Co to jest RODO

INFORMATOR O ZMIANACH W PRZEPISACH DOTYCZĄCYCH DANYCH OSOBOWYCH

RODO
OGÓLNE ROZPORZĄDZENIE O OCHRONIE DANYCH OSOBOWYCH

ZNP

Związek Nauczycielstwa Polskiego

Co to jest RODO

INFORMATOR O ZMIANACH W PRZEPISACH DOTYCZĄCYCH DANYCH OSOBOWYCH

Warszawa, 2018

Co to jest RODO. Informator o zmianach w przepisach dotyczących danych osobowych
Copyright © Związek Nauczycielstwa Polskiego 2018

Wydawca
Związek Nauczycielstwa Polskiego
ul. Smulikowskiego 6/8
00-389 Warszawa
www.znp.edu.pl
znp@znp.edu.pl

Opracowanie merytoryczne
Kancelaria Adwokacka Wachowski

Projekt graficzny
Lena Maminajszwili/masz

Zdjęcia
fotolia

Korekta
Jolanta Lewińska

Skład, łamanie i druk
studio reklamy i wydawnictw masz

Publikacja nieodpłatna, nie może być sprzedawana. Dostępna w wersji elektronicznej na stronie www.znp.edu.pl. Wszelkie prawa zastrzeżone. Przedruk, kopiowanie, skracanie, wykorzystywanie całości tekstu lub jego fragmentu może być dokonane wyłącznie w celach niekomercyjnych, pod warunkiem podania źródła.

WSTĘP

Koleżanki i Koledzy,

oddajemy w Wasze ręce informator omawiający zagadnienie ochrony danych osobowych w Związku Nauczycielstwa Polskiego, uregulowane przez RODO (Rozporządzenie Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE), czyli ogólne rozporządzenie o ochronie danych, które wchodzi w życie 25 maja 2018 r.

Z tego informatora dowiecie się, jakie będą zadania Związku, jego oddziałów i okręgów w przetwarzaniu i ochronie danych osobowych, jakie są podstawowe pojęcia używane w RODO oraz jakie zasady ono wprowadza. Poznacie również zadania Inspektora Ochrony Danych i sytuacje, w jakich możesz lub musisz się z nim skontaktować.

Publikacja ta zawiera liczne przykłady i wyjaśnienia dotyczące przetwarzania danych osobowych z uwzględnieniem specyfiki działalności Związku Nauczycielstwa Polskiego.

Zastosowane wyróżnienia graficzne podkreślają to, co jest szczególnie ważne i godne zapamiętania.

Przykład:
Jeśli pobieramy dane ze względu na działalność związkową, to nie możemy następnie rozsyłać danych naszych członków np. do firm zajmujących się marketingiem, bo byłoby to niezgodne z celem ich pobrania.

Wierzymy, że informator wyjaśni Wasze wątpliwości i rozwieje obawy dotyczące wejścia w życie RODO. Pokaże również, że ochrona danych osobowych nie jest trudna do wdrożenia, jeśli podejdzie się do niej rozważnie.

Dostosowanie działalności ZNP do wymogów RODO nie tylko ułatwi nam funkcjonowanie i pracę z danymi osobowymi, ale ukaże Związek jako instytucję profesjonalną i odpowiedzialną za swoje członkinie i swoich członków.

Jakie zmiany?

Od 25 maja 2018 roku zaczyna obowiązywać tzw. RODO, czyli Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Po co te wszystkie zmiany?

Prawo już od jakiegoś czasu nie nadąża za zmieniającą się dynamicznie rzeczywistością. W przypadku ochrony danych osobowych, gdzie postęp technologiczny zrewolucjonizował możliwości magazynowania, przetwarzania i analizowania danych, które ludzie zostawiają niemalże wszędzie, zmiany w prawie były konieczne.

Dane osobowe to nie tylko imię i nazwisko czy numer PESEL, ale także numer telefonu, adres IP (nawet zmienny), a nawet nagrany głos, jeśli można rozpoznać osobę mówiącą za pomocą odpowiedniego oprogramowania do przetwarzania takich informacji.

Co to oznacza?

Oznacza to, że trzeba przygotować się do zmiany. To znaczy poznać jej zakres, zrozumieć jej sens i dostosować swoje wewnętrzne procedury do nowych wymogów prawnych.

Niektóre z dotychczasowych obowiązków znikną, dojdzie kilka nowych.

Ważną rzeczą, którą trzeba mieć na uwadze, jest wprowadzenie administracyjnych kar pieniężnych za nieprzestrzeganie przepisów RODO aż do wysokości 20 000 000 euro (dwudziestu milionów euro)!

W dalszej części zostaną przedstawione podstawowe informacje związane z nowym przetwarzaniem danych osobowych.

PODSTAWOWE DEFINICJE

Podane dalej definicje pozwolą na zrozumienie charakteru zmian. Niektóre z tych pojęć zostały ze sobą zestawione i wskazane w grupach, aby od samego początku dostrzec różnice bądź podobieństwa między nimi.

Administrator danych osobowych to podmiot (osoba fizyczna, osoba prawna lub jednostka nieposiadająca osobowości prawnej, jak np. filie OUPiS), który ustala cele i środki przetwarzania. Cele przetwarzania należy rozumieć jako pewne wartości, które mają zostać osiągnięte poprzez przetwarzanie danych osobowych.

Przykład:
Celem przetwarzania danych członka związku zawodowego jest działalność związkowa, celem przetwarzania przy przyjmowaniu kandydatów do pracy jest rekrutacja, a celem przetwarzania danych pacjenta jest jego leczenie przez szpital.

Ważne!
Z powyższego wynika, że w strukturze Związku Nauczycielstwa Polskiego administratorami danych osobowych będą:
- **Związek Nauczycielstwa Polskiego jako osoba prawna,**
- **filie OUPiS.**

Pamiętaj! Zadaniem okręgów i oddziałów ZNP będzie:
- **korzystanie z danych osobowych zgodnie z postanowieniami RODO;**
- **usuwanie danych osobowych, kiedy przestajemy z nich korzystać i pozwala na to przepis prawa;**
- **niezwłoczne (w ciągu 24 godzin) zgłaszanie Inspektorowi Ochrony Danych (IOD) wszystkich naruszeń w zakresie ochrony danych osobowych, aby ten mógł zgłosić wyciek danych organowi nadzorczemu;**
- **konsultowanie z IOD zasad przetwarzania danych, jeśli rodzą się w tym zakresie wątpliwości.**

Środki przetwarzania, czy też sposoby przetwarzania, to pewne narzędzia, które mają doprowadzić do osiągnięcia celów.

Współadministrator jest z kolei podmiotem, który wspólnie z innym administratorem ustala cele i sposoby przetwarzania.

Przykład:
Możemy upoważnić jednego pracownika do przetwarzania danych i cel, dla którego te dane zostały przez nas zebrane, zostanie osiągnięty.

Pamiętaj jednak, że współadministratorzy są odmiennymi podmiotami, np. prowadzenie rekrutacji przez różne firmy i w tym celu wspólne działanie mające zmierzać do zatrudnienia pracowników do tych firm.

Podmiot danych to osoba, której dane osobowe są przetwarzane. Niekoniecznie musi to być osoba bezpośrednio przekazująca nam dane, bo często pozyskanie danych następuje od osoby trzeciej,

Przykład:
W sytuacji, w której członek związku podaje dane członków swojej rodziny w celu skorzystania z zasiłku statutowego.

Podmiot przetwarzający jest osobą, która przetwarza dane osobowe, ale nie jako administrator, bo nie ustala celów i sposobów przetwarzania, ale dokonuje przetwarzania w imieniu administratora. Wyjaśnić można to tak, że gdyby nie było administratora, to wówczas podmiot przetwarzający nie przetwarzałby tych konkretnych danych. To administrator przekazuje dane do przetwarzania podmiotowi przetwarzającemu.

Przykład:
Korzystamy dzisiaj z usług dysków sieciowych, czyli miejsc, gdzie możemy przechowywać swoje dane. Aby móc korzystać z takich miejsc, musimy najczęściej zaakceptować regulamin na stronie internetowej lub zawrzeć umowę. Następnie umieszczamy np. listę osób będących członkami związku w danym okręgu na takim właśnie dysku sieciowym. Właściciel przestrzeni, na której magazynujemy dane, nie gromadzi ich dla siebie. Gdyby nie nasza działalność, nie otrzymałby tych konkretnych danych. To my pierwotnie otrzymaliśmy dane, a następnie umieściliśmy je na przestrzeni dyskowej, aby je tam przechowywać. Właściciel przestrzeni dyskowej magazynuje więc te dane w naszym imieniu.
Drugim przykładem takiej działalności może być obsługa księgowo-płacowa, jeśli jest zewnętrzna.

