MICHAŁ NOSOWSKI

POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

KOMPLEKSOWY PORADNIK DLA PRZEDSIĘBIORCÓW

WWW.MICHALNOSOWSKI.PL
WWW.WSRODDANYCH.PL

WSTĘP

W dobie Internetu przepływ informacji, w tym danych osobowych, pomiędzy różnymi podmiotami stanowi dla nas normalny element prowadzenia działalności gospodarczej. Często wymiana takich danych spowodowana jest tym, że jeden podmiot świadczy usługi na rzecz drugiego, a te wymagają dostępu do danych osobowych, których administratorem jest usługobiorca – to on bowiem je zgromadził i to jemu są potrzebne do realizacji swoich celów.

Dzieje się tak np. w przypadku korzystania przez firmy z usług biur rachunkowych (które mają dostęp do danych kontrahentów, pracowników, zleceniobiorców), usług serwerowych (które przechowują dane zapisane na serwerze, w tym dane osobowe) usług związanych z obsługą IT (bo działania w ramach systemów informatycznych mogą łączyć się z dostępem do danych) czy też np. ze świadczeniem usług ochrony (bo ochroniarz ma dostęp do listy osób upoważnionych do wejścia na teren jakiegoś zakładu).

Przepisy Rozporządzenia ogólnego o ochronie danych osobowych (RODO) przewidują taką możliwość i regulują tę kwestię, nazywając ją powierzeniem przetwarzania danych osobowych. Nakładają przy tym obowiązki zarówno na przekazującego (administratora) jak i otrzymującego dane (podmiot przetwarzający). Pomimo wielu artykułów i wypowiedzi o RODO, które miały miejsce do tej pory, umowy powierzenia nadal sprawiają przedsiębiorcom sporo problemów, zarówno w związku z tym, czy w ogóle należy je podpisywać, kiedy trzeba to robić, jak również tym co w tych umowach powinno się znaleźć.

Niniejszy poradnik skierowany jest w szczególności do przedsiębiorców, zarówno tych, którzy działają jako administratorzy danych i powierzają je innym podmiotom, jak również tych, którzy działają jako usługodawcy i otrzymują od swoich klientów dane osobowe, a tym samym są zobowiązani do zawierania umów powierzenia przetwarzania danych osobowych. Część z porad zawartych w poradniku ma jednak charakter na tyle ogólny, że mogą być pomocne nie tylko dla przedsiębiorców, ale np. również dla jednostek samorządu terytorialnego czy innych podmiotów publicznych, które przekazują dane poza swoją organizację.

Pisząc ten poradnik chciałem uwzględnić zarówno interesy administratorów jak i podmiotów przetwarzających. Doradzając różnym przedsiębiorstwom w zakresie ochrony danych osobowych często spotykam się z takimi wzorami umów powierzenia, które zabezpieczają interes właściwie tylko jednej strony, nakładając mnóstwo obowiązków na drugą stronę. Dotyczy to z reguły tych umów, które są przygotowywane przez administratorów i przesyłane ich podwykonawcom. Z drugiej strony, zdarzają się także niezbyt zgodne z RODO umowy przygotowane przez podmioty przetwarzające, które oferują ich zawarcie swoim klientom – zdejmują one niekiedy jakąkolwiek odpowiedzialność z podmiotu przetwarzającego, obowiązki ograniczają do minimum, a ich wartość dla administratora jest bliska wartości papieru, na którym zostały napisane – z tym, że zanim ten papier został zadrukowany można było dla tych kartek znaleźć jakieś lepsze zastosowanie.

Dlatego to co przeczytasz poniżej nie uwzględnia wyłącznie interesów administratorów albo podmiotów przetwarzających. Wręcz przeciwnie – starałem się zwrócić uwagę na to co jest ważne zarówno dla tych, którzy dane przekazują, jak również dla tych, którzy otrzymują do nich dostęp i wykonują na nich operacje. Ważna była dla mnie równowaga pomiędzy podmiotami, które powinny występować w obrocie jako równorzędni partnerzy – co w przypadku umów powierzenia przetwarzania danych jest szczególnie istotne. Stąd też w poradniku albo załączonym wzorze nie znajdziesz postanowień rażąco naruszających równowagę pomiędzy stronami albo tworzących stosunek prawny korzystny tylko dla jednej strony.

O MNIE

Nazywam się Michał Nosowski i jestem radcą prawnym. Specjalizuję się w prawie ochrony danych osobowych i prawie nowych technologii.

Doradzam przedsiębiorcom we wdrażaniu regulacji dotyczących ochrony danych, przygotowuję stosowną dokumentację i na bieżąco wspieram w kwestiach związanych z danymi osobowymi. Innymi słowy, pomagam we wdrażaniu RODO.

Prowadzę również szkolenia i uczestniczę w przeprowadzaniu audytów dotyczących ochrony danych osobowych.

Pomagam przedsiębiorcom działającym w branży nowych technologii i startupom w prawnym uregulowaniu ich biznesów.

Prowadzę bloga o prawie nowych technologii, na którym zamieszczam artykuły dotyczące prawnych aspektów prowadzenia działalności w branży IT – www.wsroddanych.pl

Zapraszam Cię do odwiedzenia mojej strony internetowej: www.michalnosowski.pl

Jeśli chcesz się ze mną skontaktować, napisz na: kontakt@mnosowski.pl

Kiedy musimy zawrzeć umowę powierzenia przetwarzania danych?

Umowę powierzenia powinniśmy zawrzeć zawsze wtedy, gdy mamy jakąś relację, łączącą administratora danych z podmiotem przetwarzającym dane w jego imieniu. Co to oznacza?

Z jednej strony musimy mieć administratora, czyli kogoś kto decyduje o celach i sposobach przetwarzania danych osobowych. Innymi słowy – o tym dlaczego zbiera dane osobowe, po co to robi i w jaki sposób je przechowuje i wykorzystuje. Kryterium decydowania jest tutaj kluczowe – innymi słowy, ważne jest to kto wskazuje na to jakie dane mają być przetwarzane, w jaki sposób i po co.

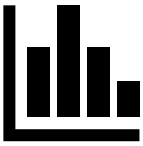
To oznacza, że administrator czasem nie musi nawet mieć tych danych fizycznie „u siebie". Może być tak, że administrator nawet nigdy nie widział tych danych – po prostu zlecił komuś zbudowanie bazy (np. dotyczącej kontaktów marketingowych) a następnie wykonywanie określonych operacji przetwarzania danych (np. wysyłania wiadomości e-mail o charakterze marketingowym).

Natomiast podmiot przetwarzający to ten, który przetwarza dane osobowe w imieniu administratora. Czyli coś dla niego robi, świadczy jakąś usługę i w związku z tym posiada dostęp do danych administratora. Działa tutaj na podstawie jego decyzji, która mówi o tym jakie dane są przetwarzane, w jaki sposób i po co. Podmiot przetwarzający realizuje przy tym interesy administratora – niejednokrotnie po prostu w ramach świadczenia przez siebie różnych usług. Dlatego podmiotem przetwarzającym często jest wykonawca jakiejś usługi dla administratora.

