Creativa

DOKUMENTY RODO – INSTRUKCJA

Spis treści

1. Wskazówki ogólne

1.1. Przygotowane dokumenty należy zgromadzić i przechowywać w jednym, bezpiecznym miejscu, w formie dokumentowej:
   1.1.1. papierowej (np. specjalnym segregatorze) **lub**
   1.1.2. **elektronicznej** (np. w „chmurze” wykorzystywanej w organizacji Administratora).

2. Polityka ochrony danych osobowych

2.1. **Polityka ochrony danych osobowych** jest „konstytucją” systemu ochrony danych osobowych w organizacji Administratora. Wdrażanie pakietu RODO należy zatem zacząć od jej przeczytania oraz przyswojenia użytych w niej pojęć.
2.2. Pozostałe dokumenty pakietu są „zakorzenione” w Polityce oraz służą do wprowadzenia jej postanowień w życie.
2.3. Z Polityką powinny zapoznać się wszystkie osoby, z którymi Administrator współpracuje w ramach swojej organizacji (niezależnie od podstawy tej współpracy).
2.4. Poza uzupełnieniem danych, nie należy modyfikować postanowień Polityki bez konsultacji ze specjalistą.
2.5. Politykę należy wydrukować a następnie umieścić w Segregatorze RODO. Niezależnie, elektroniczny plik z Polityką może zostać umieszczony w „chmurze” wykorzystywanej w organizacji Administratora, aby była ona łatwo dostępna dla każdego Członka Personelu.
2.6. Polityka jest dokumentem wewnętrznym i nie musi być nigdzie zgłaszana.

3. Regulamin bezpieczeństwa dla Członków Personelu

3.1. **Regulamin bezpieczeństwa dla Członków Personelu** ma na celu zapewnienie bezpieczeństwa danych osobowych w toku bieżącej działalności Administratora.

3.2. Postanowienia Regulaminu mają charakter całkowicie techniczny, zatem można swobodnie dostosowywać je do potrzeb Administratora.
3.3. Z Regulaminem powinny zapoznać się wszystkie osoby, z którymi Administrator współpracuje w ramach swojej organizacji (niezależnie od podstawy tej współpracy).
3.4. Regulamin należy wydrukować a następnie umieścić w Segregatorze RODO. Niezależnie, elektroniczny plik z Regulaminem może zostać umieszczony w „chmurze" wykorzystywanej w organizacji Administratora, aby był on łatwo dostępny dla każdego Członka Personelu.
3.5. Regulamin jest dokumentem wewnętrznym i nie musi być nigdzie zgłaszany.

4. Wykaz środków ochrony danych osobowych

4.1. **Wykaz środków ochrony danych osobowych** jest przede wszystkim podręcznym źródłem informacji o środkach ochrony danych, które w swojej organizacji stosuje Administrator (może okazać się przydatny np. w razie kontroli).
4.2. Po zapoznaniu się z wymienionymi w Wykazie przykładami, należy dostosować go do stanu rzeczywistego (usuwając środki, które nie są stosowane, lub dopisując środki niewymienione jako przykłady). Wykaz powinien być także regularnie aktualizowany.
4.3. Wykaz jest dokumentem wewnętrznym i nie musi być nigdzie zgłaszany.

5. Procedura realizacji uprawnień osób fizycznych, Wykaz uprawnień przysługujących osobom fizycznym na mocy przepisów RODO i Rejestr informacji o wykonywaniu uprawnień przysługujących osobom fizycznym na mocy przepisów RODO