Dane osobowe są to wszelkie informacje, które mogą doprowadzić do bezpośredniego lub pośredniego zidentyfikowania oso-

by fizycznej. Danymi osobowymi są więc: imię, nazwisko, PESEL, fotografia, linie papilarne, numer telefonu, adres e-mail (jeśli zawiera w sobie element identyfikujący właściciela skrzynki pocztowej, np. jankowalski@poczta.pl) czy też adres IP, i to zarówno stały, jak i zmienny. Nawet zakodowana praca pisemna na egzaminie, sporządzona przez studenta, może być traktowana jako dana osobowa.

RODO rozróżnia **dane osobowe zwykłe**, te, o których mowa powyżej, i **dane osobowe wrażliwe**, którymi są:

- pochodzenie rasowe lub etniczne;
- poglądy polityczne;
- przekonania religijne lub światopoglądowe;
- przynależność do związków zawodowych;
- dane genetyczne;
- dane biometryczne (dane, które dzięki specjalnemu przetwarzaniu technicznemu mogą doprowadzić do identyfikacji osoby, np. za pomocą programu do rozpoznawania twarzy);
- dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby.

Przetwarzanie to wszelkie operacje przeprowadzane na danych osobowych. Może to być ich zbieranie, magazynowanie, przechowywanie, udostępnianie, przesyłanie, pobieranie itd. Nawet kiedy niszczysz dane osobowe, to wykonujesz operacje przetwarzania. Przetwarzaniem jest więc niemalże każda operacja na danych osobowych.

Naruszenie ochrony danych to wszelkie sytuacje, w których dane osobowe są przypadkowo utracone, zniszczone lub ujawnione nieuprawnionym odbiorcom.

Odbiorca to z kolei osoba, której ujawnia się dane osobowe.

Pseudonimizacja jest to takie przetworzenie danych osobowych, że nie można ich przypisać do konkretnej osoby bez użycia dodatkowych informacji znajdujących się w innym miejscu. Przykładem pseudonimizacji jest działanie polegające na tym, że na karcie pacjenta nie ma jego imienia i nazwiska, ale

wygenerowany numer, a identyfikacja tego pacjenta może nastąpić poprzez sprawdzenie w osobnej bazie, do którego imienia i nazwiska odnosi się wygenerowany numer. Należy jednak odróżnić pseudonimizację od anonimizacji, czyli takiego zmodyfikowania danych, że nie można na ich podstawie zidentyfikować osoby, której dotyczą, np. jeśli danym zamiast imienia i nazwiska zostały nadane numery bez połączenia tych numerów z imionami i nazwiskami przechowywanymi w innym miejscu.

Zgoda jest to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie swoich danych osobowych. Dalej dowiesz się, kiedy trzeba odbierać oświadczenie, a kiedy wystarczy do przetwarzania wyraźne działanie potwierdzające osoby, której dane dotyczą.

Przykład:
Uporządkowane według daty e-maile w elektronicznej skrzynce pocztowej.

Zbiór danych to z kolei zestaw danych uporządkowany według określonych kryteriów. Zbiór może być scentralizowany, zdecentralizowany, rozproszony funkcjonalnie lub geograficznie.

Przykład zbioru zdecentralizowanego.
Administratorem jest związek zawodowy, który ma zbiór danych swoich członków. Związek działa na terenie całego kraju, bo na terenie całego kraju zamieszkują jego członkowie. Dane zbierane przez poszczególne ogniwa związku do zbioru danych są częścią jednego zbioru. Nie mamy tu do czynienia z sytuacją, w której istniałoby tyle zbiorów danych członków, ile byłoby miejsc, w których dane są zbierane czy przechowywane.

ZASADY PRZETWARZANIA

RODO jest aktem prawnym ogólnym, dlatego też wprowadza zestaw zasad, według których należy dokonywać przetwarzania. Co oznacza, że za każdym razem, kiedy dokonuje się operacji przetwarzania, trzeba mieć na względzie wskazane zasady w taki sposób, aby zabezpieczyć się przed ewentualnymi karami.

Zasadami wskazanymi w RODO są:

- **Zasada zgodności z prawem**, rzetelności oraz przejrzystości przetwarzania, polegająca na tym, że za przetwarzaniem musi stać uzasadnienie prawne, a przetwarzanie musi być jasne i klarowne dla osoby, której dane są przetwarzane, oraz musi być prowadzone w sposób rzetelny, czyli taki, żeby nie narażać interesów czy praw osób, których dane są przetwarzane.
- **Zasada ograniczenia celu,** która polega na tym, że za przetwarzaniem już przy samym pozyskiwaniu danych stoi ściśle określony cel. Nie można gromadzić danych „na zapas".
- **Zasada minimalizacji danych**, czyli zbieranie w zakresie niezbędnie koniecznym do osiągnięcia celów.
- **Zasada prawidłowości** ma na celu zapobieganie niepożądanym konsekwencjom dla podmiotów danych w związku z przetwarzaniem ich nieprawidłowych danych. Dlatego też RODO nakłada obowiązek badania, czy dane są prawidłowe, oraz w miarę możliwości obowiązek ich usunięcia albo sprostowania, jeśli okażą się nieprawidłowe.

Przykład:
Jeśli pobieramy dane ze względu na działalność związkową, to nie możemy następnie rozsyłać danych naszych członków np. do firm zajmujących się marketingiem, bo byłoby to niezgodne z celem ich pobrania.

Przykład:
Jeśli chcemy przyjąć kogoś w poczet członków związku, to wówczas nie prosimy go o dane dotyczące jego wzrostu, wagi, imion rodzeństwa, gdyż nie jest to potrzebne do osiągnięcia celu, którym jest zrzeszenie w związku zawodowym.

Przykład:
Kiedy w poczet członków związku zostanie przyjęta omyłkowo osoba, która nie ma ze związkiem zawodowym nic wspólnego (nie składała deklaracji), związek ma obowiązek przywrócenia zgodności danych ze stanem faktycznym, w tym przypadku usunięcia lub zniszczenia danych osoby przypadkowo przyjętej do związku.

- **Zasada ograniczenia przechowywania** polega z kolei na tym, że dane osobowe nie mogą być przechowywane przez nieskończenie długi czas i muszą zostać usunięte lub zniszczone, kiedy już nie są niezbędne do celów, dla których zostały pobrane.

Pamiętaj jednak, że dane osobowe mogą być pobierane w kilku celach, a wówczas ich usunięcie może nastąpić, kiedy nie są już potrzebne do żadnego z nich.

- **Zasada integralności i poufności** wskazuje, że należy dbać, aby nie doszło do naruszeń ochrony danych osobowych. Jeśli wdrożona została polityka ochrony danych osobowych, wówczas należy przestrzegać jej postanowień.

Przykład:

Przykład: Jeśli przetwarzane są dane wrażliwe, nie można dopuścić do tego, by ich nośniki (to znaczy: dokumenty, otwarte ekrany komputerów) były ogólnodostępne np. na biurku. Tak samo, jeśli przechowywane są takie dane, nie można tego robić w sposób, który umożliwi każdemu dostęp do danych, np. w niezamykanej szafce.

Przykład:

Kiedy ktoś jest przyjmowany do pracy, wówczas celem przetwarzania jest przeprowadzenie procesu rekrutacji. Jeśli jednak ktoś nie zostanie przyjęty, to może wytoczyć powództwo o dyskryminację w zatrudnieniu. Aby móc bronić się, że pracodawca nie przyjął kogoś do pracy ze względów obiektywnych, może on przechowywać dane osobowe przedstawione przez kandydatów do pracy dłużej, tj. aż do czasu przedawnienia ich roszczeń (czyli do czasu, kiedy mogą pozwać potencjalnego pracodawcę do sądu z powodu niezatrudnienia). Kiedy minie ten czas, takie dane muszą być zniszczone lub usunięte. Jeśli dane są przechowywane, aby zabezpieczyć się przed roszczeniami, wówczas nie można przetwarzać ich w innym celu, np. oferując tym osobom zatrudnienie na inne stanowiska, na które jest rekrutacja, zakładając, że nie ma innej podstawy przetwarzania.

- **Zasada rozliczalności** jest zasadą najważniejszą z punktu widzenia zabezpieczenia się przed odpowiedzialnością. W każdym momencie w razie kontroli musimy być w stanie wykazać, że przetwarzamy dane osobowe w oparciu o wskazane powyżej zasady przetwarzania. To właśnie realizacja zasady rozliczalności nakłada konieczność dostosowania się do obowiązków wskazanych w następnych punktach tej broszury.

PRZESŁANKI PRZETWARZANIA

Podobnie jak w dotychczasowym stanie prawnym, nie możemy przetwarzać danych osobowych, jeśli nie jesteśmy w stanie wskazać podstawy (przesłanki) do takiego przetwarzania. **Różnica polega na tym, że teraz za przetwarzanie bez podstawy prawnej grozić będą dotkliwe sankcje.**

Różne są podstawy przetwarzania dla danych osobowych zwykłych oraz danych osobowych wrażliwych. Różne są też kary, jeśli będziemy przetwarzać dane z poszczególnych kategorii bez podstawy prawnej. Zawsze przetwarzając dane osobowe, musimy zastanowić się nad tym, czy mamy którąkolwiek z przesłanek, aby oprzeć na niej swoje operacje na danych osobowych.

