

RODO dla sołtysa

Patryk Łuczyński



Przetwarzanie danych osobowych przez jednostki pomocnicze gminy, a do takich należy sołectwo i jego organy (sołtys, zebranie wiejskie), jest zagadnieniem skomplikowanym i wielowątkowym. Budzi też ono wątpliwości w doktrynie, które dotyczą przede wszystkim kwalifikacji sołtysa (sołectwa) jako administratora, podmiotu przetwarzającego lub osoby działającej z upoważnieni administratora.

Poradnik
Witryny Wiejskiej



SOŁECTWO
NA
NOWE
CZASY

Celem poniższego artykułu jest przybliżenie zagadnienia ochrony danych osobowych w ramach sołectw, a także skonfrontowanie się z bieżącymi problemami, z którymi mierzą się sołtysi w obszarze ochrony danych osobowych.

Kto jest kim, czyli kilka słów o sołectwie

Sołectwo jest jednostką pomocniczą gminy, która stanowi pewnego rodzaju ogniwo pośrednie pomiędzy mieszkańcami gminy i jej organami. Ustanawiane jest ono przez radę gminy, po przeprowadzeniu konsultacji społecznych, w trybie uchwały. W tej formie nadawany jest też statut sołectwa, który określa jego podstawowe zadania.

W ramach sołectwa funkcjonują dwa zasadnicze organy, tj. zebranie wiejskie, które ma funkcję uchwałodawczą, a także sołtys pełniący funkcje wykonawcze w stosunku do uchwał zebrania wiejskiego, a także reprezentacyjną wobec sołectwa. Odpowiada on też za realizowanie zadań przyznanych mu na gruncie statutu lub wynikających z innych poleceń. W praktyce realizuje on również inne czynności na rzecz lokalnej społeczności. Wsparciem sołtysa w wykonywaniu zadań zajmuje się rada sołectwa, która ma funkcje opiniująco-doradczą.

Czy sołtys przetwarza dane osobowe?

Aby odpowiedzieć na wskazane pytanie, należy w pierwszej kolejności wyjaśnić pojęcie danych osobowych. Te zostały bowiem zdefiniowane w art. 4 pkt. 1 RODO jako wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Dla uznania informacji za dane osobowe nie ma znaczenia, w jakim wieku jest osoba, której te informacje dotyczą, w jakim kraju się znajduje, czy jest powszechnie znana, pełni funkcję publiczną, ani to czy jest przedsiębiorcą.

Ważne! Dane osobowe służą każdemu człowiekowi od momentu urodzenia do chwili śmierci.

Ważne! Fakt, że pewne informacje są powszechnie dostępne (np. na stronach internetowych), nie wyłącza ich spod pojęcia danych osobowych.

Z powyższej definicji należy też wyprowadzić wniosek, że żadna informacja dotycząca człowieka nie może być z góry wykluczona jako dane osobowe, jak również nie można założyć, że jakaś informacja zawsze będzie stanowiła dane osobowe. Każdorazowo ocena informacji powinna uwzględniać możliwość zidentyfikowania na jej podstawie konkretnego człowieka. Dopiero wówczas możemy mówić o tym, że mamy do czynienia z danymi osobowymi.

Takimi danymi osobowymi mogą być przy tym nie tylko standardowe identyfikatory osoby fizycznej, jak jej imię i nazwisko, numer PESEL, czy numer dowodu osobistego, ale też np. dane lokalizacyjne (adres, dane z GPS), dane kontaktowe (numer telefonu, adres e-mail, adres ePUAP), dane finansowe lub majątkowe (informacja o zarobkach, informacja o majątku), ale też mniej oczywiste informacje, jak chociażby ubiór konkretnej osoby, czy jej specyficzne cechy, jeżeli w danej sytuacji pozwolą nam one na wyróżnienie tej osoby.

Ważne! Ta sama informacja, która dla jednego podmiotu (np. wójta gminy) stanowi dane osobowe, może nie stanowić takich danych dla innego podmiotu (np. sołtysa). Trzeba każdorazowo uwzględnić kontekst sytuacji i to czy zakres posiadanych danych, w tym możliwość zgodnego z prawem uzyskania dodatkowych informacji, daje administratorowi możliwość dokonania identyfikacji człowieka.

Ważne! Przy ocenie możliwości identyfikacji uwzględnia się m.in. koszt i czas potrzebne do identyfikacji człowieka, a także dostępną technologię i postęp technologiczny.