W związku z tym co napisałem na poprzedniej stronie, warto zapoznać się z kilkoma przykładami powierzenia przetwarzania danych:

1) Przedsiębiorstwo korzysta z hostingu poczty elektronicznej zapewnianej przez zewnętrzny podmiot, a dane o kontach użytkowników oraz dane zawarte w treści korespondencji e-mail są przechowywane na serwerze, którym zarządza ten zewnętrzny podmiot. W takim przypadku korzystający z usług firmy hostingowej jest administratorem danych, a firma hostingowa – podmiotem przetwarzającym dane.

2) Przedsiębiorstwo korzystające z usług biura rachunkowego w celu obsługi księgowej i kadrowej – w celu wykonywania przez biuro rachunkowe swoich zadań musi ono mieć dostęp do danych kontrahentów i pracowników przedsiębiorstwa, które jest jego klientem. Dlatego przedsiębiorstwo to, będąc administratorem swoich danych osobowych, powierza je podmiotowi przetwarzającemu, jakim jest biuro rachunkowe, w celu umożliwienia mu realizacji usług zgodnie z zawartą umową.



3) Przedsiębiorstwo korzystające z usług chmurowych, w ramach których przetwarzane są dane osobowe – w takich przypadkach usługodawca, świadczący usługi chmurowe na rzecz swojego klienta jest podmiotem przetwarzającym dane, a klient – ich administratorem.

4) Przedsiębiorstwo zlecające zewnętrznej agencji marketingowej prowadzenie działań marketingowych w jego imieniu. W takiej sytuacji przedsiębiorstwo może przekazać agencji swoją bazę danych osób, do których kierowane będą informacje marketingowe lub zlecić agencji rozpoczęcie budowania takiej bazy w imieniu zlecającego przedsiębiorstwa. W obu tych przypadkach administratorem danych będzie klient agencji, a agencja – podmiotem przetwarzającym dane. Zwróć uwagę na ważną rzecz – w drugim przypadku administrator danych może nie mieć fizycznego dostępu do danych i nie przechowywać ich samodzielnie – a mimo to jest uznany za podmiot, który decyduje o celach i sposobach przetwarzania danych osobowych,

5) Korporacja korzysta z usług podwykonawcy zajmującego się profesjonalnym niszczeniem dużej ilości dokumentów, w tym również takich zawierających dane osobowe. Musimy pamiętać o tym, że niszczenie

lub usuwanie danych również jest czynnością przetwarzania – a tym samym konieczne jest w takim przypadku zawarcie umowy powierzenia danych osobowych.

Kiedy nie musimy zawierać takiej umowy? Gdy nie przekazujemy danych osobowych podmiotom trzecim. Tu sprawa jest prosta. Nie musimy też zawierać takiej umowy w sytuacji gdy podmiot, który przetwarza dane osobowe (które mu przekazujemy) działa także jako administrator. Nie mamy więc do czynienia z relacją administrator – podmiot przetwarzający, ale z występowaniem dwóch odrębnych administratorów danych. Taka relacja pomiędzy dwoma podmiotami ma miejsce m.in.:

1) Gdy pracodawca wysyła pracownika do przychodni medycyny pracy na wstępne lub okresowe badania lekarskie, zgodnie z obowiązkami nałożonymi na niego przez przepisy prawa pracy. W takiej sytuacji pracownik staje się pacjentem takiej placówki, a ona jest administratorem jego danych osobowych. Tym samym nie ma konieczności zawierania z nią umowy powierzenia przetwarzania danych osobowych.

2) Gdy podania danych osobowych żądają od nas uprawnione organy państwowe, zgodnie z przepisami prawa, które przyznają im prawo np. do prowadzenia różnego rodzaju postępowań. Taka sytuacja ma miejsce np. w momencie prowadzenia kontroli przez organy skarbowe, Zakład Ubezpieczeń Społecznych lub prowadzenia postępowań przez sądy, policję, prokuratury czy też komorników sądowych.

Czy przed zawarciem umowy powierzenia administrator powinien coś zrobić?

Administrator powinien spełnić pewne obowiązki wynikające z przepisów RODO już przed zawarciem umowy powierzenia. Jest bowiem zobowiązany do tego aby sprawdzić, czy podmiot przetwarzający spełnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi Rozporządzenia ogólnego i chroniło prawa osób, których dane dotyczą.

Upraszczając: już przed przekazaniem danych przez administratora i zawarciem umowy powierzenia, administrator powinien zweryfikować, czy podmiot przetwarzający stosuje w ogóle jakieś zabezpieczenia dotyczące danych osobowych, na jakim są one poziomie oraz jak dotychczas zachowywał się w kontekście ochrony przetwarzanych przez siebie danych osobowych. Jeżeli więc (co niestety zdarza się dość często) potencjalny podmiot przetwarzający wprost informuje nas o tym, że:

1) nie posiada zabezpieczeń dotyczących przetwarzanych przez siebie danych,
2) zabezpiecza dane, ale odmawia wskazania sposobów ich zabezpieczania,
3) nie zawiera umów powierzenia bo nie uznaje swojej odpowiedzialności w tym zakresie,

lepiej od razu poszukać sobie innego usługodawcy.

We wstępnym określeniu czy dany podmiot przetwarzający spełnia wystarczające wymogi w zakresie stosowania środków bezpieczeństwa pomocne może być poszukiwanie opinii o tym podmiocie w Internecie. Nie oszukujmy się – jeżeli usługodawca ma ciągłe problemy z bezpieczeństwem,

zdarzają mu się wycieki lub przerwy w dostępie do usług albo opieszale reaguje na skargi klientów, nie jest to dobry kandydat na podmiot przetwarzający dane osobowe, za które odpowiada administrator.

Innym sposobem weryfikacji takiego podmiotu przetwarzającego jest zadanie mu szeregu pytań dotyczących przestrzegania zasad dotyczących ochrony danych osobowych (checklisty) lub nawet zrobienie audytu przed zawarciem umowy. Spotykamy się z takimi sytuacjami zwłaszcza w przypadku większych podmiotów, które dysponują odpowiednim zapleczem, umożliwiającym profesjonalne przeprowadzenie takiego audytu.

Jaką formę ma mieć umowa powierzenia?

Umowa powierzenia może zostać zawarta w formie pisemnej, w tym elektronicznej.