Dla danych osobowych zwykłych przesłankami przetwarzania są:

- **Zgoda** osoby, której dane dotyczą. Zgoda musi zostać wyrażona w jednym określonym celu lub w większej liczbie określonych celów. RODO wprowadza nowość polegającą na tzw. zgodzie konkludentnej (innymi słowy dorozumianej), która polega na tym, że możemy przetwarzać dane osobowe osoby, która nie wyraziła swojej zgody bezpośrednio, np. nie klikając w okienko formularza na stronie internetowej, ale przez samo korzystanie ze strony internetowej i zostawianie tam swoich danych osobowych.
  Należy jednak wskazać, że osoba, która wyraża zgodę na przetwarzanie swoich danych osobowych, musi zostać poinformowana o celach przetwarzania oraz o możliwości wycofania zgody na przetwarzanie w dowolnym momencie. Pamiętać też należy, że **wycofanie zgody nie wpływa w żaden sposób na wcześniejsze przetwarzanie, które odbywało się zgodnie z prawem i jest ważne** (za takie przetwarzanie nie można ponieść negatywnych konsekwencji). Informacja o możliwości każdorazowego wycofania zgody na przetwarzanie danych osobowych musi być przedstawiona przed rozpoczęciem przetwarzania.

RODO nakłada także jeszcze jedno obostrzenie dotyczące zgody oraz jej wycofania, a mianowicie zgoda

Przykład:
Kiedy prowadzimy stronę internetową, to przy pierwszym włączeniu strony powinno pojawić się wyraźne zawiadomienie o tym, że korzystanie ze strony jest zezwoleniem na przetwarzanie danych osobowych, oraz o tym, że w dowolnej chwili można taką zgodę wycofać.

musi być równie łatwa do wycofania, co jej udzielenie. Pamiętaj zatem, że jeśli odbieramy zgodę ustnie, to nie możemy wymagać, aby jej wycofanie nastąpiło na piśmie, ponieważ pisemne wycofanie zgody czy zaznaczenie właściwego okienka wyboru na stronie internetowej jest trudniejsze niż deklaracja typu: „Wycofuję swoją zgodę na przetwarzanie moich danych osobowych".

Miej na względzie także to, że jeśli odbieramy od kogokolwiek zgodę na przetwarzanie danych osobowych na piśmie, musimy wyraźnie oddzielić zapytanie o zgodę od innych zapytań!

Przykład:

NIEPRAWIDŁOWO

Wyrażam zgodę na przekazywanie do mnie informacji drogą elektroniczną o promocjach i ofertach sklepu internetowego Wehikuł na podany przeze mnie adres e-mail. Wyrażam zgodę na przetwarzanie moich danych osobowych w celach marketingowych przez sklep internetowy Wehikuł, który jest administratorem danych osobowych przeze mnie podawanych.

PRAWIDŁOWO

Wyrażam zgodę na przekazywanie do mnie informacji drogą elektroniczną o promocjach i ofertach sklepu internetowego Wehikuł na podany przeze mnie adres e-mail.

Wyrażam zgodę na przetwarzanie moich danych osobowych w celach marketingowych przez sklep internetowy Wehikuł, który jest administratorem danych osobowych przeze mnie podawanych.

Jeśli nie dostosujemy swojego zapytania o zgodę do wskazanego formatu, wówczas przetwarzanie będzie odbywało się niezgodnie z prawem, a tym samym będziemy mogli ponieść administracyjną karę pieniężną. Chociaż możliwość pobierania zgód w sposób dorozumiany może się wydawać wygodna, to jednak pamiętaj o zasadzie rozliczalności, o której mowa w pkt. 2. Zgodnie z RODO można przetwarzać dane na podstawie zgody, pod warunkiem że się wykaże organom nadzorczym, iż faktycznie posiada się powyższą zgodę na przetwarzanie danych osobowych. Dlatego też tworzenie systemów przetwarzania opartych na zgodzie dorozumianej jest ryzykowne.

Ważne! Nie trzeba pobierać zgody na przetwarzanie danych osobowych w sytuacji, w której posiadamy inną podstawę do przetwarzania. Z przetwarzaniem na podstawie zgody wiąże się wiele praw osób, których dane są przetwarzane (o czym przeczytasz dalej), a z których nie można skorzystać, jeśli przetwarzanie odbywa się na innej podstawie prawnej. Dlatego też odebranie zgody na przetwarzanie danych osobowych, kiedy występują inne przesłanki może zostać potraktowane

jako wprowadzenie podmiotów danych w błąd, a tym samym może zostać zinterpretowane jako naruszające zasadę zgodności z prawem, rzetelności oraz przejrzystości przetwarzania. Dlatego też nie należy zabezpieczać przetwarzania danych osobowych przez dodatkowe odbieranie zgód.

- RODO dopuszcza także jako przesłankę do przetwarzania **niezbędność do wykonania umowy, której stroną jest osoba, której dane dotyczą**, lub przetwarzanie jest niezbędne do podjęcia działań na żądanie osoby przed zawarciem umowy.

Przykład:
Zawierając umowę najmu mieszkania, nie musimy od najemcy pobierać zgody na przetwarzanie jego danych osobowych, gdyż są one nam potrzebne do zawarcia umowy.

Pamiętaj jednak o zasadzie minimalizacji danych przy pobieraniu danych osobowych (pobierać należy tylko te dane osobowe, które są niezbędne do zawarcia określonej umowy)

- **Przetwarzanie może być także związane z podjęciem przetwarzania potrzebnego przed zawarciem umowy.** Modelowym przykładem jest proces rekrutacyjny. Przed zawarciem umowy o pracę nie ma żadnej umowy między stronami, dlatego też ta przesłanka jest wówczas spełniona. Inaczej jednak rzecz się ma w przypadku, kiedy ten sam kandydat bierze udział w innych procesach rekrutacji na podstawie jednego CV, które przesłał. Jeśli nie odebraliśmy od niego przy pierwszej rekrutacji zgody na przetwarzanie jego danych **w związku z innymi procesami rekrutacji na stanowiska tożsame,** wówczas nie możemy używać jego CV do innego przetwarzania danych osobowych w procesach rekrutacyjnych.

Przykład:
Jeśli jesteśmy pracodawcą, wówczas przepisy prawa pracy nakładają na nas obowiązek przetwarzania danych pracowników. Tak samo jest w przypadku, w którym przetwarzamy dane osobowe w celach opieki zdrowotnej i musimy przetwarzać dane osobowe pacjentów.

- W zależności od branży **przetwarzanie może być także oparte na ciążącym na podmiocie obowiązku prawnym.**
- RODO dopuszcza także przetwarzanie danych w celu ochrony żywotnych interesów osoby, której dane dotyczą. Żywotne interesy to takie, które dotyczą zdrowia, życia, ale także interesu majątkowego.

Ważne! Jest to jednak podstawa przetwarzania, z której można skorzystać wyłącznie w sytuacji, w której nie można oprzeć przetwarzania na żadnej innej podstawie prawnej.

- Kolejną przesłanką jest **przetwarzanie danych w celu ochrony interesu publicznego** lub **skutecznego sprawowania władzy publicznej.**

- Ostatnią z podstaw przetwarzania **danych osobowych zwykłych** jest **niezbędność do celów, które wynikają z prawnie uzasadnionych interesów realizowanych przez administratora**, chyba że nadrzędny charakter mają prawa i wolności osób, których dane są przetwarzane.

Ważne! Inaczej jest w przypadku danych osobowych wrażliwych, których, poza kilkoma wyjątkami, nie wolno przetwarzać.

Podobnie jak przy danych osobowych zwykłych, można przetwarzać dane osobowe wrażliwe pod warunkiem otrzymania zgody osoby, której dane dotyczą. **Uzyskana zgoda na przetwarzanie danych osobowych wrażliwych musi być zgodą wyraźną, czyli wyraźnie wskazywać, że osoba. której dane dotyczą. wyraża zgodę na przetwarzanie jej danych osobowych. Nie może być tu mowy o zgodzie konkludentnej.** Natomiast **nie jest możliwe przetwarzanie danych osobowych wrażliwych na podstawie zgody, jeśli jest to zabronione przez przepisy prawa powszechnie obowiązującego.**

Można również przetwarzać dane wrażliwe, jeśli wynika to z obowiązków lub praw w dziedzinie prawa pracy, zabezpieczenia społecznego lub ochrony socjalnej.