Przykład: numer identyfikacji podatkowej (NIP), który składa się z ciągu 10 cyfr, należy uznać za dane osobowe (o ile przypisany jest on do osoby fizycznej, w tym tzw. jednoosobowego przedsiębiorcy). Identyfikacja człowieka na podstawie takiego numeru jest bowiem bardzo prosta dzięki publicznym, internetowym rejstrum.

Przykład: stały adres IP co do zasady uznawany jest za dane osobowe. Jeżeli jednak sołtys uzyska taki adres IP bez dodatkowych informacji, np. informacji kontekstowych, które pozwoliłyby mu powiązać ten adres z konkretną osobą, to nie będzie on stanowił dla niego danych osobowych. Jednocześnie jednak ten sam adres IP będzie danymi osobowymi np. dla operatora telekomunikacyjnego.

Warto zwrócić uwagę, że ocena czy określone informacje stanowią dane osobowe, często nie jest oczywista i wymaga uwzględnienia okoliczności konkretnego przypadku. W tym zakresie warto wskazać na rozbieżności w orzecznictwie co do kwalifikowania jako danych osobowych numeru

telefonu komórkowego – WSA w Warszawie w wyroku z 23.03.2023 r. II SA/Wa 2219/22 uznał numer telefonu za dane osobowe, wskazując że pozwala on na łatwe oznaczenie osoby fizycznej w sposób, który pozwala wywierać na nią określony wpływ. Jednocześnie jednak ten sam sąd w wyroku z 13.02.2024 r. II Sa/Wa 1122/23 stanął na odmiennym stanowisku, uznając że numer telefonu nie pozwala na prostą identyfikację człowieka.

Ważne! Niezależnie od doktrynalnych i orzeczniczych rozważań na temat kwalifikacji numeru telefonu jako danych osobowych, jeżeli w zasobach sołtysa numer ten służy do kontaktu z mieszkańcem, niewątpliwie będzie on wchodził w zakres danych osobowych.

Pozostając w obszarze definicji danych osobowych, warto jeszcze zwrócić uwagę, że na gruncie art. 6 i art. 9 RODO, wyróżniamy tzw. dane osobowe zwykłe i dane osobowe szczególnych kategorii.

Pierwsza z tych kategorii obejmuje informacje, które wykorzystujemy w codziennym obrocie – np. imię i nazwisko, PESEL, adres zamieszkania, numer telefonu, adres e-mail, numer rachunku bankowego. Natomiast druga z ww. kategorii obejmuje dane, które zasługują na wzmożoną ochronę i zostały enumeratywnie wskazane w art. 9 ust. 1, a w ich skład wchodzi m.in. informacje dotyczące stanu zdrowia, poglądów politycznych, orientacji seksualnej czy seksualności, dane genetyczne oraz dane biometryczne wykorzystywane do jednoznacznej identyfikacji.

W świetle ww. definicji nie powinno budzić wątpliwości, że sołectwa – a konkretniej ich organy, czyli sołtys i zebranie wiejskie przetwarzają dane osobowe. Wśród tych danych znajdować będą się przede wszystkim dane mieszkańców, ale też dane urzędników gminy, czy innych osób, z którymi sołtys jako reprezentant sołectwa utrzymuje kontakt w związku z wykonywanymi zadaniami.

Status sołectwa/sołtysa na gruncie RODO

Skoro wiemy, że w ramach sołectwa dochodzi do przetwarzania danych osobowych, należy podjąć się próby oceny, jaka jest rola organów sołectwa w procesie przetwarzania tych danych. Skupię się w tym zakresie przede wszystkim na sołtysie, którego zadania są najszersze, a przez to przetwarzać on będzie najwięcej danych, występując w różnorodnych rolach.

W pewnym skrócie można wskazać, że RODO wyróżnia trzy rodzaje podmiotów, które przetwarzają dane osobowe.

Pierwszym z nich jest administrator – podmiot wiodący, który ustala cele i sposoby przetwarzania danych, czyli inaczej mówiąc, określa po co dane będą przetwarzane, w jakim zakresie i jakimi metodami.

Drugim z podmiotów jest procesor – podmiot przetwarzający, czyli osoba/organ, który dokonuje przetwarzania danych osobowych, ale na zlecenie (w imieniu) innego podmiotu (administratora) oraz w zakresie wyznaczonych przez niego celów i sposobów. Taki procesor nie ustala samodzielnie po co będzie przetwarzał dane, lecz wykonuje polecenia administratora.