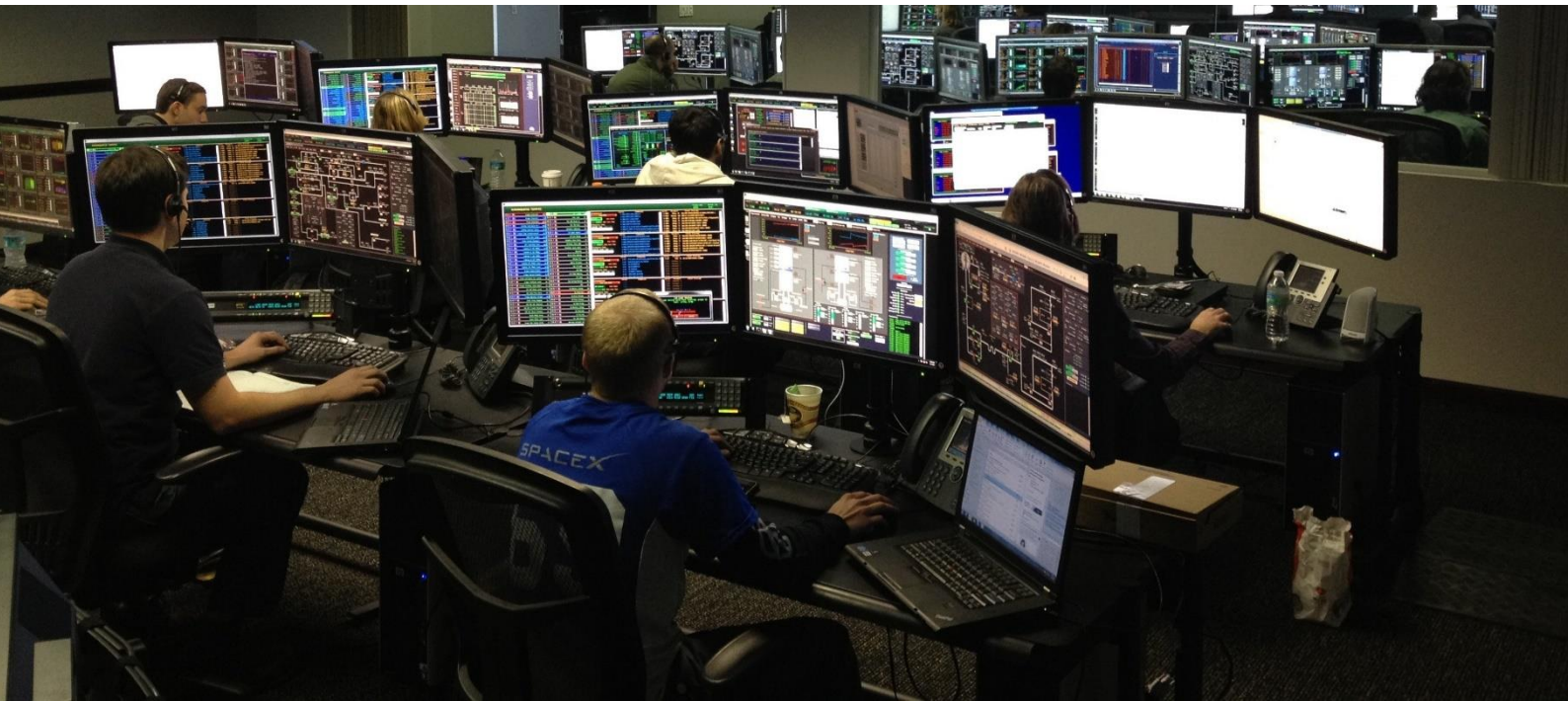
Co to oznacza?

Forma pisemna

Umowę powierzenia możemy podpisać w sposób tradycyjny – przygotowując dwa egzemplarze umowy (bo z reguły będziemy mieli do czynienia z dwiema stronami umowy), które są podpisywane przez osoby uprawnione do reprezentacji obu stron. Następnie każda ze stron otrzymuje swój podpisany egzemplarz.

Forma elektroniczna

Ten zapis w RODO oznacza, że umowa może zostać zawarta także np. poprzez zaakceptowanie odpowiedniego regulaminu (zawierającego zapisy dot. przetwarzania danych osobowych) na stronie internetowej usługodawcy.



Ważne jest abyśmy, jako administrator lub podmiot przetwarzający, byli w stanie wykazać:

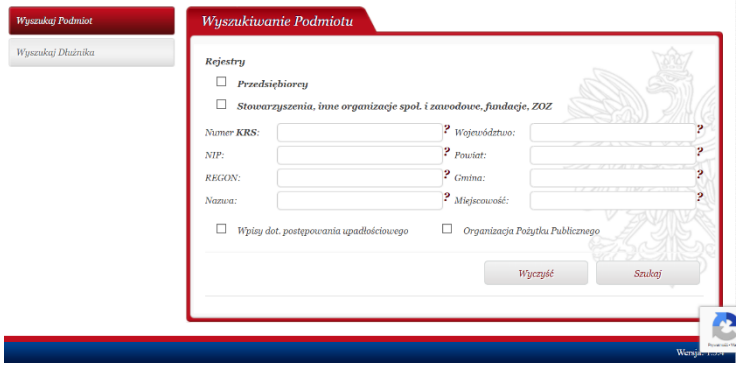
Kto zawarł umowę – czyli musimy mieć dane podmiotów, które ją zawarły oraz dane osób, które reprezentowały strony – takie wskazanie jest istotne również w sytuacji gdy osoba reprezentująca administratora akceptuje umowę powierzenia w Internecie.

Kiedy została zawarta umowa – tak aby móc wykazać, że dane zostały przekazane podmiotowi przetwarzającemu po jej faktycznym zaakceptowaniu przez strony.

Jaka jest treść umowy – w przypadku umów zawartych w formie elektronicznej najlepiej abyśmy przechowywali jej treść na jakimś trwałym nośniku – np. plik pdf. z treścią umowy powierzenia na swoim dysku/swoim serwerze.

Co ważne, większość osób zajmujących się ochroną danych osobowych wskazuje na to, że umowa zawarta w formie elektronicznej nie musi być opatrzona kwalifikowanym podpisem elektronicznym. Ważne jest to, aby nie można było jednostronnie zmienić jej treści i aby wiadome było jakie strony zawarły taką umowę, kiedy została ona zawarta i na co strony się zgodziły.

Pamiętajmy, że umowa powinna być podpisana przez osoby, które mają umocowanie do reprezentacji obu podmiotów – zarówno administratora jak i podmiotu przetwarzającego. Jeżeli stroną jest przedsiębiorca prowadzącym działalność gospodarczą pod własnym nazwiskiem, to właśnie on powinien podpisać umowę. W przypadku gdy stroną umowy jest spółka prawa handlowego, umowa powinna być podpisana zgodnie z zasadami reprezentacji, wskazanymi w KRS (do sprawdzenia tutaj: https://ekrs.ms.gov.pl – przez członka/członków zarządu lub prokurentów, jeżeli tacy są wskazani w KRSie.



Jeżeli umowa ma być podpisana przez jakieś inne osoby, pamiętajmy o tym, że powinny one legitymować się stosownym pełnomocnictwem. Pełnomocnictwo takie powinno być podpisane przez osoby uprawnione do reprezentowania podmiotu, a poszczególne egzemplarze pełnomocnictwa – załączone do umowy.

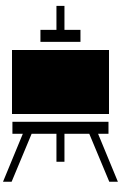
Jestem podmiotem przetwarzającym. Czy powinno mi zależeć na zawarciu umowy powierzenia?

Tak. Wbrew pozorom, umowa powierzenia przetwarzania danych osobowych zabezpiecza nie tylko interesy administratora, ale również podmiotu przetwarzającego. Nieustalenie pomiędzy administratorem i podmiotem przetwarzającym celów i sposobów przetwarzania danych może powodować stwierdzenie, że podmiot przetwarzający sam ustalił te cele i sposoby. Tym samym może on zostać uznany za administratora, który w dodatku przetwarza dane bez odpowiedniej podstawy prawnej. A to niestety może skutkować nałożeniem przez organ nadzorczy kary pieniężnej.