Przetwarzanie danych wrażliwych jest także możliwe w sytuacji, w której jest niezbędne do ochrony żywotnych interesów osoby, której te dane dotyczą, a jest ona fizycznie lub prawnie niezdolna do wyrażenia zgody na przetwarzanie.

Przykład:
Banki w swojej działalności muszą bronić się przed nieuczciwymi klientami, którzy nie spłacają pożyczek bankowych. Dlatego też ich uzasadnionym prawnie interesem jest tworzenie tzw. czarnych list klientów, którzy nie spłacają kredytów i pożyczek, aby nie destabilizować systemu bankowego, w którego skład wchodzą także ludzie terminowo regulujący swoje długi.

Przykład:
Pracownicy przedstawiają pracodawcy zaświadczenia dotyczące ich stanu zdrowia i przechodzą badania kontrolne. Chociaż pracodawca jest uprawniony wyłącznie do otrzymywania informacji dotyczących tego, czy pracownik jest zdolny lub niezdolny do pracy, to jednak ze względu na kontekst są to dane wrażliwe – niezdolność do pracy informuje o ogólnym stanie zdrowia pracownika, co jest daną wrażliwą.

Przykład:
Osoby chore, wymagające opieki, często są prowadzone przez profesjonalnych opiekunów. Zdarza się, że demencja podopiecznych uniemożliwia jakikolwiek kontakt z nimi, a tym bardziej uniemożliwia udzielenie przez nie zgody na przetwarzanie danych. Najczęściej to rodzina przekazuje opiekunom dane osób, którymi mają się zajmować.

Możliwe jest przetwarzanie, które odbywa się w ramach struktur związku zawodowego, związku wyznaniowego, fundacji czy partii politycznej, pod warunkiem że dotyczy ono członków i ich rodzin, byłych członków lub osób utrzymujących z nimi stałe

kontakty. Pamiętaj, że przetwarzanie takich danych jest możliwe tylko w sytuacji, w której prawa i wolności osób, których dane są przetwarzane, zostały odpowiednio zabezpieczone.

Wolno przetwarzać dane osobowe wrażliwe, jeśli zostały w sposób wyraźny upublicznione.
Można przetwarzać dane wrażliwe w następujących przypadkach:

- ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
- jeżeli jest to niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, przy założeniu, że robi to osoba, która jest prawnie zobowiązana do zachowania w tajemnicy informacji z takiego przetwarzania;
- jeżeli jest to niezbędne do celów archiwalnych, w interesie publicznym, do celów badań naukowych, historycznych lub do celów statystycznych.

Ta przesłanka przetwarzania danych wrażliwych nie wyłącza jednak konieczności dostosowania swoich działań na danych osobowych do przepisów prawa powszechnie obowiązującego. Oznacza to tyle, że jeśli przetwarzasz takie dane, to powinieneś zapewnić im ochronę analogiczną do tej, którą zapewniasz danym w swojej codziennej działalności. Jeśli jednak twoje zbiory archiwalne obejmują wyłącznie informacje o osobach zmarłych, wówczas nie musisz do nich stosować wymogów wskazanych przez RODO.

Przykład:
Przetwarzając dane dotyczące członkostwa w związku zawodowym, należy dołożyć szczególnej staranności, aby nie dochodziło do naruszeń oraz aby naruszeniom zapobiegać. Poza tym inny będzie cel przetwarzania danych osobowych obecnych członków, a inny w przypadku byłych członków. Celem przetwarzania w przypadku byłych członków jest limitowanie ich roszczeń do związku zawodowego, po tym, kiedy z tego związku wystąpią, a także możliwość korzystania z niektórych uprawnień wypływających z członkostwa w związku dla rodzin osób, które w związku niegdyś były.

Przykład:
Danymi wrażliwymi są informacje ujawniające przekonania religijne lub światopoglądowe danej osoby. Jeśli zatem dana osoba upublicznia swoje przekonania światopoglądowe w serwisie internetowym czy też poprzez udział w manifestacji, w czasie której uczestnicy manifestują bezwyznaniowość, wówczas wolno przetwarzać jej dane w upublicznionym zakresie.

Ważne! Informacja o przynależności do związku zawodowego jest daną osobową wrażliwą.

Przykład:
Pracodawcy, posiadając tę informację, mogą unikać przyjmowania do pracy osób, które należą do związku zawodowego.

PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

RODO wprowadza katalog praw osób, których dane są przetwarzane.

Osoby te mają w pierwszej kolejności prawo do bycia poinformowanymi. Jako administrator danych jesteśmy zobowiązani przedstawić tym osobom zbiór informacji dotyczących administratora oraz przetwarzania (patrz: zasada zgodności z prawem, przejrzystości i rzetelności).

Informacje, które musimy w tym przypadku przekazać, to:

- kto jest administratorem oraz podać jego dane kontaktowe;
- dane Inspektora Ochrony Danych, jeśli to nas dotyczy (patrz niżej);
- cele przetwarzania oraz podstawę tego przetwarzania (podstawy wymienione w pkt. 3 przewodnika);
- prawnie uzasadnione interesy administratora, jeśli przetwarzanie odbywa się w oparciu o tę przesłankę;
- informacje o odbiorcach danych lub ich kategoriach;
- czas przetwarzania, jeśli to możliwe;
- informacje o prawie dostępu do danych, ich sprostowania, usunięcia, czy ograniczenia przetwarzania, prawie do wniesienia sprzeciwu oraz prawie do przenoszenia danych;
- informacje o prawie do cofnięcia zgody, tylko w sytuacji, w której jest ona podstawą przetwarzania;
- informacje o prawie wniesienia skargi do organu nadzorczego;
- informacje dotyczące tego, jaka jest podstawa podania danych i konsekwencje ich niepodania;
- informacje o zautomatyzowanym podejmowaniu decyzji oraz o profilowaniu;
- informacje o zmianie celu przetwarzania, jeśli to nas dotyczy.

Pamiętaj jednak, że nie zachodzi obowiązek informacyjny, jeśli osoba, której dane dotyczą, posiada powyższe informacje.

Zwróć uwagę na to, że często dane osobowe nie są pobierane od osób, których one dotyczą. Przykładowo przy korzystaniu z usług medycznych i dokonywaniu rejestracji często pobiera się dane kontaktowe osoby, która ma

zostać poinformowana w razie wykonywania jakichś zabiegów medycznych na pacjencie. RODO przewidziało i tę sytuację. Do elementów wskazanych powyżej przy realizacji obowiązku informacyjnego musisz dodać:

- źródło pozyskiwania danych (czyli np. osobę, od której otrzymaliśmy dane osobowe) czy wskazanie źródła publicznie dostępnego, jeśli to właśnie z niego zaczerpnęliśmy dane osobowe (np.: centralna ewidencja informacji o działalności gospodarczej może być takim źródłem).

Na udzielenie powyższych informacji mamy określony czas. Nowe prawo daje na to miesiąc od pozyskania danych. Jeśli jednak będziemy chcieli skontaktować się z osobą, której dane dotyczą, za pomocą udzielonych nam danych, informacje powinniśmy przekazać najpóźniej przy pierwszym kontakcie, a jeśli mamy zamiar ujawnić dane osobowe innemu odbiorcy, informacje powinniśmy przekazać najpóźniej przy takim ujawnieniu (czyli wtedy, kiedy przekazujemy te dane swoim podmiotom przetwarzającym, wówczas musimy poinformować osobę, której dane dotyczą).

Pamiętaj! Jeżeli zamierzamy przetwarzać dane osobowe w innym celu, niż zostały zebrane, musimy zawiadomić o tym daną osobę.

Inne prawa osób, których dane są przetwarzane, mają charakter bardziej konkretny. **Zgodnie z prawem dostępu osoba, której dane dotyczą, ma prawo uzyskania informacji, czy przetwarzamy dane osobowe jej dotyczące.** Jeśli nie przetwarzamy jej danych osobowych, zapytanie nie wywołuje skutków, poza koniecznością udzielenia jednej odpowiedzi, że dane osobowe tej osoby nie są przetwarzane.
Jeśli jednak przetwarzamy jej dane osobowe, wówczas musimy umożliwić tej osobie dostęp do jej danych, a także udzielić jej informacji, które w dużej mierze pokrywają się z tymi wymienionymi już wcześniej.

Nową rzeczą jest to, że musimy udostępnić kopię danych osobie, której dane przetwarzamy. Możemy ją udostępnić w formie elektronicznej tylko wtedy, kiedy osoba, która chce uzyskać swoje dane, nie wskaże innej formy, a zwraca się o to do nas e-mailem.

Przez takie przekazanie danych należy rozumieć nie informacje o tym, jakie dane osobowe osoby są przetwarzane, ale rzeczywiste dostarczenie kopii danych, które były świadomie przekazane przez osobę do przetwarzania.

