

OCHRONA DANYCH OSOBOWYCH

- 1 CZY SPÓŁKA ZARZĄDZAJĄCA NIERUCHOMOŚCIĄ W IMIENIU WSPÓLNOTY MIESZKANIOWEJ MA PRAWO DOSTARCZAĆ JEJ CZŁONKOM KORESPONDENCJĘ DOTYCZĄCĄ SPRAW WSPÓLNOTY ZA POŚREDNICTWEM SWOICH PRACOWNIKÓW?2
- 2 CZY WSPÓLNOTA MIESZKANIOWA MOŻE UDOSTĘPNIĆ INFORMACJE O ZALEGŁOŚCIACH WE WNOŚZENIU OPŁAT SWOICH CZŁONKÓW INNYM OSOBOM NALEŻĄCYM DO WSPÓLNOTY?.....3
- 3 CZY POWIERZENIE PRZEZ WSPÓLNOTĘ MIESZKANIOWĄ ZARZĄDCY ZARZĄDU NIERUCHOMOŚCIĄ WSPÓLNĄ WYMAGA ZAWARCIA ODRĘBNEJ UMOWY O POWIERZENIU PRZETWARZANIA DANYCH OSOBOWYCH?.....4
- 4 DO JAKICH CELÓW ZARZĄDCA NIERUCHOMOŚCI MOŻE WYKORZYSTYWAĆ DANE OSOBOWE CZŁONKÓW WSPÓLNOTY MIESZKANIOWEJ?5
- 5 CZY POSZCZEGÓLNI CZŁONKOWIE WSPÓLNOTY MIESZKANIOWEJ UPRAWNIENI SĄ DO UZYSKANIA INFORMACJI O ZALEGŁOŚCIACH WE WNOŚZENIU OPŁAT EKSPLOATACYJNYCH INNYCH CZŁONKÓW TEJ WSPÓLNOTY?6
- 6 CZY WSPÓLNOTA MIESZKANIOWA JEST ADMINISTRATOREM DANYCH OSOBOWYCH SWOICH CZŁONKÓW I CZY MA OBOWIĄZEK ZGŁOSZENIA TAKIEGO ZBIORU DO REJESTRACJI GENERALNEMU INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH?7
- 7 JAKIE WYMAGANIA ODNOŚNIE ZABEZPIECZENIA DANYCH OSOBOWYCH MUSI SPEŁNIĆ WSPÓLNOTA MIESZKANIOWA, A JAKIE ZARZĄDCA NIERUCHOMOŚCI?7
- 8 JAKIE WYMAGANIA ODNOŚNIE ZABEZPIECZENIA DANYCH OSOBOWYCH MUSI SPEŁNIĆ WSPÓLNOTA MIESZKANIOWA, A JAKIE ZARZĄDCA NIERUCHOMOŚCI?8
- 9 NIE, BOWIEM ŻADEN Z PRZEPISÓW PRAWA NIE UPOWAŻNIA WSPÓLNOTY DO UPUBLICZNIENIA TEGO TYPU DANYCH.9
- 10 CZY WSPÓLNOTA MIESZKANIOWA MA PRAWO PRZECHOWYWAĆ AKTA NOTARIALNE DOTYCZĄCE POSZCZEGÓLNYCH LOKALI?9
- 11 CZY SPÓŁDZIELNIA MIESZKANIOWA MOŻE ZA POŚREDNICTWEM DOZORCÓW DORĘCZAĆ KORESPONDENCJĘ KIEROWANĄ DO CZŁONKÓW TEJ SPÓŁDZIELNI?10
- 12 CZY SPÓŁDZIELNIA MIESZKANIOWA, KTÓRA JAKO ZABEZPIECZENIE SPŁATY KREDYTU, WSKAZAŁA PRZELEW WIERZYTELNOŚCI WPŁAT CZŁONKÓW SPÓŁDZIELNI NA FUNDUSZ REMONTÓW, MOŻE UDOSTĘPNIĆ BANKOWI DANE OSOBOWE OSÓB DOKONUJĄCYCH TYCH WPŁAT?.....11
- 13 CZY SPÓŁDZIELNIA MIESZKANIOWA MOŻE PUBLIKOWAĆ NA SWOJEJ STRONIE INTERNETOWEJ KIEROWANĄ DO NIEJ KORESPONDENCJĘ ZAWIERAJĄCĄ DANE OSOBOWE CZŁONKA TEJ SPÓŁDZIELNI?12
- 14 CZY SPÓŁDZIELNIA MIESZKANIOWA MA PRAWO UDOSTĘPNIĆ INFORMACJE DOTYCZĄCE ROZLICZENIA INDYWIDUALNYCH KOSZTÓW ZUŻYCIA CIEPŁA W POSZCZEGÓLNYCH LOKALACH? ...13
- 15 CZY W STATUCIE SPÓŁDZIELNI MOŻNA WSKAZAĆ, ŻE W REJESTRZE CZŁONKÓW ODNOTOWYWANE BĘDĄ INFORMACJE O ZALEGŁOŚCIACH Z TYTUŁU WYDATKÓW ZWIĄZANYCH Z CZŁONKOSTWEM WRAZ Z IMIENIEM I NAZWISKIEM ORAZ ADRESEM ZAMIESZKANIA ZADŁUŻONEGO CZŁONKA?14
- 16 CZY STRAŻ MIEJSKA MA PRAWO POZYSKAĆ, NA POTRZEBY SKIEROWANIA DO SĄDU WNIOSKU O UKARANIE, INFORMACJE O DOCHODACH, STANIE MAJĄTKOWYM CZY TEŻ LICZBIE OSÓB POZOSTAJĄCYCH NA UTRZYMANIU OSOBY, KTÓRA POPEŁNIŁA WYKROCZENIE?14
- 17 CZY DANE OSOBOWE PRZETWARZANE PRZEZ STRAŻ MIEJSKĄ, ZAWARTE W DOKUMENTACH PAPIEROWYCH, TAKICH JAK NOTATNIKI SŁUŻBOWE, NOTATKI URZĘDOWE,

