoznania się innym podmiotom zewnętrznym, np. firmie księgowej, z którą zawiera Pani umowę, czy informatykowi, który ma wprowadzać zmiany na stronie. Każdy dokument ma w tym zakresie nieco inny wymóg, opisany bezpośrednio przy danym punkcie.

1. Klauzula informacyjna do umów

Klauzula RODO do umowy, powinna służyć jako załącznik do zawieranych umów z innymi podmiotami, w szczególności z przedsiębiorcami.

Przykładowo, jeśli będę Pani zawierać umowę współpracy w zakresie poprawek na stronie, przy zawieraniu umowy o świadczenie danej usługi, do takiej umowy, należy zamieścić załącznik w postaci klauzuli informacyjnej RODO, w którym poinformuje Pani m.in. w jakim zakresie, w jakim celu przetwarzane są dane otrzymane w ramach zawartej umowy.

Każda ze stron umowy jest zobowiązana do poinformowania drugiej o przetwarzaniu danych osobowych. Zwykle każda strona dostarcza swoją klauzulę informacyjną. Jednak dla uproszczenia i w celu ujednolicenia dokumentacji, można umieścić klauzule jako załączniki do umowy, co zapewnia przejrzystość i jednoznaczność w relacjach biznesowych.

Czy klauzula musi być załącznikiem do umowy?

Nie musi. Klauzula może być przekazana w inny sposób, np. w odrębnym dokumencie, mailowo. Ważne jest, aby druga strona była poinformowana przed rozpoczęciem przetwarzania jej danych.

2. Treść stopki mailowej i wyjaśnienia

Wyjaśnienia są zawarte w pliku ,,Treść stopki mailowej RODO''.

3. Umowa powierzenia przetwarzania danych osobowych - wzór

Do zawierania z podmiotami, którym firma przekazuje dane, którymi sama administruje, czyli je przetwarza, np. dane swoich klientów, użytkowników strony, współpracowników. Przykładowo, jeśli będzie Pani zawierać umowę z firmą księgową, która będzie mieć dostęp do danych osobowych kontrahentów, którym wystawiane są fv, do danych klientów. Firma księgowa jest więc podmiotem przetwarzającym dane i należy z nią zawrzeć taką umowę. Może to być też np. podmiot obsługujący e-mail marketing, który ma bazę danych mailowych i wysyła do potencjalnych klientów informacje handlowe, marketingowe. Jeśli firmy, którym powierza się dane nie wyjdą z inicjatywą i taka umowa nie będzie załącznikiem do umowy podstawowej, czy do akceptowanego regulaminu, administrator powinien sam dostarczyć umowę powierzenia, bo odpowiada przed osobami, których dane przetwarza i przekazuje dalej, a więc odpowiada również za to, żeby wyjść z inicjatywą w kwestii ich zabezpieczenia.

Warto tutaj nadmienić, że administrator powinien korzystać wyłącznie z usług takiego podmiotu przetwarzającego, który daje odpowiednie gwarancje spełnienia wymogów wynikających z RODO. Współpraca z podmiotami niedającymi odpowiednich gwarancji powinna zostać wykluczona. Ciężar odpowiedzialności za dokonanie odpowiedniego wyboru spoczywa na administratorze. Warto więc zwracać uwagę, jakie wybiera Pani firmy hostingowe, chmurowe, do obsługi newslettera, czy wszelkie inne, które mają dostęp do danych użytkowników, klientów. Najlepiej sprawdzić w ich politykach, umowach, regulaminach w jaki sposób te firmy przetwarzają powierzane im dane, czy przekazują je poza EOG, a jeśli tak, czy są jakieś zabezpieczenia.

Na podstawie zawartych umów powierzenia przetwarzania danych osobowych, należy prowadzić kolejny dokument, który znajduje się w pliku dokumentacja wewnętrzna, czyli ewidencję umów powierzenia przetwarzania danych osobowych.

4. Odwołanie upoważnienia do przetwarzania danych osobowych – wzór

Do podpisu po zakończeniu współpracy z osobą, która miała dostęp do danych, wygaśnięciu umowy zlecenie, umowy o dzieło, czy b2b.

5. Upoważnienie do przetwarzania danych osobowych - wzór

Dokument do przekazania do podpisu osobie, z którą firma współpracuje i która będzie mieć dostęp do danych osobowych przetwarzanych w firmie, np. osoba na zleceniu, na umowie b2b. Dokument dotyczy wszystkich pracowników, zarówno tych zatrudnionych na podstawie

umowy o pracę (gdyby takie osoby pojawiły się w przyszłości), jak i umów cywilnoprawnych, np. umowy zlecenie, b2b czy o dzieło.

6. Oświadczenie o zobowiązaniu się do zachowania poufności danych osobowych - wzór

Dokument do podpisu dla pracownika, współpracownika (zlecenie/dzieło/b2b), który otrzymał dostęp do danych na podstawie upoważnienia do przetwarzania danych osobowych.

7. Klauzula informacyjna Instagram i Facebook

Klauzula informacyjna dotycząca przetwarzania danych użytkowników na Instagramie. Można zamieścić ją na dysku i na koncie firmowym na Instagramie i Facebooku zamieścić link do klauzuli RODO.