Przykład:
Dane osobowe Jana Kowalskiego są przetwarzane przez Związek Nauczycielstwa Polskiego. Zwraca się on do Związku (lub oddziału ZNP) o kopię danych listownie. Związek odpisuje mu e-mailem i na adres poczty elektronicznej przesyła skany wszystkich danych osobowych dotyczących Jana Kowalskiego. Zachowanie Związku jest nieprawidłowe, ponieważ odpowiedź powinna być wysłana Janowi listownie, o co wnioskował.

Zapamiętaj jednak, że nie mamy obowiązku każdorazowo wysyłać kopii danych bezpłatnie.

Pierwszorazowe wysłanie kopii danych jest bezpłatne. Za kolejne kopie wysyłane do tej samej osoby możemy pobierać opłatę, nie wyższą jednak niż rozsądny koszt administracyjny (to znaczy, że nie powinniśmy czerpać korzyści z udostępnienia danych osobie, które jej dotyczą, czyli poniekąd są jej własnością).

Kolejnym prawem, o którym musimy pamiętać, jest **prawo do sprostowania danych.** To oznacza, że na żądanie podmiotu danych musimy niezwłocznie sprostować te dane, jeżeli są one nieprawidłowe. Jeżeli dane, które mamy, są niewystarczające do osiągnięcia celów przetwarzania, dla których je pobraliśmy, osoba ta może żądać ich uzupełnienia.

Następne prawo to **prawo do bycia zapomnianym** (czy też prawo do usunięcia danych). Jest ono powiązane z zasadą ograniczonego przechowywania. Prawo to budzi najwięcej kontrowersji, dlatego też powinniśmy wiedzieć, że:

- nie jest prawem bezwzględnym, czyli kiedy ktoś będzie chciał z niego skorzystać, nie zawsze będziemy musieli je zrealizować;
- dane osobowe będące przedmiotem tego prawa są zbędne do celów, dla których zostały zebrane, lub nie są przetwarzane w inny sposób;
- prawo do bycia zapomnianym należy wykonać, jeśli cofnięto zgodę na przetwarzanie, a nie sposób wskazać na inne podstawy prawne do przetwarzania;
- prawo do bycia zapomnianym musi zostać wykonane, gdy osoba wniosła sprzeciw do przetwarzania (patrz niżej), a nie mamy nadrzędnych podstaw do przetwarzania jej danych osobowych jako administrator;
- musimy wykonać to prawo, jeśli wcześniejsze przetwarzanie, które wykonywaliśmy, było niezgodne z prawem;
- dane osobowe muszą zostać usunięte, bo stanowi tak prawo, któremu podlegamy;
- jeśli świadczyliśmy danej osobie usługi drogą elektroniczną i zwróci się ona do nas o bycie zapomnianym, wówczas musimy zrealizować jej prawo.

Zapamiętaj, że jeśli nie wystąpi żadna z przesłanek, która pozwoli na przetwarzanie danych osobowych, pomimo zgłoszenia chęci skorzystania z prawa do bycia zapomnianym, wówczas **musimy niezwłocznie usunąć dane osoby,** która chce skorzystać z tego prawa.

Kolejna uwaga dotyczy prawa do ograniczenia przetwarzania. Ograniczenie przetwarzania polega na tym, że możemy przetwarzać dane osobowe tylko przez ich przechowywanie, tj. nie możemy wysyłać,

przekazywać, a nawet niszczyć czy usuwać danych. Chyba że otrzymamy zgodę osoby na przetwarzanie jej danych lub przetwarzanie jest nam potrzebne do obrony roszczeń (np. kiedy chcemy kogoś pozwać lub ktoś pozywa nas), bądź też przetwarzanie jest potrzebne do ochrony praw innej osoby fizycznej lub prawnej.

Będziemy musieli wykonać prawo do ograniczenia przetwarzania, jeśli zażąda tego osoba, której dane dotyczą, oraz w następujących przypadkach:

- podmiot danych zakwestionuje prawidłowość jego danych;
- przetwarzaliśmy dane niezgodnie z prawem, ale osoba nie chce skorzystać z prawa do bycia zapomnianym, lecz woli ograniczenie przetwarzania;
- dane nie są potrzebne do celu, w którym je pobraliśmy, ale są potrzebne osobie, której dotyczą, do obrony swoich ewentualnych roszczeń (np. kiedy chce kogoś pozwać i potrzebne jej dowody);
- jeśli osoba, której dane dotyczą, wniosła sprzeciw, a jeszcze nie zbadaliśmy, czy mamy prawnie uzasadnione podstawy do przetwarzania, które są nadrzędne względem praw osoby, której dane dotyczą.

Przykład:
Związek zbiera podpisy poparcia dla pewnych inicjatyw. Działalnością statutową Związku jest wpływanie na kształt aktów prawnych dotyczących statusu prawnego pracowników oświaty. Do tego, aby lista poparcia była wiarygodna, musi znaleźć się na niej dana osobowa identyfikująca jednoznacznie osobę udzielającą poparcia. Prawnie uzasadnionym interesem Związku jest w tej sytuacji, aby pobierać numer PESEL od osób popierających inicjatywę w celu realizowania wskazanego zadania statutowego, chociaż brak jest przepisu prawa, który by na jego pobieranie bezpośrednio pozwalał.

Ważne! Jeśli do ograniczenia przetwarzania dojdzie, a następnie ma zostać ono uchylone, to wówczas musimy o tym poinformować osobę, której ograniczenie przetwarzania dotyczyło!

W związku z wymienionymi prawami pamiętaj także o tym, że w przypadku ich realizacji będziemy zobowiązani do poinformowania o konsekwencji tych praw odbiorców danych. Miej jednak na względzie, że nie jest to wymóg bezwzględny, jeśli poinformowanie odbiorców będzie niemożliwe albo będzie wymagało niewspółmiernie dużego wysiłku!

Dodatkowym prawem, które obecnie będą miały osoby udostępniające dane, jest **prawo do przenoszenia danych**. Polegać ma ono na tym, że podmiot danych będzie mógł otrzymać w wersji nadającej się do odczytu na komputerze dane osobowe, które go dotyczą, ale tylko takie, które dostarczył nam jako administratorowi. Po otrzymaniu tych danych ma prawo przesłać

je do innego administratora bez jakichkolwiek przeszkód z naszej strony, jeżeli przetwarzaliśmy te dane na podstawie zgody lub umowy, a przetwarzanie odbywało się w sposób zautomatyzowany.

Jeśli jest to możliwe, osoba, której dane dotyczą, może żądać, abyśmy przesłali dane osobowe bezpośrednio do innego administratora.

Przykład:
Wyobraźmy sobie, że w Związku wprowadzaliśmy dane osób udostępnione przez nie do systemu informatycznego, który na podstawie przedstawionych danych kwalifikował poszczególne osoby do otrzymania zasiłków różnej wysokości w zależności od wprowadzonych informacji. Podmiot danych zwrócił się o przeniesienie jego danych do innego związku zawodowego. W takiej sytuacji powinniśmy w formacie możliwym do odczytu na komputerze (np. PDF) wysłać te dane do osoby, której dotyczą, a ona następnie może przesłać te dane do innego związku.

Następnym prawem jest **prawo do sprzeciwu.** Można z niego skorzystać w przypadku dwóch poniższych podstaw przetwarzania:

- kiedy przetwarzanie odbywa się na podstawie wykonywania zadania realizowanego w interesie publicznym;
- kiedy przetwarzanie następuje w celu realizacji prawnie uzasadnionego interesu administratora, a prawa i wolności osób, których dane są przetwarzane, nie mają charakteru nadrzędnego nad tym interesem.

Musisz pamiętać, że podobnie jak prawo do bycia zapomnianym, zgłoszenie sprzeciwu odnośnie do przetwarzania nie jest prawem bezwzględnym. A zatem w przypadku sprzeciwu możemy powołać się na ważne prawnie uzasadnione podstawy do przetwarzania, które są nadrzędne wobec interesów osoby, której dotyczą, oraz na ważną podstawę przetwarzania, tj. np. obronę lub dochodzenie roszczeń.

Jeśli jednak nie znajdziemy takich podstaw do przetwarzania, to nie możemy przetwarzać danych osobowych osoby, która wniosła wobec tego sprzeciw.

Pamiętaj także o tym, że o prawie do wniesienia sprzeciwu musimy poinformować podmiot danych w sposób wyraźny i przedstawić to prawo jasno oraz oddzielnie od wszelkich innych informacji.

Jeżeli przetwarzalibyśmy dane osobowe w celach marketingu bezpośredniego (czego nie robimy), w tym również profilowania, osoba, której dane dotyczą, mogłaby wnieść sprzeciw do takiego przetwarzania w dowolnym momencie. Jeśli faktycznie by się temu sprzeciwiła, nie moglibyśmy już dłużej przetwarzać jej danych w tym celu.