Trzecim z podmiotów jest osoba, która działa z upoważnienia administratora (lub podmiotu przetwarzającego). Takimi podmiotami są przede wszystkim pracownicy administratora oraz jego zleceniobiorcy. W pewnych sytuacjach mogą to być też jednak inne podmioty, np. sołtys, który chociaż formalnie nie jest pracownikiem gminy, to wykonywać będzie zadania w ramach quasi-zatrudnienia, działając w ramach poleceń organu gminy i w sposób przez taki organ ustalony.

Praktyka pokazuje, że sołtysi występują w każdej z ww. ról w zależności od rodzaju realizowanych zadań, co zostanie omówione poniżej wraz z informacją o obowiązkach, które w związku z konkretnym statutem ciążyą na sołtysie.

Sołtys jako administrator danych

Administrator, jak już wskazałem, ustala cele i sposoby przetwarzania danych. Niewątpliwie sołtys realizując zadania, które nie są mu bezpośrednio zlecone przez organy gminne, może samodzielnie decydować o przetwarzaniu danych, uzyskując status administratora.

Z taką sytuacją, w której sołtys (sołectwo) będzie występowało w roli administratora, mamy do czynienia, np. przy realizacji zadań związanych z funduszem sołeckim, w tym rozpatrywaniem wniosków mieszkańców o zawnioskowanie przez sołectwo o środki z funduszu. Tryb postępowania w ww. sytuacji określa ustawa z 21.02.2014 r. o funduszu sołeckim. Przewiduje ona możliwość złożenia przez grupę co najmniej 15 pełnoletnich mieszkańców sołectwa inicjatywy w zakresie wniosku o przyznanie sołectwu środków z funduszu, który to wniosek uchwała zebranie wiejskie. W ramach takiej „inicjatywy” mieszkańcy będą co do zasady ujawniać swoje dane. Skoro celem ich przetwarzania będzie wykonanie zadania przez sołectwo (zebranie wiejskie), to w mojej ocenie będzie ono ich administratorem.

Kolejnym obszarem, w którym sołtys będzie pełnił funkcję administratora danych, jest reprezentowanie przez niego mieszkańców w kontaktach z władzami gminnymi. W tym celu sołtys może prowadzić korespondencję z mieszkańcami, może organizować spotkania, posiedzenia, pozyskiwać

określone informacje, które będą niezbędne do pełnienia jego funkcji.

Warto zwrócić uwagę, że sołtys jako lider lokalnej społeczności może podejmować też inne działania zmierzające do solidaryzowania się mieszkańców, a także organizowania dla nich różnego rodzaju wydarzeń i przestrzeni do wspólnego działania. W takim przypadku będzie on prowadził działalność we własnym imieniu, a zatem pozyskując dane mieszkańców, będzie w stosunku do nich administratorem. Przykładem takich działań może być organizacja wycieczki i prowadzenie w tym celu zapisów, organizacja wydarzeń kulturalnych, czy nawet różnego rodzaju konkursów.

Status administratora danych sołtys może też uzyskać, jeżeli prowadzi on samodzielnie stronę internetową lub profil w mediach społecznościowych. W takim przypadku to on ustala cele i sposoby przetwarzania danych, które mogą być ujawniane w publikowanych postach lub na publikowanych zdjęciach. Analogicznie, jeżeli sołtys postanowi, np. o zamontowaniu i uruchomieniu monitoringu wizyjnego na obszarze obiektu znajdującego się w sołectwie, np. świetlicy wiejskiej, będzie on odpowiedzialny za prawidłowe przetwarzanie danych jako ich administrator.

Sołtys jako podmiot przetwarzający

Mogą jednak zdarzyć się sytuacje, w których sołtys nie będzie samodzielnie ustalał celu i sposobu przetwarzania danych, lecz będzie pełnił jedynie funkcję wykonawczą wobec celów ustalonych przez inny podmiot. Tym innym podmiotem będą zazwyczaj organy gminy.

Aby uznać sołtysa za podmiot przetwarzający, pomiędzy nim a administratorem musi zaistnieć relacja, w której administrator ustalił cele i sposoby przetwarzania, a następnie zlecił określone czynności przetwarzania do wykonywania w swoim imieniu sołtysowi. Przykładem niech będzie monitoring wizyjny. Jeżeli gmina postanowi, że sołtys będzie obsługiwał monitoring wizyjny zainstalowany przez nią na terenie sołectwa, to na gruncie przepisów RODO będzie on wykonywał zadania podmiotu przetwarzającego. W takiej sytuacji może on dokonywać na danych osobowych (nagraniach) jedynie takich czynności, na które pozwoli mu gmina. Nie może on przetwarzać takich danych na swoje własne potrzeby.