OCHRONA DANYCH OSOBOWYCH

CZY WYPEŁNIONE BLANKIETY MANDATÓW KARNYCH STANOWIĄ ODREBNE, OD ZAREJESTROWANYCH U GİODO, ZBIORY DANYCH W ROZUMIENIU USTAWY O OCHRONIE DANYCH OSOBOWYCH?.....	15
18 CZY ZGODNE Z PRAWEM JEST DZIAŁANIE JEDNOSTEK STRAŻY MIEJSKIEJ POLEGAJĄCE NA WYKONYWANIU FOTOGRAFII OSOBOM ZATRZYMANYM W CELU DOPROWADZENIA TYCH OSÓB DO IZBY WYTRZEŻWIEN?	16
19 CZY STRAŻE MIEJSKIE SĄ UPOWAŻNIONE DO POZYSKIWANIA - POPRZEC "PROTOKOŁY PRZESŁUCHANIA PODEJRZANEGO O POPEŁNIENIE WYKROCZENIA";- OD OSÓB PODEJRZANYCH O POPEŁNIENIE WYKROCZENIA, DANYCH O STANIE ICH ZDROWIA?.....	17
20 CZY OD RODZICÓW ZAPISUJĄCYCH DZIECKO DO ŚWIETLICY SZKOLNEJ MOŻNA ŻAĐAĆ PODANIA TAKICH DANYCH, JAK ICH MIEJSCE ZATRUDNIENIA, STANOWISKO ORAZ WYNAGRODZENIE?	19
21 CZY PLACÓWKI OŚWIATOWE SĄ ZOBOWIĄZANE DO ZAWARCIA PISEMNEJ UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH Z PRZEDSIĘBIORCĄ, KTÓRY UDOSTĘPNIA IM SYSTEM INFORMATYCZNY DO PROWADZENIA E-DZIENNIKÓW?.....	20
22 CZY MOGĘ UZYSKAĆ OD OPERATORA TELEKOMUNIKACYJNEGO WYKAZ ROZMÓW PRZYCHODZĄCYCH NA MÓJ TELEFON?.....	20
23 CZY ZGODA ABONENTA NA UMIESZCZENIE JEGO DANYCH OSOBOWYCH W KSIĄŻCE TELEFONICZNEJ MOŻE BYĆ WYRAŻONA W KAŻDYM CZASIE?.....	21

1 Czy spółka zarządzająca nieruchomością w imieniu wspólnoty mieszkaniowej ma prawo dostarczać jej członkom korespondencję dotyczącą spraw wspólnoty za pośrednictwem swoich pracowników?

Tak, ale pod warunkiem że pracownikom dostarczającym korespondencję nadane zostały upoważnienia do przetwarzania danych osobowych.

Uzasadnienie

Zgodnie z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, każda osoba, która przy wykonywaniu obowiązków służbowych ma dostęp do danych osobowych, powinna posiadać stosowne upoważnienie do przetwarzania danych, o którym mowa w art. 37 ustawy. Zgodnie z tym przepisem, do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych (w tym przypadku spółkę). Tym samym każdy pracownik, który przetwarza dane osobowe, musi legitymować się takim upoważnieniem. Upoważnienia należy zatem nadać nie tylko osobom, które zatrudnione zostały bezpośrednio w celu przetwarzania danych, ale również osobom, które mogą w takim przetwarzaniu uczestniczyć.