Ostatnim prawem, jest **prawo do niepodlegania decyzji wydanej w sposób zautomatyzowany.** Decyzja wydana w sposób zautomatyzowany polega na tym, że dane są wprowadzane bezpośrednio do systemu, który na podstawie jakichś wzorów wydaje rozstrzygnięcie. W Związku nie mamy do czynienia z taką sytuacją, jednak warto mieć świadomość występowania tego uprawnienia.

Od niepodlegania takiej decyzji są jednak przewidziane wyjątki:
- decyzja wydana w sposób zautomatyzowany jest niezbędna do zawarcia lub wykonania umowy pomiędzy administratorem a podmiotem danych;
- zautomatyzowane wydanie decyzji jest dozwolone prawem;
- osoba, której zautomatyzowana decyzja dotyczy, udzieliła na to wyraźnej zgody.

Jeśli wydawalibyśmy taką decyzję jako administrator, musielibyśmy wdrożyć odpowiednie środki ochrony podmiotów danych. Niezbędnym minimum, które obowiązani bylibyśmy zapewnić, to:
- interwencja człowieka (to znaczy, żeby osoba, której dane dotyczą, mogła przedstawić swój problem człowiekowi, a nie otrzymywała automatycznie generowanych komunikatów);
- możliwość przedstawienia własnego stanowiska przez osobę, której dane dotyczą;
- możliwość zakwestionowania takiej decyzji wydanej w sposób zautomatyzowany.

Ważne! Decyzja podejmowana w sposób zautomatyzowany nie może być podejmowana w oparciu o dane wrażliwe!

OBOWIĄZKI ADMINISTRATORA DANYCH

Prawa osób, których dane są przetwarzane, w naturalny sposób powodują powstanie po naszej stronie obowiązków jako administratora. Oprócz tych obowiązków jako administrator jesteśmy także zobowiązani do wypełnienia szeregu innych czynności, które są związane z technicznym aspektem przetwarzania.

Nowe przepisy nakładają na nas obowiązek, aby przetwarzanie odbywało się w sposób zgodny z prawem. Ponieważ nie ma wytycznych i wskazówek, a więc to my sami musimy ustalić, jaki będzie najlepszy sposób na zabezpieczenie praw i wolności podmiotów danych.

Przy wdrażaniu środków odpowiednich do przetwarzania należy brać pod uwagę:

- charakter (np. jakie dane przetwarzamy – zwykłe czy wrażliwe);
- zakres (czyli ile danych będziemy przetwarzali – czy będą to dane kilkudziesięciu osób, czy tysięcy);
- kontekst (co pozwala nam na przetwarzanie danych oraz jaki wpływ ma przetwarzanie na osoby, których dane są przetwarzane, oraz jakie będą tego konsekwencje dla nich);
- cele przetwarzania (ma nam to pomóc zrealizować zasadę ograniczenia celu, o której było mówione wyżej);
- ryzyko naruszenia praw i wolności osób, których dane dotyczą (co może się stać w przypadku naruszenia ochrony danych osobowych).

Tylko takie podejście do sprawy ochrony danych osobowych sprawi, że przetwarzanie będzie zgodne z prawem, a my będziemy mogli to wykazać.

Zastosowanie powyższych wytycznych sprawi, że będzie możliwe wdrożenie odpowiedniej polityki ochrony

danych osobowych. Jednorazowe wdrożenie odpowiednich zabezpieczeń nie jest wystarczające – musimy mieć na względzie, że nasze środki bezpieczeństwa muszą być możliwe do skontrolowania oraz aktualizacji.

Ponadto od 25 maja 2018 roku będziemy zobowiązani do kierowania się kryterium zgodności z prawem przy wyborze podmiotu przetwarzającego, jeśli korzystamy z jego usług.

Dodatkowo przy korzystaniu z usług podmiotu przetwarzającego musimy pamiętać także o tym, aby:

- mieć zawartą umowę na świadczenie usług przez podmiot przetwarzający;
- mieć zawarte w umowie odpowiednie postanowienia dotyczące:
  - przetwarzania tylko na udokumentowane polecenie administratora (może to być w samej umowie oraz w aneksach do niej);
  - zobowiązania się pracowników podmiotu przetwarzającego do zachowania w tajemnicy danych osobowych, z którymi zapoznali się w związku z przetwarzaniem;
  - zapewnienia podmiotu przetwarzającego, że przetwarzanie przez niego odbywa się w sposób bezpieczny oraz że jest on w stanie to wykazać (np. ma zakodowane hasłem komputery, na których znajdują się dane, oraz że nie mają do nich dostępu żadne osoby postronne);
  - przestrzegania ustaleń dotyczących korzystania z usług innego podmiotu przetwarzającego;
  - wspierania administratora w wywiązywaniu się przez niego z obowiązków wobec podmiotów danych (patrz pkt 4 niniejszego informatora dotyczący praw osób, których dane są przetwarzane);
  - wspierania administratora w kontaktach z organem nadzorczym oraz w sytuacjach, kiedy dojdzie do naruszenia ochrony danych;
  - losu danych po zakończeniu świadczenia usług przez podmiot przetwarzający (czy zwróci dane, czy być może je usunie, czy też komisyjnie zniszczy i sporządzi z tego protokół);
  - możliwości przeprowadzenia u niego audytu dotyczącego tego, czy przetwarzanie odbywa się w sposób zgodny z prawem.

Ważne! Umowa z podmiotem przetwarzającym musi bezwzględnie mieć formę pisemną.

W interesie podmiotu przetwarzającego leży, aby umowa podpisana z administratorem danych bardzo dokładnie określała jego prawa i obowiązki. Jak pamiętasz, podmiot przetwarzający nie ma sam w sobie celu przetwarzania, gdyby nie nasze zlecenie, nie przetwarzałby danych osobowych. Kiedy jednak podmiot przetwarzający wykroczy poza nasze polecenia związane z przetwarzaniem, wówczas jest traktowany jako samodzielny administrator, a tym samym znacznie zwiększa się jego odpowiedzialność (o odpowiedzialności przeczytasz dalej).

Zanotuj także, że samo zatrudnienie pracowników nie jest wystarczające, aby mogli oni przetwarzać dane osobowe. Aby przetwarzanie danych przez pracowników było możliwe, musimy udzielić im odpowiedniego upoważnienia. Istnieje różnica między przetwarzaniem, którego może dokonywać pracownik infolinii, a tym, którego może dokonywać główna księgowa.

Pamiętaj, że upoważnienie może być zarówno elementem umowy, jak i możemy stworzyć osobną listę pracowników upoważnionych do przetwarzania konkretnych danych osobowych.

REJESTR CZYNNOŚCI PRZETWARZANIA

Praktycznie każdy administrator jest zobowiązany do prowadzenia rejestru czynności przetwarzania. Jest to rejestr, w ramach którego dokumentuje się katalog informacji związanych z przetwarzaniem.

Taki rejestr powinien zawierać:

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora i wszelkich współadministratorów, a także – gdy ma to zastosowanie– przedstawiciela administratora oraz inspektora ochrony danych;
- cele przetwarzania;
- kategorie osób, których dane są przetwarzane;
- kategorie danych osobowych;
- kategorie odbiorców danych;
- czas, na który dane zostały pobrane, jeśli to możliwe (czas taki jest zwany retencją danych);
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

Taki rejestr powinien mieć formę pisemną (może to być także forma elektroniczna, czyli prowadzenie takiego rejestru na dysku zewnętrznym w ramach usługi chmury).

Przykładowy rejestr może wyglądać tak:

Dane administratora	Cele przetwarzania	Kategorie osób	Kategorie danych	Odbiorcy danych	Retencja danych	Zabezpieczenie

Rejestr ma konkretne funkcje, przede wszystkim pozwoli nam kontrolować dane, które w Związku Nauczycielstwa Polskiego są przetwarzane. Dodatkowo jako administrator musimy udostępnić prowadzony rejestr na żądanie organu nadzorczego.

Pamiętaj! Są sytuacje, w których prowadzenie rejestru czynności przetwarzania nie jest konieczne. Ma to miejsce, jeśli:

- przetwarzanie nie powoduje ryzyka naruszenia praw i wolności osób, których dotyczy;
- przetwarzanie ma charakter sporadyczny;
- przetwarzanie nie dotyczy danych wrażliwych.

POSTĘPOWANIE W SYTUACJACH NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Nowe przepisy przewidują także wiele rozwiązań w sytuacji naruszenia ochrony danych osobowych. Jeśli do naruszenia dojdzie, o ile nie skutkuje ono naruszeniem praw i wolności osób fizycznych, wówczas należy zgłosić je natychmiast (tego samego dnia) Inspektorowi Danych Osobowych w Związku, który w imieniu ZNP ma obowiązek niezwłocznie (nie później jednak niż w ciągu 72 godzin od stwierdzenia naruszenia) zgłosić ten fakt organowi nadzorczemu.

Jeśli spóźnimy się z wyjaśnieniami dla organu nadzorczego, będziemy musieli mu wskazać przyczyny opóźnienia.