Podstawowe elementy umowy powierzenia przetwarzania danych

Przepisy Rozporządzenia ogólnego o ochronie danych osobowych wskazują na te elementy umowy, które muszą zostać w niej uregulowane. Są to:

Przedmiot i czas trwania przetwarzania – w umowie powierzenia przetwarzania danych osobowych należy uregulować kwestie dotyczące tego jaki jest ogólny cel (np. realizacja umowy głównej) powierzenia przetwarzania danych osobowych, czyli wskazanie na to jaki jest przedmiot zawieranej umowy. W umowie należy także określić czas trwania przetwarzania danych, czyli to jak długo podmiot przetwarzający będzie wykonywał czynności przetwarzania danych. Można ten czas określić wskazując konkretne daty, liczbę miesięcy lub lat, przez który przetwarzane mogą być dane, albo odwołać się do tego, na jak długo została zawarta podstawowa umowa, regulująca relacje między administratorem a podmiotem przetwarzającym. Nie ma przeszkód aby wskazać w umowie powierzenia, że przetwarzanie jest możliwe tak długo jak długo obowiązuje umowa główna.



Charakter i cel przetwarzania – czyli to, w jaki sposób dane mogą być przetwarzane (jakie operacje przetwarzania mogą być wykonywane – np. w umowie można zastrzec, że podmiot przetwarzający ma prawo do odczytywania danych, ale nie do ich modyfikowania), jaka będzie skala przetwarzania danych osobowych, czy dane osobowe będą przetwarzane regularnie czy sporadycznie, oraz po co są one przetwarzane (cel przetwarzania jest rozwinięciem wymienionego powyżej przedmiotu przetwarzania – np. w celu świadczenia usług polegających na prowadzeniu działań marketingowych lub naprawach sprzętu IT, wsparcia biura rachunkowego w obliczaniu zaliczek na podatek dochodowy). Z reguły bowiem przetwarzanie danych przez podmiot przetwarzający jest efektem jakiejś innej umowy, zawartej pomiędzy administratorem a podmiotem przetwarzającym, który pełni rolę usługodawcy.

Rodzaj danych osobowych – w umowie powierzenia konieczne jest sprecyzowanie tego, jakie kategorie danych osobowych będą przetwarzane – np. imiona, nazwiska, nr PESEL, adresy zamieszkania. Chodzi tu tylko o wymienienie tego jakie rodzaje danych będą przetwarzane – oczywiście bez wskazywania danych konkretnych osób. Należy tu także wskazać, czy przetwarzane będą również dane szczególnej kategorii (wraz z ich wymienieniem).

Kategorie osób, których dane dotyczą – kategorie osób, których dane dotyczą, to informacje dotyczące charakterystyki określonej grupy podmiotów danych np. osoby ubezpieczone, klienci sklepów internetowych, użytkownicy określonego serwisu internetowego itd. Jeżeli dojdzie do przetwarzania danych osobowych dzieci – również należy to tutaj wyróżnić.

Obowiązki i prawa administratora – w treści umowy powierzenia przetwarzania danych osobowych należy wskazać również obowiązki i prawa administratora. Mogą one obejmować formę i sposób przekazania danych osobowych, ich aktualizowania czy też obowiązek odpłatności za niektóre czynności przetwarzania danych. Liczne prawa administratora będą przysługiwały natomiast w związku z szeregiem elementów, które musi zawierać umowa powierzenia przetwarzania. Nie ma jednak przeszkód aby strony w umowie wprowadziły także dodatkowe zapisy, niewynikające wprost z przepisów (dotyczące np. konkretnych obowiązków stron w zakresie bezpieczeństwa czy integracji systemów informatycznych.

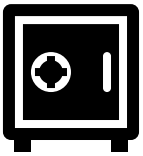
Udokumentowanie polecenia przetwarzania danych

Przepisy RODO wskazują, że podmiot przetwarzający może przetwarzać dane osobowe wyłącznie na udokumentowane polecenie administratora. Oznacza to, że administrator powinien wydać podmiotowi przetwarzającemu polecenie przetwarzania danych – określające przynajmniej cel w jakim dane mają być przetwarzane. Nie ma problemu aby takie polecenie przetwarzania znalazło się bezpośrednio w treści umowy powierzenia. Kwestia ta może jednak zostać uregulowana odmiennie – tzn. w umowie można zastrzec, że każdorazowo administrator powinien wydać odrębne polecenie przetwarzania danych (np. w formie wiadomości elektronicznej wysłanej na określony w umowie adres elektroniczny). Takie rozwiązanie, z uwagi na generowane później problemy praktyczne i utrudnienia w codziennym przetwarzaniu danych osobowych, spotykane jest rzadziej.

Upoważnienia i obowiązek zachowania tajemnicy

W treści umowy powierzenia powinien znaleźć się zapis wskazujący na to, że każdy z pracowników podmiotu przetwarzającego, który bierze udział w wykonywaniu czynności przetwarzania danych powierzonych przez administratora, powinien być:

Upoważniony do przetwarzania danych osobowych, przy czym upoważnienie powinno spełniać pewne minimalne wymogi – wskazywać cel przetwarzania, zbiory danych, do których dostęp ma dana osoba oraz to jakie czynności na danych mogą być przez nią wykonywane. Upoważnienie powinno zostać udzielone na piśmie lub w formie elektronicznej. Kwestie te również można zastrzec w umowie.



Zobowiązany do zachowania danych w tajemnicy – w praktyce w umowach z reguły wskazuje się, że obowiązek zachowania tajemnicy dotyczy nie tylko samych powierzonych danych osobowych, ale także informacji dotyczących np. sposobów zabezpieczania danych osobowych.

Kwestie związane z dalszym powierzeniem przetwarzania danych osobowych

W umowie powierzenia przetwarzania danych osobowych należy uregulować kwestie związane z dalszym przekazywaniem danych osobowych przez podmiot przetwarzający. O jakie sytuacje chodzi? O takie gdy podmiot przetwarzający sam korzysta z usług jakichś innych podmiotów przetwarzających.

> **!** W UMOWIE POWIERZENIA PRZETWARZANIA DANYCH MUSZĄ ZNALEŹĆ SIĘ UREGULOWANIA DOTYCZĄCE PRZEKAZYWANIA DANYCH OSOBOWYCH PODWYKONAWCOM PODMIOTU PRZETWARZAJĄCEGO