5.1. Zgodnie ze swoją nazwą, **Procedura realizacji uprawnień osób fizycznych** zawiera wskazówki pomocne podczas realizacji praw osób, których dane przetwarza Administrator.
5.2. Poza postanowieniami oznaczonymi jako niemożliwe do zmodyfikowania (z uwagi na przepisy RODO), postanowienia Procedury mają charakter techniczny, w związku z czym można zmodyfikować je tak, aby lepiej pasowały do sposobu funkcjonowania organizacji Administratora.
5.3. Każde otrzymane żądanie dotyczące danych osobowych należy niezwłocznie odnotować w **Rejestrze informacji o wykonywaniu uprawnień przysługujących osobom fizycznym na mocy przepisów RODO** (jego wzór wchodzi w skład pakietu dokumentów) - można prowadzić go w postaci papierowej lub elektronicznej.
5.4. Wchodzący w skład pakietu dokumentów **Wykaz uprawnień przysługujących osobom fizycznym na mocy przepisów RODO** określa przypadki, kiedy dane żądanie należy rozpatrzeć pozytywnie, a kiedy odmówić jego realizacji (jest to zatem swego rodzaju „ściągawka"). Nie należy bowiem automatycznie realizować każdego żądania, którego autor powołuje się na RODO.
5.5. Procedurę należy wydrukować a następnie umieścić w Segregatorze RODO. Niezależnie, elektroniczny plik z Procedurą może zostać umieszczony w „chmurze" wykorzystywanej w organizacji Administratora, aby była ona łatwo dostępna dla każdego Członka Personelu.
5.6. Wszystkie ww. dokumenty mają charakter wewnętrzny i nie muszą być nigdzie zgłaszane.

6. Procedura postępowania w przypadku naruszenia ochrony danych osobowych, Rejestr naruszeń ochrony danych osobowych i Wzór zawiadomienia o naruszeniu ochrony danych osobowych

6.1. **Procedura postępowania w przypadku naruszenia ochrony danych osobowych** określa zasady postępowania w przypadku wystąpienia naruszenia ochrony danych osobowych (np. ich kradzieży).
6.2. Z Procedurą powinny zapoznać się wszystkie osoby, z którymi Administrator współpracuje w ramach swojej organizacji (niezależnie od podstawy tej współpracy).

6.3. Poza postanowieniami oznaczonymi jako niemożliwe do zmodyfikowania (z uwagi na przepisy RODO), postanowienia Procedury mają charakter techniczny, w związku z czym można zmodyfikować je tak, aby lepiej pasowały do sposobu funkcjonowania organizacji Administratora.
6.4. Naruszenia ochrony danych osobowych należy niezwłocznie odnotowywać w specjalnym rejestrze, którego wzór (plik „**Rejestr naruszeń ochrony danych osobowych**") wchodzi w skład pakietu (można prowadzić go w postaci papierowej lub elektronicznej).
6.5. W przypadku, gdy zgodnie z Procedurą konieczne będzie zawiadomienie o naruszeniu osób, których dane dotyczą (np. klientów serwisu), należy wykorzystywać w tym celu **Wzór zawiadomienia o naruszeniu ochrony danych osobowych**. Wzór zawiadomienia ma charakter przykładowy, zatem może być on modyfikowany pod kątem stylistycznym.
6.6. Zawiadomienie o naruszeniu ochrony danych osobowych może zostać wysłane zarówno pocztą elektroniczną, jak i tradycyjną.
6.7. Procedurę należy wydrukować a następnie umieścić w Segregatorze RODO. Niezależnie, elektroniczny plik z Procedurą może zostać umieszczony w „chmurze" wykorzystywanej w organizacji Administratora, aby była ona łatwo dostępna dla każdego Członka Personelu.
6.8. Wszystkie ww. dokumenty mają charakter wewnętrzny i nie muszą być nigdzie zgłaszane.