Osoby trudniące się doręczaniem korespondencji, z racji wykonywanych przez nich czynności, mają dostęp do danych osobowych choćby w zakresie imion i nazwisk, czy adresów osób, którym korespondencję doręczają, a tym samym przetwarzają dane osobowe. Przetwarzanie danych osobowych to bowiem wykonywanie jakichkolwiek operacji na danych osobowych, takich jak np. zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie (art. 7 pkt 2 ustawy). W konsekwencji, osoby dostarczające korespondencję, podobnie, jak wszystkie inne osoby przetwarzające dane osobowe w imieniu i na rzecz administratora, stosownie do art. 37 ustawy o ochronie danych osobowych, muszą otrzymać od niego odpowiednie upoważnienie do przetwarzania danych osobowych.

Upoważnienie do przetwarzania danych osobowych powinno być upoważnieniem specjalnym, odrębnym, a nie wywodzonym tylko z treści umowy czy z zakresu obowiązków pracowniczych. Powinno mieć charakter imienny, a także określać dozwolony zakres przetwarzania danych osobowych.

Wskazać należy także, iż art. 39 ust. 1 ustawy przewiduje obowiązek prowadzenia przez administratora danych ewidencji osób upoważnionych do przetwarzania danych osobowych, w której powinny być zawarte takie informacje, jak: imię i nazwisko osoby upoważnionej, data nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Ewidencja powyższa powinna być prowadzona w formie pisemnej. Stanowi ona dokument poufny, chroniony tajemnicą pracodawcy, a informacje w niej zawarte są objęte również tajemnicą wyznaczoną przez art. 39 ust. 2 ustawy, zgodnie z którym osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

A zatem spółka zarządzająca nieruchomością w imieniu wspólnoty mieszkaniowej może dostarczać członkom tej wspólnoty korespondencję za pośrednictwem swoich pracowników, ale musi nadać im upoważnienia do przetwarzania danych osobowych oraz prowadzić ewidencję takich upoważnień. Spółka ta – jako administrator danych (pracodawca) – powinna dostarczać korespondencję w taki sposób, aby zagwarantować odpowiednią ochronę zawartych w niej danych oraz uniemożliwić zapoznanie się z nimi osobom nieuprawnionym.

2 CZY WSPÓLNOTA MIESZKANIOWA MOŻE UDOSTĘPNIĆ INFORMACJE O ZALEGŁOŚCIACH WE WNOŚZENIU OPŁAT SWOICH CZŁONKÓW INNYM OSOBOM NALEŻĄCYM DO WSPÓLNOTY?

Tak, wspólnota mieszkaniowa ma prawo udostępnić informacje o zaległościach we wnoszeniu opłat swoich członków innym współwłaścicielom należącym do tej wspólnoty.

Uzasadnienie

Zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przetwarzanie danych osobowych jest dopuszczalne w momencie, gdy administrator danych osobowych (wspólnota mieszkaniowa) wykaże się jedną z przesłanek legalizujących przetwarzanie tych danych. Ustawa dopuszcza możliwość przetwarzania danych tzw. zwykłych (jak np. imię i nazwisko, adres zamieszkania) m.in. wtedy, gdy wynika to z przepisów prawa (art. 23 ust. 1 pkt 2 ustawy).

Wspólnoty mieszkaniowe są tworzone na podstawie przepisów ustawy z dnia 24 czerwca 1994 r. o własności lokali, a w zakresie w niej nieuregulowanym zastosowanie znajdują przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny. Z przepisów Księgi Drugiej Tytułu I Działu IV Kodeksu wynika, że współwłaściele dla prawidłowego zarządzania współwłasnością muszą znać dane osobowe pozostałych współwłaścicieli. Zgodnie bowiem z jego art. 200 każdy ze współwłaścicieli jest obowiązany do współdziałania w zarządzie rzeczą wspólną. Podobnie, wskazana wyżej ustawa o własności lokali w art. 29 ust. 3 stanowi, że prawo kontroli działalności zarządu służy każdemu właścicielowi lokalu. Z powołanych przepisów wynika zatem przysługujące każdemu współwłaścicielowi uprawnienie dostępu do dokumentacji związanej z zarządzaniem nieruchomością.

Zakres danych i informacji przekazywanych współwłaścicielom powinien być adekwatny do ich potrzeb związanych ze zgodnym z prawem celem udostępnienia.