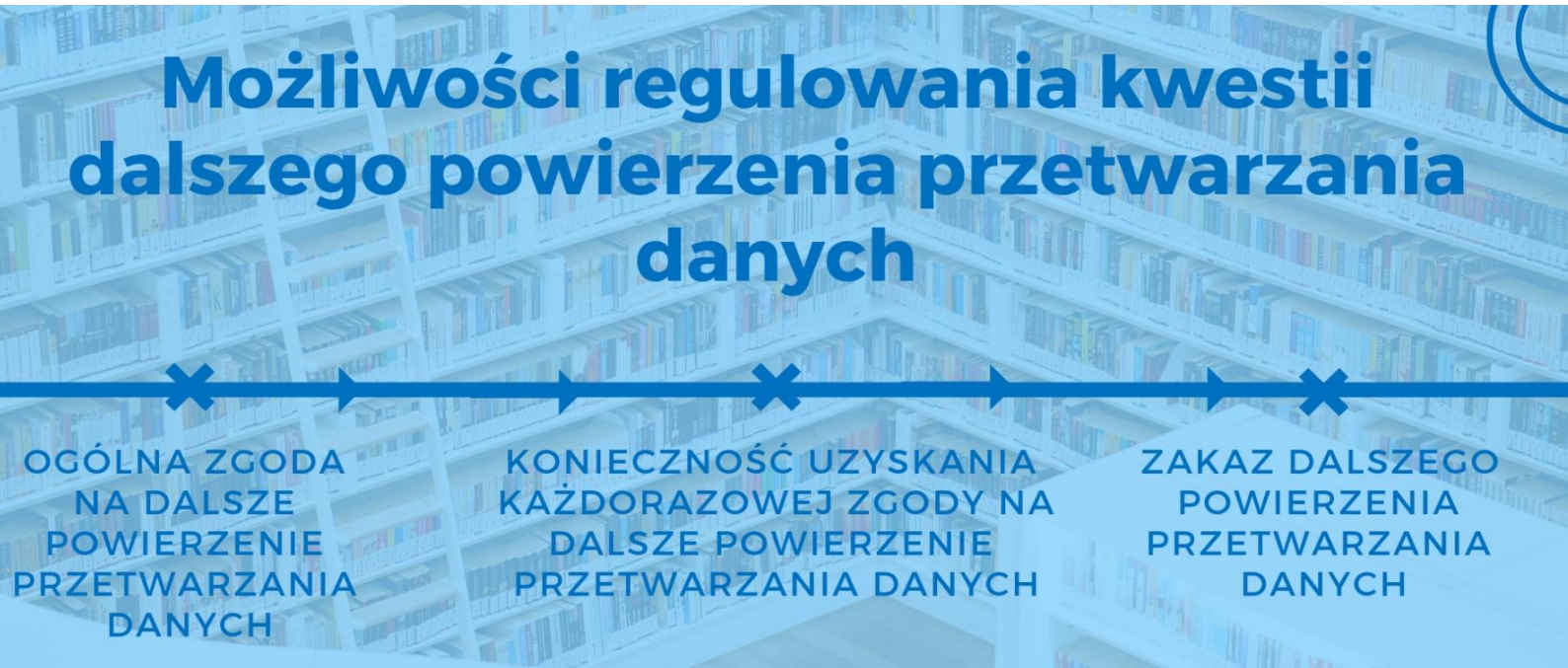
Przykładowo, biuro rachunkowe, które przetwarza dane osobowe pracowników i kontrahentów swojego klienta (czyli jest wobec niego podmiotem przetwarzającym) samo może korzystać np. z zewnętrznych usług serwerowych. Dane, które przekazuje im ich klient, są przekazywane także do firmy utrzymującej serwer – dlatego mamy do czynienia z powierzeniem tych danych, które są już wcześniej powierzone. Klient (administrator) powierza je na rzecz biura rachunkowego, a to powierza je dalej firmie informatycznej. Dalszy podmiot przetwarzający nazywany jest również subprocesorem. Kwestia dalszego powierzania przetwarzania danych osobowych powinna zostać uregulowana w umowie powierzenia.

Zgoda na dalsze powierzenie przetwarzania danych osobowych może zostać wyrażona na dwa sposoby.

Pierwszym z nich jest wyrażenie przez administratora ogólnej zgody na dalsze powierzanie danych osobowych przez podmiot przetwarzający. W takiej sytuacji w umowie należy również zobowiązać (zgodnie z wymogami RODO) do tego aby w przypadku dodania lub zmiany jakiegokolwiek subprocesora przez podmiot przetwarzający, podmiot przetwarzający:

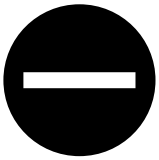
1) poinformował administratora o zmianie lub dodaniu subprocesora, w takim przypadku administrator ma prawo do złożenia sprzeciwu wobec danej osoby,
2) uzyskał wcześniejszą zgodę administratora na dodanie lub zmianę subprocesora.

Warto również w umowie określić jakie konsekwencje będą miały miejsce w sytuacji gdy administrator złoży sprzeciw, o którym mowa w pkt 1 – np. możliwość wypowiedzenia umowy przez podmiot przetwarzający. W praktyce bowiem często zdarza się, że wobec wyrażenia przez administratora sprzeciwu podmiot przetwarzający ma ograniczone możliwości dalszego świadczenia usług na rzecz administratora. Przykładowo, zamiast korzystać z outsourcingu (który jest powszechnie wykorzystywany przez przedsiębiorców) musi wykonywać pewne czynności samodzielnie – co może mieć negatywny wpływ na całość działalności biznesowej podmiotu przetwarzającego. Nie ma również przeciwwskazań aby określić termin (np. 14 dni) na złożenie przez administratora sprzeciwu.

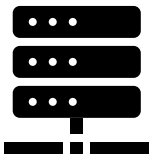


Drugim sposobem na rozwiązanie kwestii korzystania z subprocesorów przez podmiot przetwarzający jest konieczność uzyskania każdorazowej zgody administratora na każdego z subprocesorów.

Co ważne, jeżeli podmiot przetwarzający korzysta z subprocesorów już w momencie zawarcia umowy powierzenia, uzyskanie takiej zgody administratora musi nastąpić przed faktycznym rozpoczęciem przetwarzania danych przez podmiot przetwarzający i subprocesora.

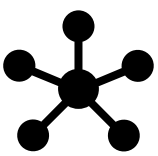


W umowie można również zastrzec, że administrator w ogóle nie zgadza się w ogóle na dalsze powierzenie przetwarzania danych osobowych (korzystanie z subprocesorów). Mając jednak na uwadze współczesne realia gospodarcze i częste korzystanie z różnego rodzaju usług zewnętrznych, rozwiązanie to może być stosowane jedynie w szczególnych wypadkach. Dopuszczalny jest również zapis, że podmiot przetwarzający może korzystać z dalszych podmiotów przetwarzających jedynie w ograniczonym zakresie (np. spośród jednego z wskazanych przez administratora podmiotów przetwarzających, albo tylko w zakresie niektórych czynności przetwarzania).



Zgoda musi być wyrażona przed takim dalszym powierzeniem. Umowa może regulować warunki uzyskania zgody – np. to jakie informacje o dalszym podmiocie przetwarzającym powinny zostać przekazane administratorowi, tak aby mógł ocenić, czy możliwe jest wyrażenie zgody. Taka zgoda powinna zostać wyrażona w formie pisemnej (w tym także – co wynika jednak z interpretacji przepisów – w formie elektronicznej).

W treści umowy powierzenia należy ponadto zawrzeć inne elementy mające wpływ na stosunki pomiędzy administratorem, podmiotem przetwarzającym a dalszym podmiotem przetwarzającym. Powinny obejmować one m.in.:



1) uregulowania dotyczące korzystania z odpowiednich zabezpieczeń danych przez subprocesora (np. podmiot przetwarzający zobowiązuje się do tego aby w umowie z subprocesorem został nałożony obowiązek stosowania przez subprocesora odpowiednich technicznych i organizacyjnych środków bezpieczeństwa danych. Możliwe jest również narzucenie bardziej szczegółowych uregulowań w tym zakresie, np. konkretnych standardów, które powinny być

stosowane przez dalszy podmiot przetwarzający. Umowa zawarta pomiędzy podmiotem przetwarzającym a subprocesorem powinna zapewniać poziom bezpieczeństwa danych nie niższy niż wynikający z postanowień umowy pomiędzy administratorem a podmiotem przetwarzającym.

