Przetwarzanie danych osobowych uczestników wydarzeń zgodnie z RODO

Poradnik dla organizatorów konferencji, kongresów, szkoleń i innych wydarzeń

Autorzy: Łukasz Krawczuk (CONREGO),
Przemysław Kilian (rodoszczecin.pl)

Wydanie VII, 2021.01

Interaktywny spis treści

Od autorów

Ten poradnik dedykujemy organizatorom wydarzeń. Jednak nawet jeśli nie jesteś organizatorem, to i tak znajdziesz tu wiele wartościowych informacji, bo RODO zapewne dotyczy też Ciebie.

Przedstawiamy wymogi narzucone przez przepisy oraz metody jakimi możesz się do nich dostosować. To wspólne działanie, ponieważ każda organizacja (Twoja i nasza), która gromadzi, przechowuje lub przetwarza dane osobowe w jakikolwiek sposób, musi podjąć działania w celu zapewnienia bezpieczeństwa danych. Wyjaśnimy więc obowiązki poszczególnych stron w sekcji **Zgodność krok po kroku**. Jeśli już wiesz, czym jest RODO, rozumiesz jakie wymogi stawia administratorom i wiesz, że musisz się dostosować - śmiało przejdź na stronę nr 5.

Czym jest RODO?

RODO, czyli Rozporządzenie Ogólne o Ochronie Danych Osobowych jest unijnym rozporządzeniem, mającym na celu ujednolicenie, modernizację i wzmocnienie ochrony danych osobowych. Weszło w życie 25 maja 2018 roku.

Warto pamiętać iż ochrona danych osobowych w Polsce nie jest niczym nam obcym. RODO, zastępuje naszą rodzimą Ustawę o ochronie danych osobowych z roku 1997.

Celem regulacji jest zapewnienie swobodnego przepływu danych osobowych pomiędzy państwami członkowskimi, ale także wprowadzenie zasad, zgodnie z którymi przetwarzanie danych osobowych będzie ujednolicone na terenie całej Unii Europejskiej.

Kogo dotyczy RODO?

W skrócie: każdą organizację działającą w Unii Europejskiej, która gromadzi lub przetwarza dane osobowe oraz organizacji, które gromadzą lub przetwarzają dane osobowe obywateli UE. W szczególności są to:

Administrator Danych

Administrator danych osobowych to podmiot, który przetwarza dane osobowe, wykorzystując je we własnych celach. Jeżeli uznamy, że nasze dane są przetwarzane przez administratora w sposób niewłaściwy lub są nieaktualne, mamy prawo do ich aktualizacji bądź możemy żądać zaprzestania ich przetwarzania.

Zgodnie z RODO administratorem danych osobowych nie jest osoba, która przetwarza dane w celach osobistych lub domowych, np. kolega, któremu daliśmy nasz numer telefonu czy adres e-mailowy, lub ciocia, której co roku wysyłamy list polecony na urodziny.

Procesor Danych

Zgodnie z definicją zawartą w (RODO), za podmiot przetwarzający powierzone dane osobowe (Procesor) uznaje się: osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Oznacza to dostawców rozwiązań technicznych - producentów systemów rejestracji uczestników i aplikacji eventowych - nas. Trzymamy dane w bazach, upewniamy się, że są odpowiednio zabezpieczone i że masz możliwość łatwo dostosować się do RODO. Czasami też procesujemy dane w Twoim imieniu.

Dlaczego powinno Cię to obchodzić?

Wizerunek

RODO stawia przed nami wyzwania natury technicznej i organizacyjnej, ale zostało tak zaprojektowane, żeby zapewnić kontrolę nad danymi przetwarzanymi przez organizacje. Można powiedzieć, że RODO obliguje Cię do szanowania prywatności uczestników oraz promuje transparentność i poprawność przetwarzanych danych osobowych. Chcesz, żeby Twoim uczestnikom przyjemnie korzystało się z Twoich usług? Zadowoleni uczestnicy polubią Twojego klienta (albo Ciebie), co zwiększy prawdopodobieństwo, że wezmą udział w następnych wydarzeniach. Jednak w tym punkcie chodzi głównie o Ciebie. Większość z nas chce być lubiana - i to nie tylko ze względów finansowych. Nie chcesz, żeby Twoja marka była postrzegana jako zła i chciwa korporacja, prawda? Szczerość potrafi dużo zdziałać.

