RODO
we wspólnocie mieszkaniowej

experto24.pl

Spis treści

Wspólnota mieszkaniowej w ramach swojej działalności będzie często występować w charakterze administratora danych osobowych czy procesora. Często bowiem niezbędne jest przetwarzanie przez wspólnotę danych osobowych, w tym mieszkańców czy dostawców różnych usług. W artykule wskażemy wybrane, podstawowe i charakterystyczne dla wspólnot mieszkaniowych zagadnienia związane z tym przetwarzaniem.

Czym są dane osobowe

Dane osobowe to wszelkie dane, które odnoszą się do osób, w tym do członków zarządu wspólnoty mieszkaniowej, jej pracowników, właścicieli lokalu. Dane są danymi osobowymi gdy wskazują na konkretną osobę. Będzie to więc zasadniczo imię i nazwisko czy adres. Ale nie zawsze – jeżeli mamy dwóch właścicieli różnych lokali o tym samym imieniu i nazwisku, samo imię i nazwisko nie będzie daną osobową bo nie pozwala na wskazanie konkretnej osoby fizycznej. Do tego trzeba jeszcze jakiejś dodatkowej informacji, np. numeru budynku i lokalu.

Dane osobowe to więc informacje dotyczące wyłącznie osób fizycznych. Osoby prawne nie mają „własnych" danych osobowych przez co należy rozumieć, że daną osobową nie jest np. nazwa takiej osoby prawnej (np. Hotel-service sp. z o.o.).

Dane dzielimy na:

- zwykłe;
- „wrażliwe" czyli szczególne dane osobowe.

Do danych wrażliwych zaliczamy dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej. Wszystkie pozostałe dane osobowe, których nie zaliczymy do żadnej z tych kategorii, stanową dane zwykłe. Istnieją dwie podstawowe różnice pomiędzy tymi kategoriami danych:

- dane wrażliwe można przetwarzać w mniejszej ilości przypadków niż dane zwykłe – w przypadku wspólnoty mieszkaniowej przetwarzanie danych wrażliwych będzie miało miejsce zupełnie wyjątkowo;
- dane wrażliwe powinny być przez wspólnotę lepiej zabezpieczone niż dane zwykłe – np. szyfrowaniem, zamykaniem dokumentów papierowych w szafkach na klucz itd.

Kto jest administratorem danych osobowych

Zgodnie z RODO administrator danych osobowych to osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Oznacza to, że nie zawsze wspólnota mieszkaniowa będzie administratorem danych osobowych. Ustalenie kim jest ADO to pierwszy i podstawowy krok przy rozwiązywaniu większości problemów z przetwarzaniem danych.

Wspólnota mieszkaniowa będzie więc na przykład administratorem danych osobowych swoich mieszkańców (właścicieli lokali). Będzie administrowała danymi osób, które zatrudnia – np. ochroniarza czy sprzątaczki. Wreszcie o administrowaniu przez wspólnotę danymi możemy przykładowo mówić w przypadku zawarcia umowy na obsługę księgową i wskazania w tej umowie danych pracownika biura księgowego oddelegowanego do obsługiwania wspólnoty. W tych bowiem przypadkach wspólnota przetwarza dane we własnym celu – aby zapewnić obsługę nieruchomości w określonym zakresie (ochrona, sprzątanie itd.).

Owo przetwarzanie to w zasadzie każda czynność na danych osobowych, taka jak zbieranie danych, ich przechowywanie, usuwanie, opracowywanie czy udostępnianie. Nie ma przy tym znaczenia czy takie przetwarzanie odbywa się na komputerze, papierowo czy ustnie ani też czy ma miejsce w sposób zautomatyzowany lub niezautomatyzowany. Trudno wyobrazić sobie jakąkolwiek wspólnotę, która w swojej działalności nie przetwarzałaby danych osobowych a więc można założyć, że każda wspólnota mieszkaniowa w Polsce jest zobowiązana do stosowania RODO.

Wspólnota a zarządca

Tak więc administratorem danych członków wspólnoty mieszkaniowej jest wspólnota mieszkaniowa, gdyż zgodnie z art. 6 ustawy o własności lokali to wspólnota jest podmiotem praw i obowiązków wynikających z tejże ustawy. Właściciele lokali mogą natomiast w umowie o ustanowieniu odrębnej własności lokali albo w umowie zawartej później w formie aktu notarialnego określić sposób zarządu nieruchomością wspólną, a w szczególności mogą powierzyć zarząd osobie fizycznej albo prawnej (art. 18 ust. 1 ustawy o własności lokali). Zarządca wspólnoty mieszkaniowej może przetwarzać dane członków wspólnoty jak i dane innych osób, dla których wspólnota jest administratorem danych (np. dane osób sprzątających) tylko jako podmiot, któremu zostało powierzone przetwarzanie danych osobowych.