2) odpowiedzialność podmiotu przetwarzającego za ewentualne niezgodne z prawem przetwarzanie danych osobowych przez subprocesora (np. podmiot przetwarzający odpowiada względem administratora za wszelkie działania subprocesora jak za własne).

Odpowiedzialność odszkodowawcza

W umowie powierzenia przetwarzania danych powinny znaleźć się postanowienia dotyczące ewentualnej odpowiedzialności odszkodowawczej, jaką ponosił będzie podmiot przetwarzający względem administratora w przypadku gdy działania tego pierwszego skutkowałyby wyrządzeniem szkody administratorowi (np. poniesieniem przez administratora strat finansowych lub konieczności zapłaty kar umownych). Wprawdzie po części taka odpowiedzialność wynika bezpośrednio z przepisów Kodeksu cywilnego, ale jej uregulowanie w umowie trzeba uznać za dobrą praktykę – a tym samym warto to robić.

Odpowiedzialność można uregulować dość zwięźle, po prostu wskazując, że podmiot przetwarzający odpowiada względem administratora za wszelkie szkody, które poniósł administrator w związku z działaniami lub zaniechaniami podmiotu przetwarzającego. Nie ma jednak przeszkód aby wskazać w umowie na konkretne elementy odpowiedzialności, jak również ograniczyć ją w jakimś stopniu.

Warto również zaznaczyć w umowie, że podmiot przetwarzający może odpowiadać odszkodowawczo w sytuacji gdyby ewentualna szkoda powstała w związku z działaniem dalszych podmiotów przetwarzających lub niewdrożeniem przez podmiot przetwarzający odpowiednich technicznych i organizacyjnych środków zabezpieczeń danych.

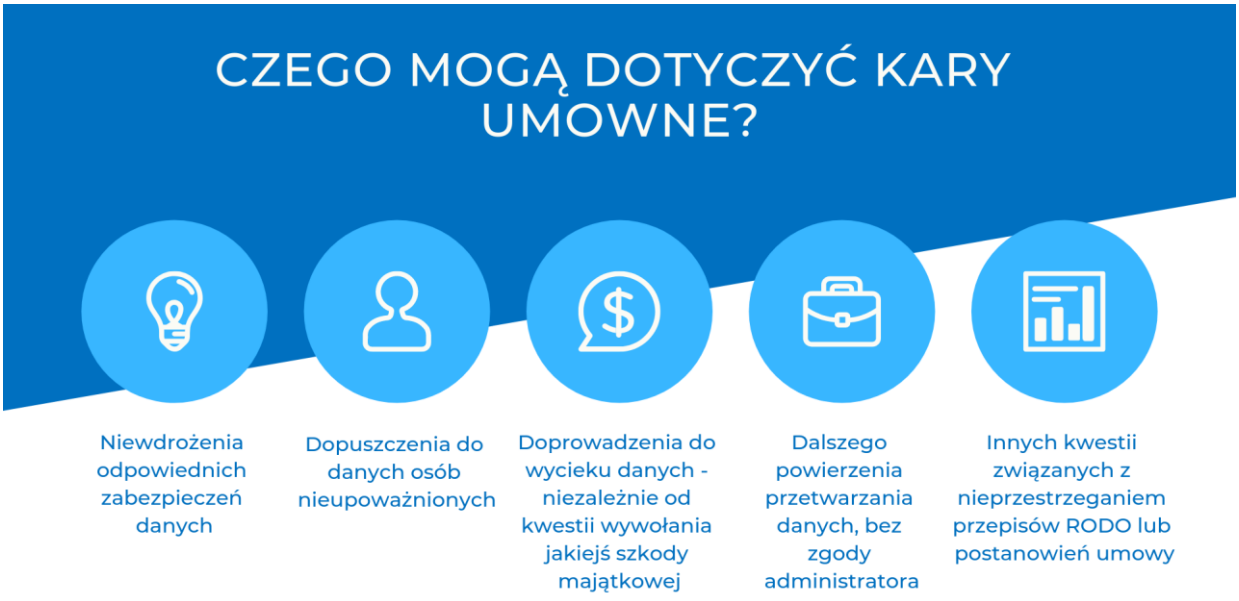
MOŻLIWE JEST OGRANICZENIE ODPOWIEDZIALNOŚCI PODMIOTU PRZETWARZAJĄCEGO ZA SZKODY SPOWODOWANE NIEPRAWIDŁOWYM PRZETWARZANIEM DANYCH

Niekiedy podmioty przetwarzające chcą ograniczenia swojej odpowiedzialności. Może ono mieć formę ograniczenia kwotowego (np. do dwukrotności rocznego wynagrodzenia, które administrator zapłaci podmiotowi przetwarzającemu w związku z korzystaniem z jego usług) lub ograniczenia dotyczącego zakresu (np. że administrator uznaje środki bezpieczeństwa wdrożone przez podmiot przetwarzający za wystarczające i w tym zakresie podmiot przetwarzający nie odpowiada wobec administratora; albo że podmiot przetwarzający odpowiada wyłącznie za te szkody, które są następstwem jego umyślnego działania – a nie takie, które są wynikiem przypadku lub działań nieumyślnych) i formy dochodzenia (tutaj w umowie można wskazać, że administrator, wobec którego np. toczy się postępowanie sądowe lub administracyjne dotyczącego niezgodnego z prawem przetwarzania danych osobowych, w którym brał udział podmiot przetwarzający, jest obowiązany zawiadomić o tym postepowaniu podmiot przetwarzający, tak aby ten drugi mógł ustosunkować się do ewentualnych twierdzeń).

Kary umowne

Niezależnie od odpowiedzialności odszkodowawczej, strony mogą zastrzec w umowie, że za niektóre działania podmiot przetwarzający będzie zobowiązany do zapłaty kar umownych na rzecz administratora (albo na odwrót, co jednak w przypadku umów powierzenia rzadko się zdarza). W takim wypadku samo zaistnienie danego zdarzenia automatycznie nakłada na podmiot przetwarzający obowiązek zapłaty na rzecz administratora kary umownej. Nie ma przy tym konieczności wykazywania jakiejkolwiek szkody (uszczerbku majątkowego poniesionego przez administratora, czyli np. konieczności zapłaty kary pieniężnej nałożonej przez PUODO), wystarczy samo zdarzenie.

Kary umowne najczęściej są wskazywane kwotowo, nie ma jednak przeszkód aby oprzeć je np.% od wartości wynagrodzenia a nawet czynnikach zewnętrznych (np. średnim wynagrodzeniu albo cenie jakiegoś surowca – to jednak rzadziej spotykane przypadki).



Warto w umowie zastrzec, że obowiązek zapłaty kar umownych nie wyłącza możliwości żądania przez administratora odszkodowania na zasadach ogólnych – dzięki temu, gdyby strata finansowa administratora wynikająca z nieprawidłowego działania podmiotu przetwarzającego przekroczyła wysokość kary umownej, będzie mógł on dochodzić odszkodowania zgodnie z tym co zostało napisane wyżej.

Przekazywanie danych do państwa trzeciego

W przypadku gdy dane osobowe będą przekazywane poza teren Unii Europejskiej, kwestia ta powinna zostać uregulowana w umowie. Dzieje się tak szczególnie w sytuacji gdy podmiot przetwarzający korzysta z usług IT innych dostawców spoza Europy – np. usług chmurowych z USA. Czasem zdarza się również, że podmiot przetwarzający jest częścią jakiegoś międzynarodowego koncernu i w związku z tym dane mogą również trafić gdzieś poza UE.