7. Procedura usuwania i niszczenia danych osobowych

7.1. Zgodnie ze swoją nazwą, **Procedura usuwania i niszczenia danych osobowych** zawiera wskazówki dotyczące usuwania i niszczenia danych przetwarzanych przez Administratora.
7.2. Postanowienia Procedury mają charakter całkowicie techniczny, zatem można swobodnie dostosowywać je do potrzeb Administratora.
7.3. Usuwanie i niszczenie danych osobowych to czynności objęte pojęciem „przetwarzania danych osobowych" w rozumieniu RODO, dlatego powinny być one przeprowadzane wyłącznie w przypadku, gdy istnieje ku temu stosowna podstawa prawna. Nieautoryzowane usunięcie lub zniszczenie danych osobowych może stanowić naruszenie ich ochronny.
7.4. Korzystając z Rejestru czynności przetwarzania, Administrator powinien okresowo usuwać/niszczyć dane osobowe, co do których utracił wszystkie podstawy ich dalszego przetwarzania.
7.5. Procedurę należy wydrukować a następnie umieścić w Segregatorze RODO. Niezależnie, elektroniczny plik z Procedurą może zostać umieszczony w „chmurze" wykorzystywanej w organizacji Administratora, aby była ona łatwo dostępna dla każdego Członka Personelu.
7.6. Procedura jest dokumentem wewnętrznym i nie musi być nigdzie zgłaszana.
7.7. Niezależnie od wskazówek zawartych w instrukcji oraz komentarzach pomocniczych, zachęcamy do zapoznanie się z artykułem „Kiedy i jak usuwać dane osobowe zgodnie z RODO? – poradnik" https://creativa.legal/kiedy-i-jak-usuwac-dane-osobowe-zgodnie-z-rodo-poradnik/.

8. Procedura szkoleń z zakresu ochrony danych osobowych

8.1. Zgodnie ze swoją nazwą, **Procedura szkoleń z zakresu ochrony danych osobowych** zawiera wskazówki dotyczące przeprowadzania szkoleń z zakresu ochrony danych osobowych w organizacji Administratora.
8.2. Postanowienia Procedury mają charakter całkowicie techniczny, zatem można swobodnie dostosowywać je do potrzeb Administratora.
8.3. Przeprowadzane szkolenia powinny mieć na celu nie tylko przekazanie ich uczestnikom praktycznej wiedzy i umiejętności, lecz także ich utrwalenie (np. poprzez przeprowadzanie testów).

8.4. Procedura szkoleń powinna zostać dostosowana do rzeczywistych warunków panujących w organizacji Administratora (w tym liczby osób zatrudnionych).
8.5. Procedurę należy wydrukować a następnie umieścić w Segregatorze RODO. Niezależnie, elektroniczny plik z Procedurą może zostać umieszczony w „chmurze" wykorzystywanej w organizacji Administratora, aby była ona łatwo dostępna dla każdego Członka Personelu.
8.6. Procedura ma charakter wewnętrzny i nie musi być nigdzie zgłaszana.

9. Oświadczenie o zapoznaniu się z zasadami ochrony danych osobowych

9.1. **Oświadczenia o zapoznaniu się z zasadami ochrony danych osobowych** należy odebrać od wszystkich osób, z którymi w ramach swojej organizacji współpracuje Administrator (niezależnie od podstawy tej współpracy). Chodzi tu przede wszystkim o osoby, które:
  9.1.1. posiadają fizyczny lub elektroniczny dostęp do infrastruktury Administratora, której używa on do przetwarzania danych osobowych (co niekoniecznie wiąże się z upoważnieniem do przetwarzania samych danych osobowych);
  9.1.2. znajdują się z Administratorem w relacji przełożony-podwładny (innymi słowy, Administrator jest uprawniony wydawać im polecenia i egzekwować ich wykonanie). Do takich osób można zaliczyć np.:
    9.1.2.1. osobę zatrudnioną w celu bieżącego obsługiwania serwisu,
    9.1.2.2. osobę zatrudnioną w celu prowadzenia obsługi klientów i użytkowników,
    9.1.2.3. osobę zatrudnioną w ramach serwisu sprzątającego,
    9.1.2.4. wolontariusza/stażystę.
9.2. Po uzupełnieniu Oświadczenia o dane wskazane w komentarzach dodanych do pliku, należy wydrukować w jednym egzemplarzu oraz (po podpisaniu przez osobę składającą Oświadczenie) dołączyć do dokumentów (np. akt pracowniczych) dotyczących osoby, która je złożyła. Alternatywnie, osoba składająca Oświadczenie może:
  9.2.1. samodzielnie wydrukować Oświadczenie, podpisać je, zeskanować i następnie przesłać Administratorowi albo
  9.2.2. podpisać plik z Oświadczeniem elektronicznie (np. za pomocą systemu zatwierdzania dokumentów online) i następnie przesłać Administratorowi.