Przekazywanie danych osobowych innym podmiotom na dwa sposoby (1)

Administrator danych może bowiem albo sam przetwarzać dane, albo skorzystać z usług zewnętrznego podmiotu, który te dane będzie przetwarzał dla niego. Wspólnota może przekazywać dane osobowe podmiotów danych (np. swoich pracowników czy mieszkańców) innym podmiotom (np. usługodawcom czy kancelarii prawnej zajmującej się windykacją).

Może to czynić po pierwsze w ramach umowy powierzenia przetwarzania danych osobowych. Ta sytuacja będzie miała miejsce gdy procesor (podmiot przetwarzający) będzie przetwarzał dane w celach administratora danych (wspólnoty). Załóżmy na przykład, że wspólnota zamierza zawrzeć umowę z firmą dokonującą wymiany skrzynek pocztowych, podczas której konieczne będzie przetwarzane dane osobowe osób trzecich (mieszkańców wspólnoty), bowiem po zmianie skrzynek wykonawca musi przenieść też ich zawartość a tym samym zapoznać się z danymi adresowymi umieszczonymi na korespondencji. W takim przypadku konieczne będzie zawarcie z tą firmą umowy powierzenia na mocy której firma (procesor) będzie uprawniona do przetwarzania danych tych osób ale tylko w celu wykonywania tej umowy. Procesor nie decyduje więc o celach i ani o środkach przetwarzania danych lecz działa na podstawie umowy z administratorem danych. Jest on podmiotem przetwarzającym dane osobowe w imieniu administratora.

Drugim trybem przekazania danych przez wspólnotę podmiotowi trzeciemu będzie udostępnienie danych osobowych. Dane osób trzecich mogą zostać przekazane tym podmiotom (np. Zakładowi Ubezpieczeń Społecznych, urzędowi skarbowemu czy Policji) jeżeli organy te będą uprawnione do żądania tych danych na podstawie przepisów prawa (np. Ordynacji podatkowej w związku z toczącym się postępowaniem czy Kodeksu postępowania karnego). Wówczas nie jest konieczne zawieranie umowy powierzenia przetwarzania danych osobowych.

Zgoda

Zgoda jest jedną z podstaw dopuszczalności przetwarzania danych osobowych przez administratora. Według RODO przetwarzanie danych osobowych jest zgodne z prawem m. in. jeśli osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów.

Większość danych osobowych wspólnota mieszkaniowa będzie jednak mogła przetwarzać bez takiej zgody właściciela lokalu. Najczęstszą podstawą przetwarzania danych osobowych takiego podmiotu danych będzie bowiem jakiś konkretny obowiązek prawny z ustawy o własności lokali.

Obowiązek informacyjny

Konieczne jest także informowanie (zasadniczo już na etapie pozyskiwania danych osobowych) o konkretnych danych administratora, który te dane pozyskuje (np. przy pobieraniu zgody na ich przetwarzanie). Zakres informacji, które powinny być podawane osobie, od której wspólnota bezpośrednio pozyskuje dane określa art. 13 RODO. Część z informacji wspólnota powinna przekazywać podmiotowi danych zawsze i niezależnie od okoliczności związanych z przetwarzaniem danych. Niektóre zaś z informacji administrator danych musi przekazać osobie, której dane dotyczą z uwagi na podstawę prawną przetwarzania danych czy zasady przetwarzania.

Prawo wycofania zgody

Przed uzyskaniem zgody osoba, której dane dotyczą musi być też poinformowana przez wspólnotę o możliwości jej wycofania w dowolnym momencie, a administrator powinien być w stanie wykazać, że ten obowiązek uprzedniego powiadomienia spełnił. Zgodnie bowiem z art. 7 ust. 3 RODO osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę i powinna zostać o tym poinformowana, zanim wyrazi zgodę. Wycofanie zgody musi być przy tym równie łatwe jak jej wyrażenie co przede wszystkim oznacza dopuszczalność cofnięcia zgody w tej samej formie w jakiej zgoda została udzielona (np. ustnie, e-mailowo).

Wycofanie zgody nie działa wstecz

RODO przyznaje prawo podmiotowi danych (tj. osobie, której dane dotyczą) do wycofania zgody w dowolnym momencie. W takim przypadku:

- wycofanie zgody nie ma wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem;
- podmiot danych przed wyrażeniem zgody na przetwarzanie danych osobowych musi być o tym braku wpływ poinformowany;
- wycofanie zgody musi być równie łatwe jak jej wyrażenie.