I w takiej sytuacji uregulowania dotyczące przekazania danych poza UE powinny znaleźć się w umowie powierzenia. Przede wszystkim muszą obejmować zgodę administratora na takie przekazanie danych do państwa trzeciego, wskazanie komu dane zostaną przekazane oraz w jakim celu, jak również wskazanie podstawy do przekazania danych do państwa trzeciego, wynikającej z RODO – najlepiej aby to była:

- decyzja komisji w przedmiocie uznania odpowiedniego stopnia ochrony w państwie trzecim,
- oparcie przekazania na standardowych klauzulach umownych, przyjętych przez Komisję
- oparcie przekazania na zatwierdzonych przez organ nadzorczy wiążących regułach korporacyjnych.

Z uwagi na to, że dane są najczęściej przekazywane różnym podmiotom działającym w branży IT w USA, na szczególną uwagę zasługuje program Tarcza Prywatności (*Privacy shield*). Jest to umowa pomiędzy Komisją Europejską a Rządem USA, na mocy której firmy w USA mogą dobrowolnie przystąpić do specjalnego programu (czyli właśnie do Tarczy prywatności) i zobowiązać się do przestrzegania określonych reguł dot. ochrony danych osobowych, obowiązujących w Unii Europejskiej. Lista tych podmiotów znajduje się tutaj: https://www.privacyshield.gov/list. Jeżeli więc podmiot przetwarzający planuje przekazanie danych do organizacji w USA, powinien zweryfikować, czy ta organizacja przystąpiła do programu Tarcza prywatności. Jeśli tak – mamy wskazówkę, że przekazanie danych nie naruszy unijnych przepisów dot. ochrony danych osobowych.

Bezpieczeństwo

W większości umów powierzenia znajdują się standardowe postanowienia dotyczące stosowania przed podmiot przetwarzający zabezpieczeń dotyczących danych, które są powierzone przez administratora. Oparte są one na treści przepisu art. 32 RODO. Stąd też w umowach powierzenia znajdują się zapisy, wskazujące na to, że podmiot przetwarzający zobowiązuje się do wdrożenia odpowiednich środków technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, przy uwzględnieniu stanu wiedzy technicznej, kosztu wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania.

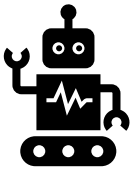
Ale można to uregulowanie rozszerzyć, np. nakładając na podmiot przetwarzający obowiązek sporządzenia oceny ryzyka według określonych kryteriów lub standardów (a nawet udostępnić własną metodologię) lub konieczność wdrożenia konkretnych zabezpieczeń, takich jak np. szyfrowanie, określenia zasad uwierzytelniania dostępu czy też stosowania określonych programów lub urządzeń zabezpieczających.

Pamiętajmy, aby dobrać ewentualne zabezpieczenia do tego jakie dane będą przetwarzane oraz tego w jaki sposób będą one przetwarzane. Powinien to wiedzieć nie tylko podmiot przetwarzający, ale również administrator. On więc także musi (zanim jeszcze powierzy dane) ocenić ryzyko związane z ich przetwarzaniem oraz przekazywaniem podmiotowi przetwarzającemu. To administrator odpowiada za dane osobowe, w stosunku do których ustala cele i sposoby przetwarzania danych. On też

powinien w odniesieniu do konkretnych sposobów przetwarzania, przeprowadzić analizę ryzyka. Jeżeli dane mają być przekazane podmiotowi przetwarzającemu, to analiza ryzyka powinna tę kwestię uwzględniać.

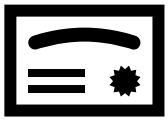
PODSTAWĄ WDROŻENIA ODPOWIEDNICH ZABEZPIECZEŃ DANYCH POWINNA BYĆ PRZEPROWADZONA ANALIZA RYZYKA

Dopiero na podstawie przeprowadzonej oceny ryzyka, zarówno administrator, jak i podmiot przetwarzający, mogą stwierdzić jakie ryzyka związane są z przetwarzaniem danych osobowych oraz w jaki sposób je zabezpieczyć. Środki zabezpieczające powinny bowiem odpowiadać poszczególnym ryzykom. Dlatego bezrefleksyjne wpisywanie wszystkich zabezpieczeń jakie nam przyjdą do głowy nie jest zbyt dobrym pomysłem. Dotyczy to zwłaszcza szyfrowania, które z jednej strony jest bardzo



skutecznym narzędziem zabezpieczania danych, a z drugiej – może utrudnić do nich bieżący dostęp. Nie jest również skuteczne we wszystkich przypadkach. Spotkałem się z takimi umowami powierzenia, które nakładały na podmiot przetwarzający obowiązek szyfrowania dokumentów papierowych – tego typu zapisy nie są zbyt fortunne. Należy pamiętać, że finalne wdrożenie przez podmiot przetwarzający odpowiednich zabezpieczeń leży właśnie po jego stronie. Administrator ma prawa wymagać bezpieczeństwa, a nawet wskazywać metody jego uzyskania, ale musimy pamiętać, że to finalnie podmiot przetwarzający będzie stosował te zabezpieczenia. Dlatego praktyka „narzucania" przez administratorów pewnych zabezpieczeń nie zawsze się sprawdza.

Dobrą praktyką w zakresie bezpieczeństwa będzie zapewne odwoływanie się do (stosowanych przez podmiot przetwarzający) zatwierdzonych kodeksów postępowania, które będą tworzone na podstawie RODO i akceptowane przez Prezesa Urzędu Ochrony Danych osobowych. Możliwe będzie również powoływanie się na certyfikaty dotyczące zgodności z zasadami ochrony danych osobowych, które będą nadawane na podstawie RODO. Jest to jednak kwestia przyszłości – na dzień tworzenia niniejszego poradnika żaden certyfikat nie został jeszcze nadany, a pierwsze kodeksy postępowania są dopiero na etapie zatwierdzania i nie mamy decyzji w tym zakresie.



Prawa osób z rozdziału III RODO

RODO wskazuje, że w umowie powierzenia przetwarzania danych osobowych powinna zostać uregulowana kwestia wsparcia administratora (przez podmiot przetwarzający) w odpowiadaniu na żądania osób, których dane dotyczą – dotyczących np. dostępu do danych, ich usunięcia czy też ograniczenia przetwarzania. Obowiązek pomocy w tym zakresie nie jest absolutny – przepisy RODO wskazują, że powinien uwzględniać charakter przetwarzania i możliwości podmiotu przetwarzającego, a pomoc powinna opierać się o wdrożone środki techniczne i organizacyjne.

W wielu umowach powierzenia podmioty przetwarzające po prostu ogólnie zobowiązują się do tego, aby pomagać administratorowi, w miarę możliwości, mając na uwadze charakter przetwarzania danych, w odpowiadaniu na żądania osób wynikające z rozdziału III RODO. I to jest wystarczające. Niekiedy jednak uregulowania są bardziej szczegółowe i obejmują np.:

- czas w jakim podmiot przetwarzający powinien udzielić odpowiedzi,
- szczegółowy zakres informacji, które podmiot przetwarzający przekazuje administratorowi (np. wykaz poszczególnych czynności, które były przeprowadzane na danych dotyczących konkretnej osoby),
- obowiązek umożliwienia przez podmiot przetwarzający dostępu administratorowi danych do systemu informatycznego podmiotu przetwarzającego tak aby samodzielnie mógł on weryfikować jakie dane są przetwarzane lub je usuwać w razie konieczności.