Co istotne, sołtys, który występuje w roli podmiotu przetwarzającego jest związany poleceniami administratora, a ponadto może zostać przez niego skontrolowany.

Sołtys jako osoba upoważniona do przetwarzania danych

Praktyka pokazuje, że organy gminy często przenoszą wykonywanie pewnych swoich obowiązków na sołtysów, co przede wszystkim ma ułatwić ich wykonanie dzięki temu, że sołtys jest bliżej mieszkańców. Do takich obowiązków należy np. pełnienie funkcji inkasenta należności podatkowych, dla których organem podatkowym jest wójt, czy też dokonywanie doręczeń w postępowaniu podatkowym.

W sytuacji, gdy sołtysowi zlecone jest dokonanie określonych czynności przynależnych do organu gminy, np. wskazanego wyżej inkasowania należności czy doręczania korespondencji, przyjmuje się, że nie pełni on roli podmiotu przetwarzającego, zaś jego status zbliżony jest bardziej do pracownika gminy. Stanowisko takie nie jest w pełni akceptowane w doktrynie, jednak zostało zaaprobowane przez organ nadzorczy – Prezesa Urzędu Ochrony Danych Osobowych.

We wskazanych sytuacjach organ gminy, w imieniu którego działa wójt, powinien nadać mu stosowne upoważnienie do przetwarzania danych osobowych. W takim przypadku sołtys działa poniekąd w ramach wewnętrznej struktury takiego organu, będąc zobowiązanym do stosowania jego procedur dotyczących ochrony danych osobowych oraz wdrożonych w takim organie środków bezpieczeństwa.

Jakie są obowiązki sołtysa będącego administratorem danych?

Status administratora danych nakłada na sołtysa najwięcej obowiązków – niektóre z nich omówię poniżej.

Przed wszystkim sołtys – administrator pozostaje w pełni odpowiedzialny za prawidłowość przetwarzania przez siebie danych osobowych, w tym za przestrzeganie zasad ogólnych wynikających z art. 5 RODO. Spośród nich warto wyróżnić zasady:

1. **zgodności z prawem i przejrzystości** – która wymaga, aby sołtys przetwarzał dane tylko wówczas, gdy istnieje ku temu podstawa przetwarzania określona w art. 6 ust. 1 RODO, a ponadto, aby osoby, których dane przetwarza były o tym poinformowane,
2. **ograniczenia celu** – która zakłada, że dane osobowe mogą być przetwarzane przez sołtysa (administratora) tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach. Aby zatem sołtys mógł przetwarzać dane, powinien najpierw ustalić cel takiego przetwarzania (czyli po co mu te dane). Cel ten nie może być sprzeczny z prawem i nie może mieć ogólnego charakteru,
3. **minimalizacji danych** – wymagającą, aby dane osobowe przetwarzane przez administratora (sołtysa) były adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów przetwarzania. Sołtysowi nie wolno zatem pozyskiwać danych, które są nadmiarowe wobec celu.

Przykład: sołtys organizuje dla mieszkańców sołectwa konkurs na najlepszy plakat. Nagrodą w konkursie są upominki z logo sołectwa, kalendarz ścienny i opakowanie lokalnych przysmaków. W formularzu zgłoszeniowym sołtys zawarł rubryki na podanie przez uczestnika konkursu: imienia i nazwiska, adresu zamieszkania oraz numeru PESEL i numeru dowodu osobistego. Realizacja ww. celu przetwarzania, którym jest organizacja i rozstrzygnięcie konkursu, nie wymaga jednak przetwarzania tak szerokiego zakresu danych. Błędne jest zatem zawarcie w formularzu miejsca na PESEL i numer dowodu osobistego.

Z realizacją ww. zasad silnie wiąże się ustalenie przez sołtysa właściwej podstawy legalizującej przetwarzanie przez niego danych osobowych. Podstawa ta będzie wynikała z celu przetwarzania. W zakresie danych osobowych, które sołtys przetwarza w związku z realizacją swoich ustawowych lub statutowych zadań, podstawą taką będzie art. 6 ust. 1 lit. e RODO (realizacja zadania w interesie publicznym) lub art. 6 ust. 1 lit. c RODO (realizacja obowiązku prawnego).

W przypadku, gdy sołtys działa poza zakresem tych zadań, np. organizując konkurs lub wycieczkę dla mieszkańców, w grę wchodzi też inne podstawy przetwarzania, np. art. 6 ust. 1 lit. b RODO, czyli niezbędność do wykonania umowy (niezależnie czy jest to umowa odpłatna, czy nieodpłatna, np. w zakresie udziału w wycieczce) lub art. 6 ust. 1 lit. a RODO, czyli zgoda osoby, której dane dotyczą (przykładowo – gdy sołtys chce stworzyć sobie bazę kontaktową do mieszkańców).