Zysk

Punkt nieco związany z poprzednim, ale jest w tym jeszcze coś. Ogólnie przyjmuje się, że dobrze postrzegana, transparentna i uczciwa marka zwiększa przychód. Dzieje się tak, ponieważ:

- uczestnicy chętniej zaufają tej marce w przyszłości,
- Twoi pracownicy będą lepiej się czuli, utożsamiając się z wartościami marki i będą pracowali wydajniej.

Inną sprawą, którą chciałbym poruszyć, jest Twoja lista kontaktów i listy kontaktów Twoich klientów i sponsorów. Chodzi o to, że w świetle RODO musisz zbierać osobne zgody na wykorzystywanie danych do celów marketingowych i do przekazywania ich innym organizacjom. Co za tym idzie, prawdopodobnie nie będziesz już zbierać tak wielu kontaktów marketing-owych, a jeszcze mniej dodasz do list marketingowych sponsorów. Z drugiej strony, jak już zbierzesz kontakty, które wyraziły zgodę na przetwarzanie danych do wszystkich celów, to zyskasz naprawdę zainteresowaną bazę odbiorców. Pozwoli Ci to na zbudowanie zdrowej listy kontaktów. Dzięki temu możesz skupić zasoby na kontaktach, które prawdopodobnie przyniosą zysk, zamiast kierować komunikację do osób zupełnie niezainteresowanych.

Kary

Prezes UODO może nałożyć karę pieniężną do **20 mln euro** lub **4% obrotu za najpoważniejsze naruszenia**, m.in. zasad przetwarzania danych, praw osób, których dane dotyczą, lub niestosowanie się do nakazów organu nadzorczego, a za pozostałe naruszenia – do **10 mln euro** lub **2% obrotu**, w zależności od tego, która kwota jest wyższa. Poza karami pieniężnymi Prezes UODO może wydawać nakazy związane z przywróceniem zgodności z RODO, a nawet nakazać ograniczenie przetwarzania wyłącznie do przechowywania, co może zatamować proces biznesowy i być bardziej dotkliwe niż kara pieniężna. Ponadto pracownik, który narusza RODO, powinien liczyć się także z odpowiedzialnością odszkodowawczą w przypadku pozwu, karną w przypadku zawiadomienia do prokuratury lub dyscyplinarną w przypadku niestosowania się do wewnętrznych polityk i procedur.

Zgodność z RODO krok po kroku

Wiesz, że musisz się dostosować i rozumiesz dlaczego. Ale jak się do tego zabrać? Opiszę wszystkie najważniejsze zmiany, które trzeba wziąć pod uwagę oraz przedstawię, co musisz zrobić (i co my zrobiliśmy), żeby się dostosować.

Zgoda

To oczywiste, że potrzebujesz zgody, ale kilka rzeczy się zmieniło:

- **zgoda musi być aktywna** - koniec domyślnie zaznaczonych checkbox'ów i klauzul braku zgody,
- **transparentność co do celu przetwarzania danych** - dla Ciebie to oczywiste, że część danych musisz przekazać obsłudze obiektu albo hotelowi, ale musisz o tym poinformować uczestników. Do tego musisz wskazać (wraz z nazwą) organizacje, które będą miały dostęp do danych. Już nie wystarczy wskazać branży, musisz przedstawić konkretne organizacje i cele,
- **osobne klauzule dla osobnych celów przetwarzania danych** - zgoda na przetwarzanie do celów marketingowych musi teraz być osobną klauzulą i nie może być wymagana. Podczas rejestracji na wydarzenie podstawowym celem jest obsługa podczas tego wydarzenia. Marketing jest osobną kwestią i tak też musi być traktowany,
- **przekazywanie danych osobowych stronom trzecim** - jeśli chcesz przekazywać dane wystawcom, musisz takie zgody umieścić w osobnych klauzulach wraz z nazwami wystawców. Jeśli chcesz, żeby uczestnicy wyrażali zgodę na podstawie skanowania identyfikatorów przy stoiskach wystawców, taka informacja musi być umieszczona w widocznym miejscu.

Co musisz zrobić, żeby się dostosować?

Upewnij się, że Twoje klauzule są precyzyjne, szczegółowe i odpowiednio podzielone. Utwórz ich treść zgodnie z powyższymi punktami i będzie dobrze.