Pamiętaj! Jeśli będziemy korzystać z usług podmiotów przetwarzających, to muszą one informować nas o każdym naruszeniu ochrony danych osobowych, ponieważ to Związek jako administrator ma dokonać oceny tego, czy naruszenie może powodować naruszenie praw i wolności osób, których dane są przetwarzane.

Zgłoszenie musi zawierać:

- opis charakteru naruszenia;
- kategorię osób, których naruszenie dotyczy;
- liczbę osób, których naruszenie dotyczy;
- dane Inspektora Ochrony Danych;
- opis możliwych konsekwencji naruszenia ochrony danych osobowych;

- zastosowane środki w celu zaradzenia naruszeniu;
- proponowane środki w celu zapobieżenia naruszeniom;
- środki zastosowane lub proponowane, które mają zmniejszyć negatywne skutki naruszenia ochrony danych.

Zgłoszenie może przybrać dowolną postać, tj. zarówno można zgłaszać naruszenie, opisując wskazane powyżej punkty, jak również stworzyć tabelę. Dla wygody łatwiej stworzyć szablon dokumentu, który następnie będzie wypełniany w razie naruszenia. Pamiętaj także o czasie, w którym należy dokonać zgłoszenia naruszeń.

Szablon w formie tabeli może przybrać taki kształt:

Opis naruszenia	Kategoria osób, których dotyczy naruszenie	Liczba osób, których dotyczy naruszenie	Dane IOD	Możliwe konsekwencje naruszenia	Środki zastosowane w celu zaradzenia	Środki proponowane w celu zaradzenia	Środki mające zmniejszyć skutki

Natychmiastowe uzupełnienie tabeli może być niemożliwe. Dlatego prawdopodobnie będzie trzeba uzupełniać ją stopniowo. W taki sam sposób należy przekazać informację Inspektorowi Ochrony Danych, który będzie zgłaszał je organowi nadzorczemu.

Nie tylko organ nadzorczy musi zostać zawiadomiony o naruszeniach w ochronie danych osobowych. Również osoby, których dane przetwarzamy, mogą chcieć dowiedzieć się, co dzieje się z ich danymi osobowymi.

W jakich okolicznościach musimy je zawiadomić?
Kiedy naruszenie ochrony danych osobowych może powodować **wysokie ryzyko naruszenia praw** lub wolności osób fizycznych.

W jaki sposób trzeba to zrobić?
Bez zbędnej zwłoki.

Pamiętaj! Zwracając się do podmiotów danych z informacją o naruszeniu, należy:

- **poinformować o danych kontaktowych inspektora (IOD);**
- **opisać możliwe konsekwencje naruszenia;**
- **opisać środki podjęte w celu zmniejszenia naruszenia.**

Wyobraź sobie jednak, że mamy w swojej bazie miliony osób, których prawa zostały naruszone. Trudno byłoby poinformować je wszystkie w sposób indywidualny o naruszeniu. Nowe przepisy przewidują kilka sytuacji, w których pomimo wystąpienia naruszenia nie będziemy musieli dokonywać zawiadomienia osób, których dane dotyczą. Te sytuacje występują, jeśli:

- wdrożyliśmy środki techniczne i organizacyjne do danych naruszonych, np. dane są zaszyfrowane i pomimo tego, że trafiły w niepowołane ręce, niemożliwe jest ich odczytanie bez klucza, który posiadamy;
- zastosowaliśmy środki mające zapobiec naruszeniu, np. wyciek z naszej bazy trwał tylko 5 minut i polegał na tym, że dane były powszechnie widoczne na naszej stronie internetowej, a po tych kilku minutach zablokowaliśmy dostęp do tej strony;
- poinformowanie wymagałoby niewspółmiernie dużego wysiłku – wówczas wystarczy, jeśli poinformujemy o naruszeniu w sposób ogólny (np. na swojej stronie internetowej przy jej wyświetleniu, czy też przez wysłanie zbiorowej wiadomości).

Pamiętaj! Decyzja dotycząca informowania o naruszeniu w naszej organizacji będzie kontrolowana przez organ nadzorczy. Innymi słowy, jeśli stwierdzimy, że naruszenie nie może powodować wysokiego ryzyka dla osób, których dane dotyczą, to organ nadzorczy może mieć inne zdanie na ten temat. Jeśli organ nadzorczy będzie miał w tej kwestii inne zdanie, to wówczas może nakazać nam ich poinformowanie. Organ nadzorczy może też stwierdzić, że w naszej sytuacji występuje jeden z przypadków, który pozwala nam na nieinformowanie o naruszeniu osób, których dane dotyczą.

INSPEKTOR OCHRONY DANYCH

Nastał koniec ery ABI – czyli administratora bezpieczeństwa informacji. Na jego miejsce od 25 maja 2018 roku wejdzie Inspektor Ochrony Danych (w skrócie IOD).

Ważne! Związek Nauczycielstwa Polskiego jako administrator danych osobowych powołał IOD tak, aby objął on swoje obowiązki w dniu wejścia w życie RODO. Oddziały i okręgi nie powołują swoich IOD, robią to tylko filie OUPiS.

Obowiązek powołania IOD istnieje, gdy:

- przetwarzanie danych dokonywane jest przez organ publiczny;
- główna działalność to przetwarzanie, które wymaga regularnego i systematycznego monitorowania osób na dużą skalę (np. agencje ochrony);
- główna działalność to przetwarzanie danych wrażliwych na dużą skalę.

W pozostałych przypadkach administrator lub podmiot przetwarzający nie musi powoływać IOD. Istnieją jednak sytuacje, kiedy jest to rekomendowane.

Pamiętaj! IOD nie musi być powołany, kiedy nie wymaga tego przepis prawa, ale można wskazać osobę, która będzie pełniła jego obowiązki. Wówczas osoba ta nie musi pełnić wszystkich funkcji IOD, które są wymagane.

IOD może:

- być wyznaczony dla grupy podmiotów (czyli np. w sytuacji gdy przedsiębiorstwa są powiązane organizacyjnie);
- być wyznaczony na podstawie kwalifikacji zawodowych, ale szczególnie wiedzy fachowej, którą posiada, oraz umiejętności wypełniania swoich zadań w ramach ochrony danych osobowych;
- być zarówno pracownikiem personelu administratora, pracownikiem personelu podmiotu przetwarzającego, jak też może pełnić swoje funkcje na podstawie umowy.

Pamiętaj! IOD, z którym podpisuje się umowę, a który nie jest pracownikiem, będzie traktowany jako podmiot przetwarzający dane w czyimś imieniu. W takiej sytuacji należy zawrzeć stosowną umowę jak z podmiotem przetwarzającym, o której było już wcześniej wspomniane.

Należy opublikować dane kontaktowe do IOD oraz zawiadomić o nich organ nadzorczy. Opublikowanie jego numeru telefonu może niestety sprawić, że całe dnie będzie on spędzał na linii telefonicznej, udzielając podmiotom danych stosownych wyjaśnień. Dlatego jako dane kontaktowe IOD wystarczy wskazać adres jego poczty e-mail, za pomocą której będzie obsługiwał zapytania do niego skierowane. Takie wskazanie adresu e-mail nie będzie musiało zawierać nawet jego imienia i nazwiska, ale powinno wskazywać, że w organizacji pełni on funkcje IOD.

IOD pełni funkcję nadzorczą w ramach struktury, w której został powołany. Samo powołanie IOD nie wystarczy, aby realizować nowe przepisy dotyczące ochrony danych osobowych. Należy więc:

- uwzględniać IOD we wszystkich sprawach dotyczących ochrony danych;
- zapewnić mu zasoby niezbędne do wypełnienia jego obowiązków oraz zapewnić mu utrzymanie wiedzy fachowej (np. wysyłać go na stosowne szkolenia);
- nie dawać IOD instrukcji dotyczących wykonywania jego zadań;
- nie karać IOD za wykonywanie jego zadań ani nie odwoływać go za to;
- umożliwić osobom, których dane dotyczą, kontakt z IOD.

IOD ma obowiązek zachować w tajemnicy informacje związane z wykonywaniem jego zadań.

Pamiętaj! IOD może być członkiem personelu i wykonywać inne obowiązki, jeśli nie będą one powodowały konfliktu interesów. Na przykład administrator, czyli podmiot, który wyznacza cele i sposoby przetwarzania, nie może być IOD – doszłoby wówczas do sytuacji, w której sam kontrolowałby swoje własne działania.