Kolejnym ważnym zadaniem, które stoi przed administratorem danych osobowych jest ich odpowiednie zabezpieczenie. Sołtys jako administrator ma bowiem zapewnić, że zachowana zostanie poufność, dostępność i integralność danych, a zatem, że nie zostaną one ujawnione nieuprawnionym osobom, utracone albo zmienione w sposób nieuprawniony.

Aby to zrobić sołtys powinien przede wszystkim ustalić jakie zagrożenia dla danych (osoby, której dane dotyczą) mogą wystąpić w związku z przetwarzaniem przez niego takich informacji. Te zagrożenia mogą mieć różnoraki charakter, np. kradzieży nośnika danych, zagubienia dokumentacji, ujawnienia informacji nieuprawnionej osobie przez telefon, ale też np. ataku hackerskiego na komputer sołtysa, na którym przechowuje on dane mieszkańców. Wynikiem ww. analizy zagrożeń, powinno być ustalenie, jakie techniczne lub organizacyjne środki bezpieczeństwa mogą zminimalizować ryzyko ich wystąpienia.

Ważne! Nie istnieje jedna metoda przeprowadzania analizy ryzyka. Sołtys może wybrać jeden z wielu dostępnych sposobów. Najważniejsze

pozostaje jednak przewidzenie, jakie negatywne zdarzenia mogą wystąpić i jaki mogą mieć one wpływ na osoby, których dane przetwarza. Takimi zdarzeniami są najczęściej zagubienie nośników danych, np. papierowej dokumentacji lub elektronicznych nośników (pendrive'ów).

Ważne! Środki bezpieczeństwa powinny być adekwatne do zidentyfikowanego ryzyka, ale powinny też uwzględniać charakter przetwarzania, rodzaj przetwarzanych danych, a także koszt ich wdrożenia i dostępną technologię. Takimi środkami może być np. przechowywanie dokumentacji w zamkniętych szafach, stosowanie silnych haseł do komputerów (hasło składające się z co najmniej 14 znaków), stosowanie aktualnego systemu operacyjnego, stosowanie oprogramowania antywirusowego, nieklikanie w podejrzane linki lub w załączniki od nieznanych nadawców, nieujawnianie danych osobowych w rozmowie telefonicznej, jeżeli nie znamy rozmówcy, wykonywanie kopii zapasowej dokumentacji przechowywanej papierowo i elektronicznie, np. przez zgrywanie jej na pendrive i przechowywanie go w innej, bezpiecznej lokalizacji.

Zadaniem, które stoi przed sołtysem – administratorem jest również realizacja obowiązku informacyjnego, czyli powiadomienie osób, których dane przetwarza o tym, że będzie tego dokonywał. Taki obowiązek przyjmuje zwykle formę klauzuli informacyjnej (wzór na końcu artykułu). Zakres informacji, które muszą się w nim znaleźć wyznacza art. 13 i art. 14 RODO. Sołtys, który pozyskuje dane bezpośrednio od podmiotu danych (np. od mieszkańca), powinien przekazać mu ww. informacje najpóźniej w momencie ich pozyskania.

Następnym zadaniem, o którym nie powinien zapomnieć sołtys mający status administratora, jest reagowanie na wszelkie przypadki naruszenia ochrony danych osobowych. Takim zdarzeniem jest naruszenie bezpieczeństwa przetwarzanych danych, które doprowadza do ich przypadkowego lub niezgodnego z prawem ujawnienia, utracenia lub zmodyfikowania.

Przykład: sołtys zagubił papierowy dokument zawierający wykaz wszystkich mieszkańców sołectwa wraz z ich imionami, nazwiskami, adresami i numerami telefonu.

Przykład: doszło do ataku na skrzynkę e-mail sołtysa, która służyła mu do korespondencji z mieszkańcami i przedstawicielami organów gminy. Na

skutek ataku mogło dojść do utracenia poufności danych, ponieważ hacker mógł zapoznać się z ich treścią, a nawet sporządzić ich kopie.