Co my zrobiliśmy, żeby się dostosować?

W CONREGO możesz dodać dowolną ilość klauzul do formularza rejestracyjnego i dodać do nich odnośniki do plików z regulaminami. Dla każdej integracji z zewnętrznymi usługami przetwarzania danych, możesz utworzyć regułę, na podstawie której tylko uczestnicy zaznaczający konkretną klauzulę zostaną automatycznie dodani do usługi zewnętrznej. Co więcej, każda klauzula jest zapisywana w rekordzie uczestnika, dzięki czemu możesz udowodnić, że posiadasz wymaganą zgodę i wskazać IP, z którego zgoda została udzielona.

Obowiązkowe powiadomienie o wycieku

W razie incydentu należy jak najszybciej usunąć jego skutki, opisać jego okoliczności i planowaną reakcję, a także – jeśli występuje taki obowiązek – zgłosić naruszenie wraz z wymaganą dokumentacją bez zbędnej zwłoki, w ciągu 72 godzin, organowi nadzorczemu i osobom, których dotyczą dane objęte naruszeniem.

Co musisz zrobić, żeby się dostosować?

Cóż, monitoruj rekordy rejestracji.

Co my zrobiliśmy, żeby się dostosować?

Niewiele możemy w tej kwestii zrobić, bo z założenia skutecznych ataków nie da się automatycznie wykryć. Ataki wykryte są blokowane bez szkody dla danych. Wszystkie dane, które przechowujemy i przetwarzamy, znajdują się na serwerze znajdującym się na terenie Unii Europejskiej. Inne dane, takie jak obrazy i dokumenty, przechowywane są w chmurze Amazona, która również jest zgodna z RODO.

Prawo dostępu

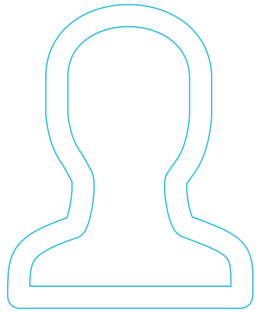
Każdy uczestnik albo inna osoba, której dane przechowujesz lub przetwarzasz, ma prawo zażądać od Ciebie kompletu dotyczących go danych, które przechowujesz. Masz obowiązek dostarczyć te dane w powszechnie używanym formacie cyfrowym w terminie 30 dni.

Co musisz zrobić, żeby się dostosować?

Reaguj na takie prośby. Dobrym pomysłem byłoby opracowanie i udokumentowanie procesu na takie okazje. Warto też zweryfikować tożsamość tej osoby przed wysyłką kompletu danych. Rozumiesz, nie chcesz odpowiadać za nielegalne udostępnienie danych osobowych. Jaki format jest powszechnie używany i cyfrowy? Najlepiej PDF albo XLS. Ten pierwszy będzie lepiej wyglądał po wydrukowaniu, za to ten drugi jest lepiej przystosowany do odczytu i importu do innych systemów (więcej o tym poniżej).

Co my zrobiliśmy, żeby się dostosować?

Możesz udostępnić swoim uczestnikom formularz kontaktowy do zgłoszenia chęci dostępu do swoich danych. Gdy otrzymasz takie zgłoszenie, możesz łatwo pobrać komplet danych uczestnika w formacie PDF i mu go wysłać.



Prawo do bycia zapomnianym

Zasada wydaje się prosta. Uczestnik chce zostać zapomniany, więc o nim zapominasz. Usuwasz wszystkie dane tego uczestnika i to tyle, prawda? Prawda. Jednak musisz **usunąć wszystkie jego dane**. To oznacza system rejestracji, CRM, listy mailingowe i wszystkie inne miejsca, w których mogą być przechowywane. Papierowe listy obecności - wymazać. Pliki XLS - usunąć wiersz. Pamiętaj jednak o bardzo ważnym aspekcie - **każde przetwarzanie danych osobowych ma podstawę prawną**. Nie usuwaj danych zbyt pochopnie! Może się okazać że masz obowiązek prawny dane te przechowywać przez określony okres!

Co musisz zrobić, żeby się dostosować?

Chyba nie wymaga to dodatkowych wyjaśnień. Najważniejsze to sumienność, dokładność i terminowość. Nie mogę powiedzieć Ci, co konkretnie masz zrobić, bo każda organizacja ma własną sieć i strukturę danych. A jeśli masz zgodę na udostępnianie danych osobowych stronom trzecim i z niej korzystasz, to musisz dopilnować, żeby strony trzecie również przestały je przetwarzać i usunęły.