Stosownie do art. 16 ust. 1 ustawy o własności lokali, jeżeli właściciel lokalu zalega długotrwale z zapłatą należnych od niego opłat lub wykracza w sposób rażący lub uporczywy przeciwko obowiązującemu porządkowi domowemu albo przez swoje niewłaściwe zachowanie

czyni korzystanie z innych lokali lub nieruchomości wspólnej uciążliwym, wspólnota mieszkaniowa może w trybie procesu żądać sprzedaży lokalu w drodze licytacji na podstawie przepisów Kodeksu postępowania cywilnego o egzekucji z nieruchomości. Aby wspólnota mogła skorzystać z tego uprawnienia, **jej członkowie powinni znać dane osobowe właściciela i wysokość jego zadłużenia wobec wspólnoty.**

A zatem dopuszczalność udostępnienia członkom wspólnoty mieszkaniowej, ale wyłącznie im, danych i informacji dotyczących zaległości we wnoszeniu opłat należnych wspólnocie przez innych jej członków wynika z przepisów prawa, a tym spełniona zostaje przesłanka określona w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

3 CZY POWIERZENIE PRZEZ WSPÓLNOTĘ MIESZKANIOWĄ ZARZĄDCY ZARZĄDU NIERUCHOMOŚCIĄ WSPÓLNĄ WYMAGA ZAWARCIA ODRĘBNEJ UMOWY O POWIERZENIU PRZETWARZANIA DANYCH OSOBOWYCH?

Nie, pod warunkiem, że w umowie o powierzeniu zarządcy zarządu nieruchomością wspólną będą zawarte postanowienia umowy o powierzeniu przetwarzania danych osobowych.

Uzasadnienie

Wspólnoty mieszkaniowe są tworzone na podstawie przepisów ustawy z dnia 24 czerwca 1994 r. o własności lokali, a w zakresie w niej nieuregulowanym przepisów ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny. Właściciele lokali mogą 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). Zarząd lub zarządca, któremu zarząd nieruchomością wspólną powierzono, jest obowiązany sporządzić protokół przejęcia nieruchomości i jej dokumentacji technicznej (budowlanej, powykonawczej i książki obiektu budowlanego) w imieniu wspólnoty mieszkaniowej, przechowywać dokumentację techniczną budynku oraz prowadzić i aktualizować spis właścicieli lokali i przypadających im udziałów w nieruchomości wspólnej (art. 29 ust. 1 b ustawy). Zarządca nieruchomości wspólnej jest zatem nie tylko upoważniony, ale i zobowiązany do gromadzenia danych osobowych dotyczących właścicieli lokali w granicach określonych w tym przepisie. Jednocześnie, administratorem danych osobowych (podmiotem, który decyduje o celach i środkach przetwarzania danych osobowych wykorzystywanych przez wspólnotę mieszkaniową) jest ta wspólnota. Zarządca nieruchomości wspólnej może przetwarzać dane członków wspólnoty tylko jako podmiot, któremu, w myśl art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przetwarzanie danych powierzono. Umowa o ustanowieniu zarządcy powinna zawierać postanowienia umowy powierzenia przetwarzania danych osobowych, o której mowa w art. 31 ustawy o ochronie danych osobowych. A zatem powinna zawierać określenie celu, w jakim podmiot, któremu powierzono przetwarzanie danych może je przetwarzać oraz zakresu powierzonych do przetwarzania danych. Podmiot ten może bowiem przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

Zarządca nieruchomością wspólną wykonuje swoje obowiązki w interesie i na rzecz wspólnoty mieszkaniowej, a jego działania służyć powinny m.in. wykonaniu uchwał wspólnoty. Zarządca nieruchomości jest więc podmiotem, który działa w imieniu i na rzecz wspólnoty mieszkaniowej. Zakres jego praw i obowiązków określają przepisy prawa i postanowienia umowy o zarządzanie nieruchomością wspólną. Innymi słowy to na wspólnocie, a nie na zarządzającym w jej imieniu nieruchomością wspólną, ciąży – stosownie do przepisów o ochronie danych osobowych – prawa i obowiązki administratora danych, czyli podmiotu decydującego o celach i środkach przetwarzania danych osobowych. Działania zarządcy nieruchomością wspólną na jej rzecz są tak długo zgodne z prawem, jak długo znajdują umocowanie w łączącej strony - wspólnotę i zarządcę - umowie. Ewentualnych roszczeń z tytułu niewykonania lub nienależytego wykonania umowy przez zarządcę wspólnota

mieszkaniowa może dochodzić na drodze sądowej na zasadach ogólnych, wynikających z Kodeksu cywilnego, w trybie przepisów ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego.