Dla funkcjonowania wspólnoty ma to takie znaczenie, że nie można domagać się od danej osoby, po wycofaniu przez nią sprzeciwu, przywrócenia stanu sprzed przetwarzania jej danych.

Przekazywanie danych dzieci

W toku działania wspólnot problem sprawa też często kwestia przekazywania przez interesantów danych osobowych ich dzieci. Czy na przykład mąż albo żona musi wyrazić zgodę na przetwarzanie danych dziecka przekazywanych do wspólnoty przez drugiego małżonka? Zasadniczo nie.

Wystarczy jeżeli ten małżonek sam złoży wniosek czy inne pismo, przekazując dane osobowe dziecka. Zgoda drugiego z rodziców nie jest wymagana na przetwarzanie danych osobowych dziecka chyba, że jest to usługa społeczeństwa informacyjnego z art. 8 RODO albo dochodzi do przetwarzania danych dziecka w celu marketingowym, w celu utworzenia jego profilu osobowego czy też skierowania bezpośrednio do tego dziecka usługi. Jeżeli jednak podstawą przetwarzania danych osobowych jest wyłącznie art. 6 ust. 1 lit. c RODO, tj. obowiązek prawny, nie ma konieczności uzyskiwania zgody drugiego małżonka.

Powiadamianie Prezesa Urzędu Ochrony Danych Osobowych o naruszeniach

Wspólnota mieszkaniowa (albo w razie jego powołania - inspektor ochrony danych zatrudniony przez tą wspólnotę) musi dokonać zgłoszenia wszelkich przypadków naruszenia ochrony danych osobowych Prezesowi UODO w miarę możliwości bez zbędnej zwłoki, jednak nie później niż w terminie 72 godzin od stwierdzenia naruszenia. W razie zgłoszenia incydentu po upływie tych 72 godzin administrator (inspektor ochrony danych) jest zobowiązany wyjaśnić przyczyny opóźnienia. Jedyny wyjątek od tego obowiązku zachodzi, gdy mało prawdopodobne jest aby naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Prowadzenie dokumentacji

Każdy administrator danych osobowych, w tym wspólnota mieszkaniowa, powinna prowadzić dokumentację ochrony danych osobowych, w tym przede wszystkim dokumentację odpowiednich zabezpieczeń. Dokumentacja danych osobowych według RODO może mieć bardzo różny kształt i tytuły. Wszystko zależy od tego jakie dane, w jakiej formie, na jakiej podstawie i w jakim zakresie wspólnota przetwarza. W szczególności dokumentacja ochrony danych powinna opisywać środki zabezpieczające przetwarzanie danych wdrożone przez daną jednostkę.

Wspólnota powinna samodzielnie ocenić czy i jakie środki należy podjąć i jak je opisać w dokumentacji RODO. Inne dokumenty – poza dotyczącymi środków zabezpieczających – jakie powinny zostać wdrożone to:

- rejestr czynności przetwarzania;
- zakres rejestru kategorii czynności przetwarzania;
- rejestr naruszeń ochrony danych;
- raport dokumentujący wyniki przeprowadzonych ocen skutków dla oceny danych.

Nie ma więc obecnie obowiązku prowadzenie m.in. polityki bezpieczeństwa danych osobowych czy instrukcji zarządzania systemem informatycznym, w którym przetwarzane są dane osobowe. Obecnie tak naprawdę jedynym obligatoryjnym dokumentem jakim ma posiadać administrator danych osobowych jest prowadzenie rejestru czynności przetwarzania danych osobowych. Jeszcze raz podkreślmy, że nie oznacza to jednak, że wspólnota może wprowadzić rejestr czynności przetwarzania i uważać, że prawidłowo prowadzi dokumentację ochrony danych osobowych. Powinna za to przeanalizować czy i jakie jeszcze dokumenty potrzebuje ona aby zapewnić bezpieczeństwo, poufność czy integralność tych danych w toku swojej działalności.

RODO nie stoi na przeszkodzie prawu do wglądu w dokumenty wspólnoty

Zgodnie z art. 29 ust. 3 ustawy z dnia 24 czerwca 1994 roku o własności lokali prawo kontroli działalności zarządu służy każdemu właścicielowi lokalu. Często jednak właściciele spotykają się z odmową udostępnienia określonych dokumentów. Zarząd lub zarządca zasłania się znaną skądinąd wymówką „bo RODO". Najczęściej jednak przepisy rozporządzenia ogólnego o ochronie danych osobowych nie stoją na przeszkodzie udostępnieniu właścicielowi dokumentacji, w tym zawierającej dane osobowe innych właścicieli lokali.