10. Upoważnienie do przetwarzania danych osobowych i Rejestr upoważnień do przetwarzania danych osobowych

10.1. **Upoważnienia do przetwarzania danych osobowych** należy wydać wszystkim osobom, z którymi w ramach swojej organizacji współpracuje Administrator (niezależnie od podstawy tej współpracy). Chodzi tu przede wszystkim o osoby, które:
  10.1.1. posiadają fizyczny lub elektroniczny dostęp do infrastruktury Administratora, której używa on do przetwarzania danych osobowych;
  10.1.2. w ramach swoich obowiązków przetwarzają dane osobowe posiadane przez Administratora;
  10.1.3. znajdują się z Administratorem w relacji przełożony-podwładny (innymi słowy, Administrator jest uprawniony wydawać im polecenia i egzekwować ich wykonanie). Do takich osób można zaliczyć np.:
    10.1.3.1. osobę zatrudnioną w celu bieżącego obsługiwania serwisu,
    10.1.3.2. osobę zatrudnioną w celu prowadzenia obsługi klientów i użytkowników,
    10.1.3.3. osobę zatrudnioną w recepcji/sekretariacie,
    10.1.3.4. wolontariusza/stażystę (jeżeli w ramach swoich obowiązków przetwarza dane osobowe).

10.2. Po uzupełnieniu Upoważnienia o dane wskazane w komentarzach dodanych do pliku, należy wydrukować je w dwóch egzemplarzach, podpisać oraz za pokwitowaniem przekazać jeden egzemplarz upoważnionej osobie. Alternatywnie, Administrator może przesłać Upoważnienie osobie upoważnionej w postaci skanu albo pliku podpisanego elektronicznie (np. za pomocą systemu zatwierdzania dokumentów online), z zastrzeżeniem pkt 10.3.
10.3. W przypadku, gdy Upoważnienie dotyczy przetwarzania danych osobowych wskazanych w art. 9 RODO, czyli tzw. „danych wrażliwych" (np. danych dotyczących zdrowia), musi być ono obowiązkowo wydane w postaci papierowej.
10.4. Wydane Upoważnienia należy na bieżąco ewidencjonować w **Rejestrze upoważnień**, którego wzór wchodzi w skład pakietu dokumentów.
10.5. Upoważnienie powinno zostać zwrócone niezwłocznie po jego odebraniu lub wygaśnięciu.