W przypadku wystąpienia naruszenia ochrony danych sołtys powinien ustalić okoliczności zdarzenia, a następnie przeanalizować, czy może ono stanowić zagrożenie dla praw i wolności podmiotów danych, np. czy na skutek ujawnienia danych nieuprawnionej osobie podmiot danych mogą spotkać przykre konsekwencje w postaci naruszenia dobrego imienia, szykan, kradzieży tożsamości, straty finansowej. Jeżeli na skutek przeprowadzonej oceny administrator dochodzi do wniosku, że ryzyko naruszenia praw lub wolności występuje, powinien on niezwłocznie, jednak nie później niż w ciągu 72 godzin zawiadomić o zdarzeniu Prezesa Urzędu Ochrony Danych Osobowych (szczegółowe zasady zgłoszenia opisane są na stronie organu pod adresem: <https://uodo.gov.pl/pl/492/2278>; dostęp na 20.11.2024 r.).

W pewnych sytuacjach – gdy ww. ryzyko naruszenia praw i wolności jest wysokie, administrator (sołtys) powinien też zawiadomić osoby, których dane dotyczą (np. mieszkańców, których dane znajdowały się na utraconym dokumencie).

Bardzo istotnym obowiązkiem, o którym powinien pamiętać każdy administrator, w tym sołtys, jest realizacja zasady rozliczalności (art. 5 ust. 2 RODO). Wymaga ona, aby sołtys był w stanie wykazać, że spełnia spoczywające na nim obowiązki. To z kolei wymaga od niego wprowadzenia pewnych sformalizowanych zasad przetwarzania danych i np. dokumentowania faktu spełnienia obowiązku informacyjnego, o którym była wyżej mowa.

Może to się odbywać przez umieszczenie klauzuli informacyjnej na drugiej stronie formularza papierowego, który służy sołtysowi do zbierania danych, czy też umieszczenie takiej klauzuli pod formularzem kontaktowym na stronie internetowej. Forma takiego dokumentowania jest dowolna, przy czym należy unikać wprowadzania obowiązku potwierdzenia przez podmiot danych, że zapoznał się on z treścią klauzuli przez obowiązek jej podpisania. Sołtys (administrator) nie ma obowiązku przechowywania takich dokumentów, zaś podmiot danych może nie wyrazić chęci złożenia podpisu pod treścią klauzuli, co nie będzie stanowiło przeszkody dla przetwarzania jego danych.

Również inne obowiązki realizowane przez sołtysa w obszarze ochrony danych osobowych powinny być stosownie udokumentowane, np. przez spisanie przeprowadzonej analizy ryzyka, czy stworzenie z niej formularza w Excelu. Podobnie w przypadku naruszeń ochrony danych sołtys, występujący w roli administratora, powinien zadbać o to, aby wszelkie ustalone okoliczności zostały utrwalone i włączone do dokumentacji z takiego zdarzenia wraz z ewentualną kopią zgłoszenia go do Prezesa Urzędu Ochrony Danych Osobowych lub potwierdzeniem zawiadomienia o nim podmiotów danych.

Warto zwrócić uwagę, że prawodawca nie określił czasu przechowywania dokumentacji związanej z wykonywaniem przez administratora zadań określonych w RODO. Można jednak przyjąć, że bezpiecznym okresem będzie 5 lat od końca roku obrotowego, w którym wystąpiło udokumentowane zdarzenie. Jest to bowiem czas, po upływie którego nie może zostać nałożona administracyjna kara pieniężna, czyli jedna z najpoważniejszych sankcji przewidzianych za niespełnienie ww. obowiązków (art. 189g § 1 Kodeksu postępowania administracyjnego).

Na koniec warto zwrócić uwagę, że sołtys występujący w roli administratora danych powinien prowadzić rejestr czynności przetwarzania danych osobowych, o którym mowa w art. 30 ust. 1 RODO. W mojej ocenie sołtys nie będzie mógł skorzystać w tym zakresie z wyjątków od prowadzenia takiego dokumentu przewidzianych w art. 30 ust. 5, w szczególności bowiem nie ma on statusu przedsiębiorcy ani podmiotu zatrudniającego, a ponadto przetwarzanie przez niego danych osobowych nie ma charakteru sporadycznego i wiąże się z ryzykiem naruszenia praw lub wolności osób, których te dane dotyczą.

Wskazany rejestr może być prowadzony przez sołtysa w formie pisemnej (papierowej) lub elektronicznej, np. w formie pliku Excel. Na końcu artykułu znajduje się wzór takiego dokumentu.

Trzeba też podkreślić, że powyższy opis obowiązków sołtysa – administratora nie ma charakteru wyczerpującego, ale obejmuje moim zdaniem najważniejsze zadania, które stoją przed sołtysem ustalającym cele i sposoby przetwarzania.