Wywiązanie się z obowiązków art. 32-36 RODO

Podobnie jak w przypadku żądań osób, których dane dotyczą, RODO nakłada obowiązek zawarcia w umowie powierzenia uregulowań dotyczących spełniania przez administratora następujących obowiązków:

- wdrożenia przez administratora odpowiednich technicznych i organizacyjnych środków zabezpieczających dane,
- zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu,
- informowania o naruszeniach ochrony danych osób, których dane dotyczą,
- dokonywania oceny skutków dla ochrony danych osobowych,
- dokonywania uprzednich konsultacji z organem nadzorczym w zakresie przetwarzania danych związanego z wysokim ryzykiem.

Oczywiście w teorii podmiot przetwarzający powinien wspierać administratora w realizacji każdego z tych obowiązków – i taki zapis powinien znaleźć się w umowie. W praktyce jednak najbardziej szczegółowe uregulowana dotyczą z reguły kwestii informowania administratora przez podmiot przetwarzający o naruszeniach ochrony danych, do których doszło w związku z przetwarzaniem przez podmiot przetwarzający tych powierzonych danych. Wskazuje się więc na termin

poinformowania administratora o wykryciu naruszenia, określając go z reguły na od 12 do 36 godzin. Dlaczego tak mało? Bo administrator ma 72 godziny na zawiadomienie organu nadzorczego o naruszeniu ochrony danych – od momentu dowiedzenia się o naruszeniu. A przyjmuje się, że czas ten biegnie również w przypadku gdy to podmiot działający w imieniu administratora uzyskał taką informację (czyli podmiot przetwarzający). Innymi słowy, w ciągu tych 72 godzin podmiot przetwarzający musi poinformować administratora, a ten następnie powinien poinformować PUODO.

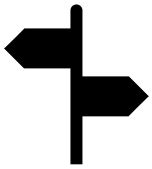
PAMIĘTAJMY O WSKAZANIU W UMOWIE TERMINU, W KTÓRYM PODMIOT PRZETWARZAJĄCY POWINIEN POWIADOMIĆ ADMINISTRATORA O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Pomoc w spełnianiu obowiązków wskazanych w art. 32-36 nie jest również nieograniczona i powinna

uwzględniać charakter przetwarzania oraz dostępne podmiotowi przetwarzającemu informacje. Należy pamiętać, że w inny sposób pomoże administratorowi taki podmiot przetwarzający, który będzie świadczył usługi

serwerowe (bo jego realna wiedza o tym jakie dane są zapisane na serwerze może być ograniczona albo wręcz nie ma do nich dostępu, bo są zaszyfrowane albo inaczej zabezpieczone), a inaczej podmiot, który przechowuje na rzecz administratora np. całość dokumentacji księgowej i kadrowej, świadcząc usługi jako biuro rachunkowe (bo jego wpływ na przetwarzanie danych będzie o wiele większy, również w zakresie np. wyboru zabezpieczeń danych).

Audyty i inspekcje



Kolejnym elementem, który musi być uregulowany w umowie powierzenia przetwarzania danych jest kwestia związana z możliwością sprawdzania przez administratora tego, czy podmiot przetwarzający spełnia obowiązki nałożone na niego przez przepisy RODO i zapisy zawartej umowy powierzenia.

Obejmuje ona w szczególności:

- możliwość żądania przez administratora informacji o tym jak podmiot przetwarzający spełnia obowiązki wynikające z umowy i przepisów RODO,
- możliwość dokonywania przez administratora audytów w tym zakresie.

W ramach tych obowiązków administratorzy zastrzegają sobie z reguły możliwość żądania określonych informacji (np. dotyczących sposobów zabezpieczania danych, o ilości osób, które mają dostęp do danych), dokumentów (kopii polityki bezpieczeństwa, analizy ryzyka, wzorów upoważnień

czy oświadczeń o zachowaniu poufności) oraz przeprowadzenia audytów (kontroli np. stosowanych zabezpieczeń) w miejscu przetwarzania danych przez podmiot przetwarzający.

Niekiedy kwestie te są bardziej szczegółowo uregulowane i wskazują np. na termin, w jakim podmiot przetwarzający powinien udzielić odpowiedzi administratorowi (od momentu otrzymania żądania), sposoby komunikacji pomiędzy administratorem a podmiotem przetwarzającym albo np. zobowiązanie się administratora do zachowania w tajemnicy wszelkich informacji, które uzyskał w toku audytu – z uwagi na to, że stanowią tajemnicę przedsiębiorstwa podmiotu przetwarzającego.

Obowiązek usunięcia danych po zakończeniu przetwarzania

W treści umowy powierzenia przetwarzania powinno znaleźć się zastrzeżenie, że podmiot przetwarzający, po zakończeniu przetwarzania (tzn. sytuacji gdy umowa przestanie wiązać strony) powinien usunąć lub zwrócić dane administratorowi – przy czym decyzja w tym zakresie należy do administratora.

Oczywiście może być tak, że niekiedy dane osobowe będą mogły być tylko usunięte albo tylko zwrócone. W innym przypadku może dojść do sytuacji, że podmiot przetwarzający będzie zobowiązany do tego aby zwrócić kopię wszystkich powierzonych mu danych (np. na trwałym nośniku), a następnie usunąć te dane z pozostałych nośników, które znajdują się w jego posiadaniu. Niekiedy w umowach wskazuje się termin, w którym podmiot przetwarzający powinien dokonać usunięcia lub zwrotu oraz obowiązek potwierdzenia usunięcia danych sporządzeniem pisemnego protokołu.

Inne postanowienia

W umowie powierzenia przetwarzania mogą zostać zawarte także inne postanowienia dotyczące zasad współpracy pomiędzy administratorem a podmiotem przetwarzającym – niekoniecznie wskazane w RODO. Należy pamiętać, że pomimo swojego specyficznego charakteru, są to umowy cywilnoprawne, a więc mogą zawierać elementy znane z innych umów występujących w obrocie, takich jak:

- wskazanie sposobu rozwiązywania sporów (mediacje, arbitraż) lub sądu właściwego, który będzie rozstrzygał spory (sąd właściwy dla siedziby powoda, pozwanego, administratora, podmiotu przetwarzającego),
- wskazanie osób do kontaktu z obu stron umowy, które są odpowiedzialne za jej wykonanie oraz sposobów, w jaki mają się ze sobą kontaktować,
- wskazanie jakie przepisy będą miały zastosowanie w zakresie nieuregulowanym w umowie (RODO, Kodeks cywilny),
- wskazanie, w ilu egzemplarzach została sporządzona umowa i dla kogo.

SKONTAKTUJ SIĘ ZE MNĄ

Zapraszam Cię do napisania wiadomości na adres kontakt@mnosowski.pl

www.wsroddanych.pl

www.michalnosowski.pl

Michał Nosowski Kancelaria Radcy Prawnego
ul. Freytaga 12/3
87-100 Toruń