Co my zrobiliśmy, żeby się dostosować?

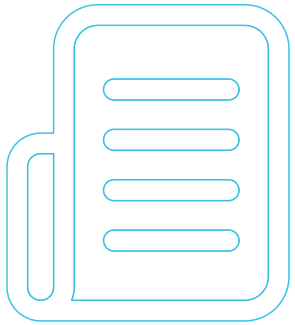
Za pomocą formularza kontaktowego uczestnik może również zażądać usunięcia swoich danych. Jeśli masz prawo dostępu do tych danych, to po zalogowaniu się możesz podjąć decyzję, czy dane należy usunąć, czy pozostawić. No właśnie, masz prawo zachować dane, ale tylko pod warunkiem, że są one niezbędne do wykonania umowy. W tym przypadku możesz zachować dane, jeśli są one niezbędne do wykonania usługi polegającej na uczestnictwie w Twoim wydarzeniu.

Przenoszenie danych

Sprowadza się to do tego, że musisz umożliwić łatwe przeniesienie danych do innych organizacji. Większość systemów przetwarzania danych przyjmuje import danych w postaci plików CSV i XLS, więc są to odpowiednie formaty do eksportowania danych z Twojego systemu.

Co musisz zrobić, żeby się dostosować?

Upewnij się, że możesz na żądanie pobrać komplet danych konkretnej osoby i możesz go łatwo zaimportować do większości systemów zewnętrznych. Jak w każdym przypadku przekazywania danych osobowych, zweryfikuj tożsamość osoby, która taki transfer zleciła.

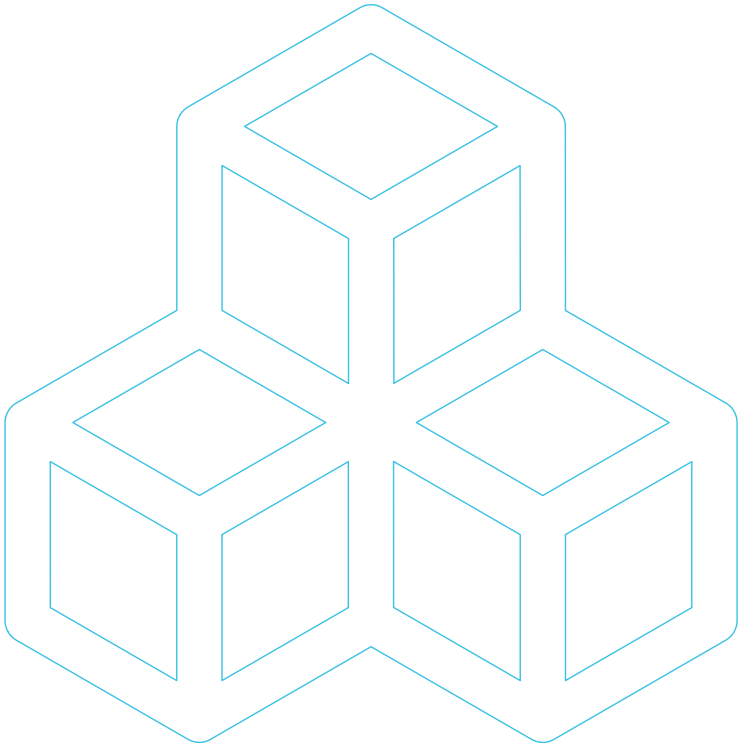


Co my zrobiliśmy, żeby się dostosować?

Możesz łatwo pobrać komplet danych rejestracji na swój dysk z poziomu panelu administracyjnego.

Projekt nastawiony na prywatność

Oznacza to, że ochrona danych nie jest ani funkcją, ani opcją. Powinna być podstawową zasadą każdego systemu i procesu związanego z danymi osobowymi. Mało precyzyjne, prawda? Ale jeśli przyjmiesz ten tok rozumowania, niemal na pewno poprowadzi Cię on do zgodności z RODO. Jest to całkiem rozsądne i jeśli uczynisz ochronę danych częścią misji swojej organizacji, spełnisz co najmniej większość z wymagań.



Co musisz zrobić, żeby się dostosować?