Zakończenie

Jak wyżej wskazałem, status sołtysa na gruncie przepisów o ochronie danych osobowych nie jest oczywisty. Z uwagi na mnogość wykonywanych zadań będzie on występował w wielu rolach w procesie przetwarzania, a w konsekwencji musi pozostawać w gotowości do realizacji szeregu różnych obowiązków. Niezależnie od roli, w której występuje, powinien też zadbać o odpowiednie przetwarzanie danych, a w szczególności o ich odpowiednie zabezpieczenie.

Na koniec chciałbym jeszcze zwrócić uwagę na pytanie, które pojawiło się na etapie tworzenia przeze mnie artykułu – czy sołtys może wykonywać i publikować w mediach społecznościowych zdjęcia z imprez organizowanych w sołectwie.

Czy sołtys może wykonywać i publikować w mediach społecznościowych zdjęcia z imprez organizowanych w sołectwie?

Wskazane zagadnienie wymaga analizy na dwóch płaszczyznach. Pierwsza to RODO i przetwarzanie danych osobowych, do których należy wizerunek zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (człowieka). Druga, to przepisy ustawy o prawie autorskim i prawach pokrewnych, które określają zasady rozpowszechniania wizerunku.

Sołtys, który dokumentuje we własnym imieniu różnego rodzaju imprezy odbywające się w sołectwie w celu publikowania zdjęć/nagrań w mediach społecznościowych, czy też na swojej stronie internetowej, jest administratorem danych osobowych. Aby przetwarzanie takich danych osobowych (wizerunku) było dopuszczalne musi on ustalić cel przetwarzania, którym może być np. informowanie o przebiegu wydarzeń, promowanie takich inicjatyw, czy też wzmacnianie więzi wśród społeczności lokalnej.

Podstawą przetwarzania danych może być w takim przypadku przede wszystkim prawnie uzasadniony interes realizowany przez administratora, który polegać będzie na promowaniu wydarzeń odbywających się w sołectwie, informowaniu o inicjatywach sołtysa, czy też zacieśnianie więzi pomiędzy mieszkańcami. O ile zatem w przypadku samego wykonywania zdjęć czy nagrywania filmu sołtys nie musi uzyskiwać zezwolenia ani odbierać zgody od osoby, która jest na nim uwieczniona, to sytuacja ta zmieni się w razie rozpowszechniania takich materiałów.

Powyższe wynika z faktu, że rozpowszechnianie wizerunku, czyli np. publikowanie go w mediach społecznościowych lub na stronie internetowej wymaga zezwolenia osoby, której ten wizerunek dotyczy na gruncie przepisów ustawy z 04.02.1994 r. o prawie autorskim i prawach pokrewnych. Zezwolenie takie może przybrać dowolną postać, np. pisemną, elektroniczną, ale może być też być zarejestrowane na początku nagrania, w którym osoba nagrywana oświadczy, że zezwala na rozpowszechnienie nagrania wraz ze swoim wizerunkiem przez określony podmiot (sołtysa), w określonym miejscu (np. na portalu społecznościowym) i przez określony czas (np. przez okres roku albo czas nieoznaczony).

Od tej zasady istnieje kilka wyjątków opisanych w art. 81 ustawy o prawie autorskim i prawach pokrewnych. Jednym z nich, który w mojej ocenie będzie miał największe znaczenie dla rozpowszechniania wizerunku przez sołtysa jest sytuacja, w której rozpowszechniany wizerunek stanowi jedynie szczegół większej całości. W takiej sytuacji sołtys nie ma obowiązku uzyskania zezwolenia od osób, które są na nagraniu/zdjęciu przedstawione. Przykładem może być zdjęcie z imprezy plenerowej, na którym widać sylwetki (wizerunki) wielu uczestników.

Ważne! Wskazany wyżej wyjątek od obowiązku uzyskania zezwolenia na rozpowszechnienie wizerunku dotyczy jedynie sytuacji, gdy wizerunek stanowi szczegół większej całości. Wyklucza to jego zastosowanie do zdjęć tzw. pozowanych, które mają na celu ujawnienie

konkretnych wizerunków. W takim przypadku konieczne będzie odebranie od takich osób zezwolenia.

Niezależnie od tego, czy dochodzi jedynie do utrwalania wizerunków na zdjęciach lub nagraniach, czy też mają być one później rozpowszechnione, sołtys powinien pamiętać, aby poinformować o tym uczestników wydarzenia przez przekazanie im wskazanej wyżej klauzuli informacyjnej. Można ją umieścić np. w regulaminie wydarzenia albo wyłożyć w widocznym punkcie w miejscu, w którym impreza się odbywa.