Z zasady minimalizacji wynika, że wspólnota mieszkaniowa może przetwarzać dane osobowe tylko w konkretnych, wyraźnych i prawnie usprawiedliwionych celach. Na przykład wynika z tego, że zarząd lub zarządca wspólnoty powinien mieć w swojej dyspozycji tylko te dokumenty, które są niezbędne do zarządzania nieruchomością wspólną. Zasadniczo więc nie powinien on posiadać aktów notarialnych (np. umów sprzedaży lokali) odnoszących się wyłącznie do konkretnych lokali.

Wspólnota mieszkaniowa jako administrator danych osobowych ma obowiązek ich należytego zabezpieczenia i nieudostępniania osobom nieuprawnionym. Nie oznacza to jednak – jak często

podnoszą zarządcy lub zarządy wspólnoty – całkowitego zakazu udostępniania do wglądu dokumentów zawierających danych osobowe. Takie postępowanie jest absurdalne i oznacza, że dany zarząd lub zarządca nie potrafi prawidłowo zinterpretować dwóch aktów prawnych (RODO i ustawy o własności lokali) dostrzegając rzekomą sprzeczność między nimi. Tymczasem takiej sprzeczności nie ma bowiem art. 29 ust. 3 ustawy o własności lokali pozwala w połączeniu z art. 6 ust. 1 lit. c RODO na udostępnienie danych właścicielowi lokalu. Zgodnie bowiem z tym przepisem RODO przetwarzanie jest zgodne z prawem gdy jest ono niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Taki obowiązek statuuje właśnie art. 29 ust. 3 ustawy o własności lokali.

Gdyby uznać pogląd przeciwny za prawdziwy to art. 29 ust. 3 ustawy o własności pozostawałby martwy a kontrola nie byłaby w ogóle możliwa – co zapewne byłoby na rękę niektórym zarządcom i zarządom podnoszącym argument „bo RODO".

Naturalnie właściciele lokali mogą także żądać kopii interesujących ich dokumentów, robić im zdjęcia czy sporządzać notatki odręczne. Decyzja o wyborze formy wglądu należy do właściciela lokalu.

Zabezpieczenie danych osobowych

To czy i jakie środki zabezpieczające przetwarzanie danych powinien wdrożyć administrator danych (wspólnota), reguluje art. 24 RODO. Zgodnie z tym przepisem „uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane".

Oznacza to, że wspólnota jako administrator danych osobowych – podobnie jak przy dokumentacji ochrony danych osobowych – samodzielnie bada co jest konieczne do tego aby dane nie wyciekły na zewnątrz. Wynika to z, wynikającego z RODO, generalnego dążenia do zwiększenia samodzielności administratora w decydowaniu o konkretnych środkach przedsiębranych przez administratora. Pozwala to uelastycznić ochronę danych i dostosować ją do potrzeb konkretnego podmiotu, który te dane przetwarza. Jest to podejście oparte na ryzyku.

Załóżmy na przykład, że wspólnota ma potrzebę przetwarzania danych osobowych poza swoją siedzibą – np. na prywatnym laptopie pracownika. W takiej sytuacji należy dostosować wewnętrzną dokumentację administratora. Chodzi tu przede wszystkim o określenie miejsc przetwarzania danych osobowych czy też dopuszczenie przetwarzania danych osobowych na urządzeniach mobilnych, w tym urządzeniach prywatnych pracowników administratora danych. Dopuszczenie do korzystania z takich urządzeń musi być połączone z określeniem warunków technicznych jakim te urządzenia powinny

odpowiadać. Należy rozważyć wprowadzenie szyfrowania przesyłanych danych lub przedsięwzięcia innych, adekwatnych zabezpieczeń. Można dopuścić okresowy audyt urządzeń prywatnych. Warto rozważyć zakaz zapisywania danych logowania na urządzeniach prywatnych (tak aby pracownik za każdym razem musiał te dane wpisywać „z pamięci").

Decydując się na konkretne rozwiązania wspólnota powinna wziąć pod uwagę:

- charakter, zakres i cel przetwarzania danych posiadanych przez wspólnotę;
- stopień ryzyka naruszenia praw lub wolności osób fizycznych (podmiotów danych);
- stan aktualnej wiedzy technicznej;
- koszt wdrożenia określonych sposobów zabezpieczania danych osobowych.