Można zatem stwierdzić, iż umowa o powierzeniu zarządcy zarządu nieruchomością wspólną jest umową, w której powinny być zawarte postanowienia dotyczące kwestii przetwarzania danych osobowych członków wspólnoty mieszkaniowej. O ile zatem umowa ta będzie tak skonstruowana, to nie jest wymagana odrębna umowa wspólnoty mieszkaniowej z zarządcą o powierzeniu przetwarzania danych osobowych, o której mowa w art. 31 ustawy o ochronie danych osobowych.

4 Do jakich celów zarządca nieruchomości może wykorzystywać dane osobowe członków wspólnoty mieszkaniowej?

Zarządca nieruchomości wspólnej może przetwarzać dane członków wspólnoty tylko jako podmiot, któremu, w myśl art. 31 ustawy o ochronie danych osobowych, przetwarzanie danych powierzono. Zarządca nieruchomości wspólnej wykonuje swoje obowiązki w interesie i na rzecz wspólnoty mieszkaniowej, a jego działania służące powinny m.in. wykonaniu uchwał wspólnoty.

Uzasadnienie

Zagadnienie zakresu kompetencji zarządcy nieruchomości rozstrzygają przepisy ustawy z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami, ustawy z dnia 24 czerwca 1994 r. o własności lokali oraz postanowienia umowy o zarządzanie nieruchomością wspólną.

W myśl art. 185 ust. 2 ustawy o gospodarce nieruchomościami, zarządca nieruchomości działa na podstawie umowy o zarządzanie nieruchomością zawartej z jej właścicielem, wspólnotą mieszkaniową albo inną jednostką organizacyjną, której przysługuje prawo do nieruchomości, ze skutkiem prawnym bezpośrednio dla tej osoby lub jednostki organizacyjnej. Ust. 3 tego przepisu stanowi, że zakres uprawnień i obowiązków zarządcy wynika z przepisów ustawy, z przepisów odrębnych ustaw oraz z umowy o zarządzanie nieruchomością.

Sposób zarządu nieruchomością wspólną pozostawiony zatem został decyzji samych członków wspólnoty mieszkaniowej i powinien być przez nich określony w umowie o ustanowieniu odrębnej własności lokali, albo w umowie zawartej później w formie aktu notarialnego.

Podobnie, ustawa o własności lokali w art. 18 ust. 1 stanowi, iż właściele lokali mogą 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. Z jej art. 29 ust. 1b wynika natomiast, że zarząd lub zarządca, któremu zarząd nieruchomością wspólną powierzono w sposób określony w art. 18 ust. 1, jest obowiązany sporządzić protokół przejęcia nieruchomości i jej dokumentacji technicznej (budowlanej, powykonawczej i książki obiektu budowlanego) w imieniu wspólnoty mieszkaniowej, przechowywać dokumentację techniczną budynku oraz prowadzić i aktualizować spis właścicieli lokali i przypadających im udziałów w nieruchomości wspólnej.

Zarządca nieruchomości jest więc podmiotem, który działa w imieniu i na rzecz wspólnoty mieszkaniowej. Zakres jego praw i obowiązków określają przepisy prawa i postanowienia umowy o zarządzanie nieruchomością wspólną. Jego działania na rzecz wspólnoty są tak długo zgodne z prawem, jak długo znajdują umocowanie w łączącej strony - wspólnotę i zarządcę - umowie. Z chwilą powołania nowego zarządu i rozwiązania dotychczasowej umowy o zarządzanie nieruchomością, zarządca nieruchomości powinien przekazać dokumenty związane ze sprawowaniem zarządu swojemu następcy. Powoływanie się w takim

przypadku na ustawę o ochronie danych osobowych, jako podstawę odmowy ich wydania nowemu zarządcy byłoby bezzasadne.

Ewentualnych roszczeń z tytułu niewykonania lub nienależytego wykonania umowy przez zarządcę wspólnota mieszkaniowa może dochodzić na drodze sądowej na zasadach ogólnych, wynikających z Kodeksu cywilnego, w trybie określonym w Kodeksie postępowania cywilnego.

Jeśli sposobu zarządu nie określono w umowie, o której mowa w art. 18 ust. 1 ustawy o własności lokali obowiązują zasady określone w rozdziale 4 tej ustawy. Art. 29 1b ustawy o własności lokali obliuguje zarządcę o prowadzenia i aktualizowania spisu właścicieli lokali i przypadających im udziałów w nieruchomości wspólnej. Zarządca nieruchomości wspólnej jest zatem nie tylko upoważniony, ale i zobowiązany do gromadzenia danych osobowych dotyczących właścicieli lokali w granicach określonych w tym przepisie. Przetwarzanie przez zarządcę nieruchomości wspólnej danych osobowych członków wspólnoty nie jest w takiej sytuacji uzależnione od wyrażenia przez nich zgody na przetwarzanie danych.