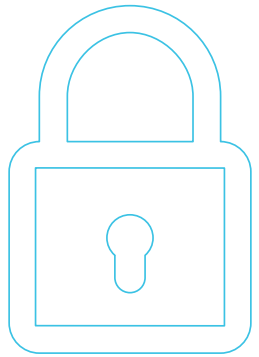
Przeanalizuj wszystkie swoje procesy, narzędzia i cały system, zadając pytania:

- czy to chroni prywatność moich kontaktów?
- czy są tu jakieś miejsca, w których dane osobowe mogłyby wyciec?
- czy stwarza to ryzyko wycieku?
- czy to w porządku, w jaki sposób zbieram i przetwarzam te dane?
- na jakiej podstawie przetwarzam dane osobowe?

Jeśli znajdziesz konflikt z RODO, to zmieniaj i wprowadzaj innowacje! Zgodność się opłaca, nie tylko ze względu na grzywny. Nie, ta treść nie jest sponsorowana przez UE.

Co my zrobiliśmy, żeby się dostosować?

Jeśli utworzysz dodatkowe konta użytkowników, możesz ograniczyć ich dostęp do sekcji zawierających dane osobowe uczestników. Twoja sesja w przeglądarce jest wygaszana po 30 minutach nieaktywności, więc jeśli zostawisz komputer bez nadzoru, jest mniejsza szansa, że ktoś niepowołany uzyska dostęp do informacji. Udostępniamy też naszym klientom subdomeny conrego.com, które są zabezpieczone certyfikatem SSL. Dla zewnętrznych domen możemy zainstalować bezpłatny certyfikat **Let's Encrypt**.



Inspektor Ochrony Danych

IOD pomaga administratorowi lub podmiotowi przetwarzającemu dane we wszystkich kwestiach związanych z ochroną danych osobowych. Oczywiście musimy mieć na względzie iż nie każdy ADO musi powoływać IOD, chyba że zachodzi jedna z poniższych przesłanek:

- organizacje, które przetwarzają dane osobowe na dużą skalę,
- organizacje zajmujące się przetwarzanie danych szczególnej kategorii np. dotyczących zdrowia.

Podczas rejestracji na niektóre konferencje będziesz zbierać takie dane, jak wymagania dietetyczne, alergie, czy też inne dane dot. zdrowie - które to są danymi szczególnej kategorii. "Duża skala" jest określeniem bardzo nieprecyzyjnym. Setki rejestracji to dużo, ale czy jest to duża skala w porównaniu z takimi korporacjami, jak na przykład Google? Nie jest to jasne, ale ja dmuchałbym na zimne i wyznaczył lub zatrudnił IOD.

Co musisz zrobić, żeby się dostosować?

Zatrudnij IOD, który przeszkoli Twoją załogę w zakresie przetwarzania danych osobowych, udokumentuje procesy związane z przetwarzaniem danych i będzie zgłaszał wszelkie niezgodności z RODO do UODO.

Co my zrobiliśmy, żeby się dostosować?

Zatrudniliśmy IOD. Pracownicy, którzy mają dostęp do danych osobowych są okresowo szkoleni. Dodatkowo udokumentowaliśmy procesy związane z przetwarzaniem i wyciekami danych.

Podsumowanie

RODO wchodząc w życie, wprowadziło obowiązek skuteczniejszej ochrony danych osobowych naszych pracowników, klientów czy także kontrahentów.

Mam nadzieję, że ten poradnik okazał się przydatny i trochę Cię uspokoił. Jeśli potraktujesz ochronę danych osobowych jako nieodzowną część swojego biznesu i naprawdę się przyłożysz, nic Ci nie grozi. Na szczęście to rozporządzenie jest całkiem racjonalne. Z drugiej strony, może niepokoić jego ogólność. Wiadomo, zabezpieczenia, które Ty uznasz za wystarczające, mogą okazać się niewystarczające dla władz. Nie lubimy niepewności, dlatego też napisałem ten poradnik ze sporym marginesem bezpieczeństwa. W końcu lepiej być dobrze przygotowanym, niż później uzasadniać swoje działania, gdy zgodność z RODO zostanie zakwestionowana.

Powodzenia!

Twój system rejestracji uczestników
powinien być funkcjonalny, elastyczny i bezpieczny.

Gratulacje! Twoje poszukiwania dobiegły końca.

https://conrego.pl

conrego