Inspektor ochrony danych

W przypadku wspólnot mieszkaniowych na ogół ustanowienie inspektora nie jest obowiązkowe. IOD musi być powołany gdy główne zadanie wspólnoty polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę oraz gdy główna działalność polega na przetwarzaniu na dużą skalę danych osobowych. Zatem powołać IOD muszą zasadniczo tylko największe wspólnoty mieszkaniowe; przy czym nie ma tu określonej konkretnego rozgraniczenia. Inspektor może być albo pracownikiem albo osobą współpracującą z zarządcą np. na podstawie umowy o świadczenie usług.

Powołanie inspektora ochrony danych nie zdejmuje z zarządu wspólnoty obowiązku podejmowania decyzji w sprawach ochrony danych. IOD zasadniczo ma rolę opiniującą oraz sprawuje bieżący nadzór nad ochroną danych osobowych w konkretnym podmiocie. Natomiast to zarząd wspólnoty ma moc zmieniania dokumentacji wewnętrznej administratora danych, wyciągania konsekwencji od pracowników czy stosowania takich czy innych zabezpieczeń danych osobowych.

Skuteczne wdrożenie RODO

Jeżeli dana wspólnota mieszkaniowa ciągle ma niezałatwione kwestie związane z ochroną danych osobowych albo też nie dostosowała swojego modelu ochrony danych do przepisów RODO obowiązujący od 25 maja 2018 roku, konieczne jest wdrożenie RODO. Oznacza to przedsiębranie następujących kroków:

- zorganizowanie wewnętrznego audytu przetwarzanych danych osobowych – taki audyt może być przeprowadzony siłami pracowników wspólnoty lub przez wyspecjalizowaną firmę zewnętrzną i powinien zawierać analizę ryzyka;
- przygotowanie dokumentów (w tym w szczególności regulacji, opisów procedur, rejestrów czynności, wzorów np. umowy powierzenia przetwarzania) oraz ich wdrożenie (rozpoczęcie praktycznego stosowania) – niekiedy zleca się to także audytorowi;
- przeszkolenie pracowników – zarówno z teoretycznej znajomości przepisów oraz aktów wewnętrznych jak i ich praktycznej realizacji.

W toku samej działalności wspólnoty absolutne minimum na jakie trzeba zwrócić uwagę, a które pokrywa większość problematycznych sytuacji to:

- pilnowanie posiadania przez wspólnotę podstawy prawnej do przetwarzania konkretnych danych osobowych;
- wykonywanie obowiązku informacyjnego;
- stosowanie zasady minimalizacji przetwarzanych danych – zbieranie tylko tych danych, które są niezbędne do wykonywania przez wspólnotę swoich funkcji;
- zawieranie umów powierzenia przetwarzania danych osobowych;
- ograniczenie dostępu do danych osobowych tylko dla tych pracowników, którzy do tych danych musza mieć dostęp.

Kolejne obowiązki, o których trzeba wspomnieć to:

- zapewnienie, aby przetwarzanie danych było zgodne z prawem i zasadami przetwarzania danych osobowych m. in. w zakresie uwzględniania ochrony danych w fazie projektowania (privacy by design) oraz domyślnej ochrony danych (privacy by default);
- analizowanie skutków podejmowanych operacji przetwarzania danych osobowych dla ochrony danych osobowych (tzw. DPIA) oraz przeprowadzenie uprzednich konsultacji z organem nadzorczym w przypadkach wskazanych w RODO;
- powołania inspektora ochrony danych (IOD) w przypadkach wskazanych w RODO;
- przestrzeganie praw osób, których dane dotyczą, oraz ułatwiania realizacji tych praw;
- zgłaszanie naruszeń ochrony danych organowi nadzorczemu;
- zawiadamianie osób, których dane dotyczą o naruszeniu ochrony danych osobowych.

Pamiętajmy też, że naruszenie wymogów RODO grozi odpowiedzialnością finansową i administracyjną.

Autor

Marcin Sarna

radca prawny

Stopka redakcyjna

Redaktor:	Anna Śmigulska- Wojciechowska
ISBN:	978-83-269-9037-3
E-book nr:	2HH1011
Firma:	Wiedza i Praktyka sp. z o.o.
Adres:	03-918 Warszawa, ul. Łotewska 9a
Kontakt:	Telefon 22 518 29 29, faks 22 617 60 10, e-mail: *cok@wip.pl*
NIP:	526-19-92-256
Numer KRS:	0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego: 200.000 zł, Nr rejestrowy BDO: 000008579