Jednocześnie, administratorem danych osobowych (podmiotem, który decyduje o celach i środkach przetwarzania danych osobowych wykorzystywanych przez wspólnotę mieszkaniową) jest ta wspólnota.

5 Czy poszczególni członkowie wspólnoty mieszkaniowej uprawnieni są do uzyskania informacji o zaległościach we wnoszeniu opłat eksploatacyjnych innych członków tej wspólnoty?

Tak, gdyż zezwalają na to przepisy prawa.

Uzasadnienie

Do wspólnot mieszkaniowych tworzonych na podstawie ustawy z dnia 24 czerwca 1994 r. o własności lokali stosuje się - w zakresie w niej nieuregulowanym - przepisy ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny. Z przepisów Kodeksu cywilnego wynika, że współwłaściele dla prawidłowego zarządzania współwłasnością muszą znać dane osobowe pozostałych współwłaścicieli. Zgodnie bowiem z jego art. 200, "każdy ze współwłaścicieli jest obowiązany do współdziałania w zarządzie rzeczą wspólną". Podobnie wskazana ustawa o własności lokali w art. 29 ust. 3 stanowi, że prawo kontroli działalności zarządu służy każdemu właścicielowi lokalu.

Z powołanych przepisów wynika zatem uprawnienie każdego współwłaściciela do dostępu do dokumentacji związanej z zarządzaniem nieruchomością. Wskazać w tym miejscu należy, iż zakres danych i informacji udostępnianych współwłaścicielom powinien być adekwatny do ich potrzeb związanych ze zgodnym z prawem celem udostępnienia. Przepis art. 26 ust. 1 pkt 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych stanowi, iż "administrator danych (...) powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane". Nie jest więc dopuszczalne udostępnienie współwłaścicielom określonej nieruchomości danych, których przetwarzanie nie jest niezbędne do współdziałania w zarządzie nieruchomością wspólną oraz do sprawowania kontroli działalności jej zarządcy.

Stosownie do art. 16 ust. 1 ustawy o własności lokali, jeżeli właściciel lokalu zalega długotrwale z zapłatą należnych od niego opłat lub wykracza w sposób rażący lub uporczywy przeciwko obowiązującemu porządkowi domowemu albo przez swoje niewłaściwe zachowanie czyni korzystanie z innych lokali lub nieruchomości wspólnej uciążliwym, wspólnota mieszkaniowa może w trybie procesu żądać sprzedaży lokalu w drodze licytacji na podstawie przepisów Kodeksu postępowania cywilnego o egzekucji z nieruchomości. Aby wspólnota mogła skorzystać z tego uprawnienia, jej członkowie powinni znać dane osobowe właściciela i wysokość jego zadłużenia wobec wspólnoty.

Wobec powyższego dopuszczalność udostępnienia członkom wspólnoty mieszkaniowej danych dotyczących zaległości we wnoszeniu opłat przez innych jej członków wynika z przepisów prawa, a tym samym znajduje oparcie w przesłance określonej w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych.

6 Czy wspólnota mieszkaniowa jest administratorem danych osobowych swoich członków i czy ma obowiązek zgłoszenia takiego zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych?

Wspólnota mieszkaniowa jest administratorem danych osobowych swoich członków, jednak jest zwolniona z obowiązku zgłoszenia takiego zbioru danych do rejestracji GIODO.

Uzasadnienie

Administratorem danych członków wspólnoty mieszkaniowej jest ta wspólnota, gdyż - jak wynika z art. 6 ustawy z dnia 24 czerwca 1994 r. o własności lokali - jest ona podmiotem praw i obowiązków wynikających z tejże ustawy. W związku z tym na niej spoczywają obowiązki wynikające z ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Zarząd wspólnoty, o ile został powołany, działa jako jej organ. Zarządca nieruchomości natomiast pełni zazwyczaj rolę podmiotu, o którym mowa w art. 31 ustawy o ochronie danych osobowych - a więc podmiotu, któremu administrator danych powierzył przetwarzanie danych. Jednakże jego status uzależniony jest od konstrukcji umowy, którą zawarł ze wspólnotą.

Wspólnota mieszkaniowa nie jest jednak zobowiązana do zgłoszenia zbioru danych swoich członków do rejestracji, gdyż z art. 43 ust. 1 pkt 4 wynika, że z tego obowiązku zwolnieni są administratorzy danych dotyczących osób u nich zrzeszonych.