11. Umowa powierzenia przetwarzania danych osobowych i Rejestr umów powierzenia przetwarzania danych osobowych

11.1. Umowę powierzenia przetwarzania danych należy zawrzeć z kontrahentem w przypadku, gdy dana współpraca wymaga przekazania danych osobowych przetwarzanych przez jedną ze stron drugiej stronie.
11.2. Omawianą umowę zawiera się w przypadku, gdy kontrahent Administratora:
  11.2.1. nie jest jego podwładnym (istnieje faktyczna równorzędność stron umowy) oraz
  11.2.2. świadczy na rzecz Administratora usługi wymagające przetwarzania danych osobowych posiadanych przez Administratora (np. wysyła newsletter do klientów Administratora, prowadzi rekrutację pracowników w imieniu Administratora albo udostępnia dysk, na którym Administrator przechowuje dane osobowe).
11.3. Treść większości postanowień Umowy jest zdeterminowana przez przepisy RODO, dlatego uzupełnić lub zmodyfikować jej wzór należy wyłącznie w miejscach zaznaczonych komentarzami.
11.4. Zawarte Umowy należy na bieżąco ewidencjonować w **Rejestrze umów**, którego wzór wchodzi w skład pakietu dokumentów.
11.5. Umowa powierzenia powinna stanowić załącznik do umowy będącej podstaw współpracy Administratora z kontrahentem (tzw. umowy głównej).
11.6. Niezależnie od wskazówek zawartych w instrukcji oraz komentarzach pomocniczych, zachęcamy do zapoznanie się z artykułem „Umowy powierzenia pod RODO – gdy udostępniasz dane osobowe" https://creativa.legal/umowy-powierzenia-pod-rodo/.

12. Rejestr czynności przetwarzania

12.1. **Rejestr czynności przetwarzania** służy do zebrania w jednym dokumencie (papierowym lub elektronicznym) wszystkich czynności, w ramach których przetwarzane są dane osobowe.
12.2. Wypełnianie Rejestru należy rozpocząć od uzupełnienia arkusza „Informacje", a następnie przejść do arkusza z właściwym Rejestrem.
12.3. W pierwszej kolejności należy wypisać wszystkie podejmowane przez Administratora czynności, w ramach których przetwarzane są dane osobowe, na następnie uzupełnić kolejne kolumny zgodnie ze wskazówkami zawartymi w komentarzach dodanych w pliku.
12.4. Wypisując czynności przetwarzania należy używać nazw o charakterze zbiorczym, obejmujących całokształt podejmowanych w jej ramach operacji na danych. Przykładowo, zbiorcza nazwa „prowadzenie dokumentacji pracowniczej" obejmuje wszystkie czynności jakie w związku z prowadzeniem takiej dokumentacji Administrator podejmuje jako pracodawca. W Rejestrze nie należy zatem wpisywać osobno „przechowywania dokumentacji pracowniczej", „porządkowania dokumentacji pracowniczej" itd., lecz posługiwać się zbiorczą nazwą „prowadzenie dokumentacji pracowniczej". Podobne zbiorcze określenia (nie ma ich

sztywnego katalogu, można je tworzyć dowolnie) należy stosować także w pozostałych przypadkach.

12.5. Przy wypełnianiu Rejestru pomocny może okazać się film instruktażowy znajdujący się pod adresem: https://youtu.be/8v6xeIKkb_A.

12.6. Rejestr jest dokumentem wewnętrznym i nie musi być nigdzie zgłaszany.

13. Rejestr kategorii czynności przetwarzania

13.1. W odróżnieniu od omówionego powyżej Rejestru czynności przetwarzania, **Rejestr kategorii czynności przetwarzania** Administrator ma obowiązek prowadzić tylko wówczas, gdy przetwarza dane osobowe na zlecenie innego podmiotu, który jest administratorem tych danych. Przykładowo, Administrator powinien posiadać omawiany Rejestr, jeżeli prowadzi wysyłkę newslettera na zlecenie podmiotu trzeciego.

13.2. Biorąc pod uwagę praktykę, prowadzenie serwisu internetowego w zakresie Państwa obszaru działalności zazwyczaj nie wiąże się z koniecznością przetwarzania danych osobowych w cudzym imieniu. Oznacza to, że w większości przypadków, prowadzenie tego rejestru nie będzie wymagane.

13.3. Wypełnianie Rejestru należy rozpocząć od uzupełnienia arkusza „Informacje", a następnie przejść do arkusza z właściwym Rejestrem.

13.4. W pierwszej kolejności należy wypisać wszystkie podejmowane czynności realizowane na rzecz podmiotów trzecich, w ramach, których przetwarzane są dane osobowe, a następnie uzupełnić kolejne kolumny zgodnie ze wskazówkami zawartymi w komentarzach dodanych w pliku.