***Patryk Łuczyński** – aplikant adwokacki przy Okręgowej Radzie Adwokackiej w Warszawie. Absolwent Wydziału Prawa i Administracji Uniwersytetu Łódzkiego. Ekspert i kierownik zespołu ochrony danych w Inspektorzy ODO sp. z o.o. Specjalizuje się w prawie ochrony danych osobowych i prawach informacyjnych, w tym prawie dostępu do informacji publicznej.*

**Poradnik
Witryny Wiejskiej**



**SOŁE
CTWO** NA
NOWE
CZASY

Wzór klauzuli informacyjnej

1. Administratorem Twoich danych osobowych jest Sołtys XYZ.
2. Możesz skontaktować się ze mną pod adresem XYZ lub e-mailowo pisząc na adres: XYZ.
3. Twoje dane osobowe przetwarzam w celu:
 - a. – na podstawie art. 6 ust. 1 lit. RODO,
 - b. – na podstawie art. 6 ust. 1 lit. RODO.
4. Twoje dane osobowe będą przetwarzane przez okres [okres może wynikać z przepisów prawa, a jeżeli nie to administrator powinien określić go samodzielnie, mając na uwadze jak długo dane są mu potrzebne do realizacji celu, np. zabezpieczenia się przed roszczeniami].
5. Odbiorcami Twoich danych osobowych będą [odbiorcy to podmioty, którym ujawniamy dane, np. operator poczty, operator telekomunikacyjny, wójt gminy, hostingodawca, dostawca poczty elektronicznej].
6. Masz prawo dostępu do swoich danych osobowych, a także do żądania ich sprostowania, ograniczenia przetwarzania, przenoszenia oraz usunięcia. W zakresie danych, które przetwarzam na podstawie prawnie uzasadnionego interesu lub w celu realizacji zadania w interesie publicznym, masz prawo do wyrażenia sprzeciwu wobec ich przetwarzania.

Jeżeli przetwarzam Twoje dane osobowe na podstawie wyrażonej przez Ciebie zgody, masz prawo do jej wycofania w dowolnym momencie. Wycofanie zgody nie będzie miało wpływu na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem [jeżeli podstawą przetwarzania danych nie jest zgoda, ten fragment należy usunąć].

Niezależnie od ww. uprawnień możesz wnieść skargę do Prezesa Urzędu Ochrony Danych Osobowych, jeżeli uważasz, że przetwarzam Twoje dane niezgodnie z prawem.

7. Podanie przez Ciebie danych osobowych jest dobrowolne / dobrowolne, ale niezbędne do realizacji ww. celów przetwarzania / warunkiem zawarcia umowy / obowiązkiem prawnym [należy wybrać prawidłowe].

Wzór zgody na przetwarzanie danych osobowych

.....
(imię i nazwisko)

Zgadzam się na przetwarzanie moich danych osobowych w zakresie [zakres danych, np. imię i nazwisko, numer telefonu, adres e-mail], w celu [np. w celu utrzymania ze mną bieżącego kontaktu w sprawach związanych z bezpieczeństwem sołectwa, w sprawach związanych z pracami zespołu wiejskiego, w celu przekazywania mi informacji o wydarzeniach kulturalnych organizowanych na terenie sołectwa]. Wiem że mogę wycofać zgodę w dowolnym momencie, co nie będzie miało wpływu na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem.

.....
Podpis

Wzór rejestru czynności przetwarzania danych

Administrator danych:

Dane kontaktowe administratora:

L.P.	Nazwa czynności (np. Utrzymanie kontaktu z mieszkańcami)	Cele przetwarzania (np. utrzymanie bieżącego kontaktu z mieszkańcami, w tym obsługa poczty elektronicznej)	Opis kategorii osób, których dane są przetwarzane (np. mieszkańcy sołectwa kontaktujący się z sołtysem)	Opis kategorii danych osobowych (np. imiona i nazwiska, adres e-mail, adres zamieszkania, numer telefonu, treść komunikacji)	Kategorie odbiorców, którym ujawnione zostały lub zostaną dane osobowe (np. dostawca poczty elektronicznej)	Czy dochodzić będzie do transferu danych osobowych do państwa trzeciego lub organizacji międzynarodowej (jeżeli tak należy wskazać gdzie będzie transfer i jaka jest dokumentacja zabezpieczeń)	Planowany termin usunięcia danych osobowych (np. 12 miesięcy od zakończenia korespondencji w sprawie)	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (np. stosowanie silnych haseł dostępu do poczty e-mail, stosowanie dwuskładnikowego uwierzytelnienia do poczty).