7 Jakie wymagania odnośnie zabezpieczenia danych osobowych musi spełnić wspólnota mieszkaniowa, a jakie zarządca nieruchomości?

Zarówno administrator, jak i podmiot, któremu przetwarzanie danych osobowych powierzono, czyli zarówno wspólnota jak i zarządca, muszą zastosować wymagania odnoszące się do zabezpieczenia danych, zgodnie z normami art. 36-39 ustawy o ochronie danych osobowych i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Ustawa o ochronie danych osobowych nakazuje tym podmiotom m.in.:

- zastosowanie środków organizacyjnych i technicznych zapewniających ochronę odpowiednią do zagrożeń i ryzyka,
- zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniam przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
- prowadzenie dokumentacji określającej sposób wykorzystania danych,
- wyznaczenie administratora bezpieczeństwa informacji,
- wydanie upoważnień do dostępu do danych osobowych,
- prowadzenie rejestru takich wydanych upoważnień,

OCHRONA DANYCH OSOBOWYCH

- zastosowanie środków sprawowania kontroli nad wykorzystywaniem danych osobowych w zbiorach.

Uszczegółowieniem tych przepisów jest ww. rozporządzenie określające sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę danych. Rozporządzenie określa też podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Należy pamiętać również, że w umowie powierzenia przetwarzania danych zawartej pomiędzy wspólnotą, a jej zarządem mogą być określone wyższe rygory niż wynikające z tych przepisów i wtedy zarząd musi podejmować działania zgodne z zawartą umową.

Ustawa o ochronie danych osobowych zawiera przepisy karne. Choćby nieumyślne naruszenie obowiązku zabezpieczenia danych przed ich zabránieniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem podlega grzywnie, karze pozbawienia wolności do roku albo karze ograniczenia wolności.

8 Jakie wymagania odnośnie zabezpieczenia danych osobowych musi spełnić wspólnota mieszkaniowa, a jakie zarządca nieruchomości?

Zarówno administrator, jak i podmiot, któremu przetwarzanie danych osobowych powierzono, czyli zarówno wspólnota jak i zarządca, muszą zastosować wymagania odnoszące się do zabezpieczenia danych, zgodnie z normami art. 36-39 ustawy o ochronie danych osobowych i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Ustawa o ochronie danych osobowych nakazuje tym podmiotom m.in.:

- zastosowanie środków organizacyjnych i technicznych zapewniających ochronę odpowiednią do zagrożeń i ryzyka,
- zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabránieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
- prowadzenie dokumentacji określającej sposób wykorzystania danych,
- wyznaczenie administratora bezpieczeństwa informacji,
- wydanie upoważnień do dostępu do danych osobowych,
- prowadzenie rejestru takich wydanych upoważnień,
- zastosowanie środków sprawowania kontroli nad wykorzystywaniem danych osobowych w zbiorach.

Uszczegółowieniem tych przepisów jest ww. rozporządzenie określające sposób prowadzenia i zakres dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę danych. Rozporządzenie określa też podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Należy pamiętać również, że w umowie powierzenia przetwarzania danych zawartej pomiędzy wspólnotą, a jej zarządem mogą być określone wyższe rygory niż wynikające z tych przepisów i wtedy zarząd musi podejmować działania zgodne z zawartą umową.

Ustawa o ochronie danych osobowych zawiera przepisy karne. Choćby nieumyślne naruszenie obowiązku zabezpieczenia danych przed ich zabránieniem przez osobę nieuprawnioną,

uszkodzeniem lub zniszczeniem podlega grzywnie, karze pozbawienia wolności do roku albo karze ograniczenia wolności.

Czy zarząd wspólnoty mieszkaniowej ma prawo upublicznić na klatce schodowej listę zawierającą numer mieszkania wraz z przypisaną do niego kwotą zaległości?

9 Nie, bowiem żaden z przepisów prawa nie upoważnia wspólnoty do upublicznienia tego typu danych.

Uzasadnienie

Zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych administrator, przetwarzając dane osobowe, czyli wykonując na nich jakiegokolwiek operacje, takie jak zbieranie, utrwalanie, przechowywanie czy też udostępnianie - by jego działanie było legalne - powinien spełnić jeden z warunków dopuszczalności przetwarzania danych wymienionych w art. 23 tej ustawy.

Jednym z nich jest istnienie innego, szczególnego wobec ustawy o ochronie danych osobowych, przepisu prawa zezwalającego na określone postępowanie (art. 23 ust. 1 pkt 2).