Jeśli IOD musi być powołany, otrzymuje wówczas minimalną listę zadań, jakie musi zrealizować. Lista ta może być rozszerzana, ale nie może być ograniczana. Jeśli natomiast nie ma obowiązku powołania IOD, ale taka osoba jest wskazana, wówczas można obowiązki takiej osoby ustalić dowolnie.
Główne zadania IOD można podzielić na dwie grupy. Pierwsza grupa dotyczy jego działalności w ramach struktury administratora. Składają się na nią:

- informowanie o obowiązkach wynikających z RODO oraz innych przepisów, spoczywających na administratorze, podmiotach przetwarzających i pracownikach;

- monitorowanie przestrzegania przepisów rozporządzenia;
- przeprowadzanie szkoleń z ochrony danych osobowych w miejscu, gdzie IOD sprawuje swoje funkcje;
- udzielanie zaleceń co do oceny skutków dla ochrony danych osobowych.

Na drugą grupę składają się jego uprawnienia związane z działaniami podejmowanymi na zewnątrz:

- współpraca z organem nadzorczym;
- bycie osobą, z którą kontaktuje się organ nadzorczy.

UPRAWNIENIA ORGANU NADZORCZEGO

Przed przejściem do ważnego zagadnienia, jakimi są kary za niestosowanie się do przepisów o ochronie danych osobowych, należy wspomnieć także o uprawnieniach organu nadzorczego względem administratora czy też podmiotu przetwarzającego.

Organ nadzorczy może w ramach kontroli:

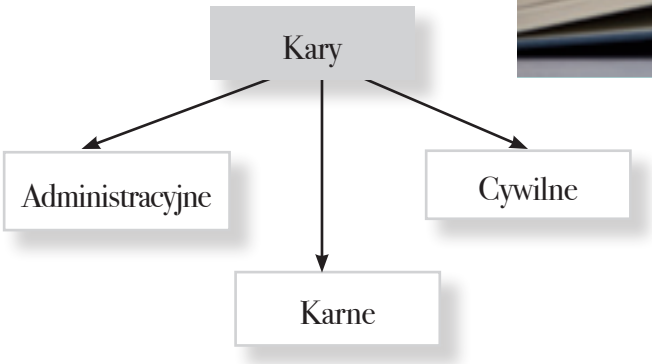
- żądać od administratora informacji, które są mu potrzebne do realizacji jego zadań;
- przeprowadzić audyt ochrony danych;
- dokonać przeglądu otrzymanych przez nas jako administratora certyfikacji;
- zawiadomić o podejrzeniu naruszenia RODO;
- uzyskać dostęp do posiadanych przez nas danych osobowych, aby mógł wypełniać swoje zadania;
- uzyskać dostęp do wszelkich pomieszczeń oraz wszelkich nośników informacji, na których przetwarzamy dane.

Organ nadzorczy ma także uprawnienia naprawcze, w ramach których może:

- wydać ostrzeżenie;
- udzielić upomnienia;
- nakazać spełnienie żądań podmiotów danych, które dochodzą realizacji swoich praw;
- kazać dostosować przetwarzanie, którego dokonujemy, do przepisów o ochronie danych;
- nakazać zawiadomić osoby, których dane dotyczą, o naruszeniu;
- ograniczyć możliwość przetwarzania danych, jak i zakazać przetwarzania;
- cofnąć certyfikację, którą otrzymaliśmy;
- zastosować administracyjną karę pieniężną.

KARY

Za nieprzestrzeganie przepisów dotyczących ochrony danych osobowych przewidziane są trzy rodzaje kar, które mogą być różne w zależności od tego, kto je nakłada. Można je podzielić w następujący sposób:



Kary cywilne grożą w sytuacji, w której jako administrator zostaniemy pozwani za naruszenie czyichś dóbr osobistych oraz przegramy w procesie. Wówczas czeka nas odpowiedzialność odszkodowawcza. Każdy sąd będzie zobligowany do poinformowania organu nadzorczego o toczącym się przeciwko nam postępowaniu cywilnym.

Sankcje karne będą z kolei groziły poszczególnym osobom, jeśli:

- nie umożliwią przeprowadzenia kontroli organowi nadzorczemu, narażając się tym samym na karę grzywny;
- przetwarzając dane osobowe bez podstawy prawnej, narażą się na karę grzywny, ograniczenie wolności lub pozbawienie wolności do roku;
- przetwarzając dane wrażliwe bez żadnej podstawy prawnej, narażą się na karę grzywny, ograniczenia wolności oraz karę pozbawienia wolności do lat dwóch.

Największe emocje wzbudzają sankcje administracyjne. Możliwości, które otrzymały organy nadzorcze, pozwalające na nakładanie im kar pieniężnych za nieprzestrzeganie przepisów dotyczących ochrony danych osobowych, sprawiają, że przestrzeganie przepisów o ochronie danych osobowych będzie traktowane poważnie.

Organ nadzorczy może nałożyć na administratora lub podmiot przetwarzający kary nawet do 20 000 000 euro lub 4% wartości jego obrotu liczonego za ubiegły rok obrotowy. Za mniejsze przewinienia (np. nie-

przestrzeganie obowiązku prowadzenia rejestru czynności przetwarzania) grożą kary administracyjne niższe – od wysokości 10 000 000 euro lub 2% wartości za ubiegły rok obrotowy przedsiębiorcy. Kary te nie będą nakładane na organy publiczne (np. organy administracji), a w przypadku podmiotów publicznych będą ograniczone do 100 000 złotych.

Ściągnięte kary będą stanowiły wpływ budżetu państwa.

ZAKOŃCZENIE

Przedstawione informacje mają charakter podstawowy, są wprowadzeniem w problematykę przepisów dotyczących ochrony danych osobowych oraz obowiązków, które czekają Związek Nauczycielstwa Polskiego z tego tytułu.

Wprowadzenie zmian może się wydać kłopotliwe, my jednak zachęcamy do tego, abyś spróbował w pierwszej kolejności zrozumieć ich sens i palącą potrzebę ich wprowadzenia.

Pamiętaj o tym, że najczęściej w życiu codziennym występujesz jako osoba, której dane są przetwarzane. Każdy krok, który czynisz, jest obecnie rejestrowany, dlatego też bezkrólewie w tym zakresie doprowadziło do poważnych nadużyć. Nowe przepisy stanowią szansę na to, że sytuacja ulegnie normalizacji.

Przetwarzając dane osobowe w sposób zgodny z przepisami dotyczącymi danych osobowych, gwarantujesz nie tylko bezpieczeństwo podmiotów, których dane przetwarzasz, ale także przyczyniasz się w znacznym stopniu do poprawy stanu prawnego, który wpłynie korzystnie także na nasze interesy.

Informator został opracowany przez Kancelarię Adwokacką Wachowski

adw. Marcin Jan Wachowski – członek Okręgowej Izby Adwokackiej w Warszawie z wieloletnim doświadczeniem w wykonywaniu usług prawnych dla przedsiębiorstw. Absolwent Uniwersytetu Szczecińskiego i Akademii Menadżerskiej Szkoły Głównej Handlowej w Warszawie, stypendysta Ośrodka Studiów Politycznych i Prawnych Hauss Rissen w Hamburgu. Ukończył aplikację sędziowską i orzekał jako referendarz sądowy w XII Wydziale Gospodarczym Sądu Rejonowego dla m.st. Warszawy. Stały mediator sądowy przy Sądzie Okręgowym w Warszawie. Od ponad 10 lat doradza klientom przede wszystkim w zakresie prawa TMT (technologii, mediów i telekomunikacji). Ostatnio pracuje przy wdrażaniu polityk ochrony danych osobowych zgodnych RODO w dużych i średnich organizacjach, członek zespołu eksperckiego ds. RODO przy Stowarzyszeniu Agencji Zatrudnienia, partner zarządzający w Kancelarii Adwokackiej Wachowski.

apl. radc. Piotr Druzgała – pracownik Kancelarii Adwokackiej Wachowski, zajmujący się zagadnieniami związanymi z prawem cywilnym oraz ochroną danych osobowych. Absolwent Uniwersytetu Jagiellońskiego na kierunku prawo oraz na kierunku administracja. Pracę dyplomową obronił w Katedrze Teorii Prawa Uniwersytetu Jagiellońskiego. Doświadczenia zawodowe gromadził, współpracując z krakowskimi kancelariami prawniczymi. Obecnie odbywa aplikację radcowską w Okręgowej Izbie Radców Prawnych w Warszawie. Jako prelegent brał udział w konferencjach dotyczących ochrony danych osobowych z uwzględnieniem ich przekazywania i ochrony w zatrudnieniu.

SPIS TREŚCI

Wstęp 3

Jakie zmiany? 5

Po co te wszystkie zmiany? 5

Co to oznacza? 5

Podstawowe definicje 6

Zasady przetwarzania 10

Przesłanki przetwarzania 12

Prawa osób, których dane dotyczą 17

Obowiązki administratora danych 23

Rejestr czynności przetwarzania 26

Postępowanie w sytuacjach naruszenia ochrony danych osobowych 27

Inspektor Ochrony Danych 30

Uprawnienia organu nadzorczego 32

Kary 33

Zakończenie 34


RODO
OGÓLNE ROZPORZĄDZENIE
O OCHRONIE DANYCH
OSOBOWYCH