13.5. Podobnie jak w przypadku Rejestru czynności przetwarzania, wypisując czynności realizowane na rzecz podmiotów trzecich należy używać nazw o charakterze zbiorczym (np. „prowadzenie rekrutacji pracowników").

13.6. Przy wypełnianiu Rejestru pomocny może okazać się film instruktażowy znajdujący się pod adresem: https://youtu.be/8v6xeIKkb_A.

13.7. Rejestr jest dokumentem wewnętrznym i nie musi być nigdzie zgłaszany.

14. Analiza ryzyka wiążącego się z przetwarzaniem danych osobowych

14.1. **Analiza ryzyka wiążącego się z przetwarzaniem danych osobowych** to arkusz, za pomocą którego Administrator może ocenić stopień ryzyka wiążącego się z przetwarzaniem danych osobowych w ramach prowadzenia serwisu.

14.2. Przeprowadzając analizę, Administrator powinien sukcesywnie uzupełniać kolejne sekcje arkusza, kierując się wskazówkami zawartymi w komentarzach pomocniczych.

14.3. W przypadku, gdy przeprowadzona analiza wykaże nieakceptowalny poziom ryzyka, Administrator powinien przeprowadzić (najlepiej przy udziale specjalisty) ocenę skutków, o której mowa w art. 35 RODO oraz wdrożyć odpowiednie środki minimalizujące stwierdzone ryzyko.

14.4. Uzupełniony arkusz należy wydrukować i umieścić w Segregatorze RODO.

14.5. W przypadku, gdy którykolwiek z czynników umieszczonych w arkuszu uległ zmianie (np. doszło do znaczącego zwiększenia liczny klientów), Administrator powinien dokonać ponownej analizy ryzyka.

14.6. Analiza jest dokumentem wewnętrznym i nie musi być nigdzie zgłaszana.

15. Klauzule informacyjne RODO

15.1. Dokumenty opatrzone zbiorczą nazwą „Klauzule informacyjne RODO" służą do wykonywania tzw. obowiązku informacyjnego przewidzianego przez RODO (powinny być zatem udostępniane ich adresatom w momencie pobierania ich danych).

15.2. W skład pakietu wchodzą Klauzule przeznaczone do wykorzystania podczas rekrutacji pracowników, zleceniobiorców (prowadzących lub nieprowadzących działalności gospodarczej) oraz wykonawców zatrudnionych na podstawie umowy o dzieło (prowadzących lub nieprowadzących działalności gospodarczej). Ponadto, w pakiecie znajduje się Klauzula przeznaczona do publikacji na firmowym profilu Administratora w serwisie Facebook.

15.3. Przygotowując poszczególne wersje Klauzul należy:

15.3.1. uzupełnić dane Administratora (w tym dane kontaktowe);

15.3.2. zwrócić uwagę, czy pobrane dane osobowe nie będą wykorzystywane w większej liczbie celów niż wymienione we wzorach (jeżeli tak, należy je dopisać);

15.3.3. zwrócić uwagę za zakres pobieranych danych (w finalnej wersji należy pozostawić tylko takie kategorie danych osobowych, które rzeczywiście są pobierane);

15.3.4. zwrócić uwagę, czy pobrane dane nie będą wykorzystywane w celu tworzenie profili (np. profili marketingowych) lub przekazywane do państw trzecich, np. poprzez przetwarzanie ich za pomocą narzędzi (np. dysków internetowych) dostarczanych przez podmioty z takich państw (jeżeli tak, należy odpowiednio to opisać);

15.3.5. wypisać kategorie podmiotów trzecich (odbiorców), które będą miały dostęp do pobieranych danych osobowych (nie trzeba wskazywać ich z nazwy, wystarczy ogólne określenie, np. „biuro księgowe”).

15.4. Klauzula informacyjna RODO może zostać przekazana adresatowi w postaci papierowej lub elektronicznej.