Dlatego, aby przetwarzanie danych (w tym przypadku upublicznienie listy dłużników), było legalne, administrator (czyli zarząd wspólnoty) powinien wskazać upoważniający go do tego przepis prawa.

I tak, podstawę przetwarzania danych osobowych członków wspólnoty mieszkaniowej przez zarząd wspólnoty stanowią przepisy ustawy z 24 czerwca 1994 r. o własności lokali, a w zakresie nieuregulowanym w tych przepisach - ustawy Kodeks cywilny

Aczkolwiek żaden z ww. przepisów nie zezwala na podawanie do publicznej wiadomości danych osobowych członków wspólnoty mieszkaniowej np. poprzez wywieszanie numerów mieszkań wraz z przypisaną do nich kwotą zaległości. Tym samym przepisy prawa nie stanowią podstawy do upublicznienia tego typu informacji.

Jednak zauważyć należy, że brak w przepisach podstawy do zamieszczania w miejscach ogólnie dostępnych informacji o zadłużeniach czynszowych członków wspólnoty mieszkaniowej nie oznacza, że informacje te nie mogą być ujawnione innym członkom tej wspólnoty. Bowiem wspólnota mieszkaniowa jest z mocy prawa uprawniona do przetwarzania danych osobowych swoich członków. Z kodeksu cywilnego zaś wynika, że współwłaściciele dla prawidłowego zarządzania współwłasnością muszą znać dane osobowe pozostałych współwłaścicieli. Natomiast zgodnie z art. 29 ust. 3 ustawy o własności lokali, prawo do kontroli działalności zarządu służy każdemu właścicielowi lokalu. W konsekwencji każdemu właścicielowi przysługuje uprawnienie do wglądu w całość dokumentacji związanej z zarządem nieruchomością wspólną.

Dlatego wszelkie informacje, które dotyczą bezpośrednio każdego ze współwłaścicieli (np. zaległości czynszowe) muszą zostać odnotowywane w dokumentacji związanej z zarządem nieruchomością wspólną. Natomiast wywieszanie – udostępnianie danych osobowych (tj. numeru mieszkania wraz z kwotą zaległości), czego następstwem jest możliwość zapoznania się z tymi danymi przez szerokie grono osób – w tym także przez osoby nieupoważnione, odbywa się bez podstawy prawnej.

10 Czy wspólnota mieszkaniowa ma prawo przechowywać akta notarialne dotyczące poszczególnych lokali?

Nie, gdyż żaden przepis prawa, na podstawie których działają wspólnoty mieszkaniowe, nie daje podstawy do przechowywania takich dokumentów.

Uzasadnienie

Wspólnoty mieszkaniowe są tworzone na podstawie przepisów ustawy z dnia 24 czerwca 1994 r. o własności lokali, a w zakresie w niej nieuregulowanym przepisów ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny. Z przepisów Księgi Drugiej Tytułu I Działu IV Kodeksu wynika, że współwłaściciele dla prawidłowego zarządzania współwłasnością muszą znać dane osobowe pozostałych współwłaścicieli. Zgodnie bowiem z jego art. 200 każdy ze współwłaścicieli jest obowiązany do współdziałania w zarządzie rzeczą wspólną.

Wspólnotę mieszkaniową tworzy ogół właścicieli, których lokale wchodzą w skład „*określonej nieruchomości*”, co oznacza, że wspólnotę mogą tworzyć tylko ci właściciele, których lokale były przed wyodrębnieniem częściami składowymi oznaczonej nieruchomości gruntowej. Wspólnoty mieszkaniowe powstają z mocy prawa z chwilą, gdy zostają spełnione ustawowe przesłanki, tzn. gdy co do określonej nieruchomości pojawia się co najmniej dwie osoby, których prawa do lokali reguluje ustawa o własności lokali. Jako najmniejszą należy wymienić wspólnotę, jaką tworzą w dwulokalowym budynku dwaj właściciele lokali oraz wspólnotę, jaką stanowią - w razie wyodrębnienia w większym domu pierwszego lokalu - właściciel tego lokalu oraz dotychczasowy właściciel nieruchomości. Inaczej mówiąc, do wspólnoty mieszkaniowej nie można się zapisać czy przystąpić; nie można też z niej wystąpić.

Aby prawidłowo wykonywać swoje obowiązki związane z zarządem nieruchomością wspólną zarząd wspólnoty (lub ustanowiony zarządca) musi mieć dostęp do dokumentów wspólnoty, czyli dokumentów wszystkich lokali wchodzących w jej skład. Zgodnie z art. 29 ust 1e ustawy o własności lokali zarząd lub zarządca, któremu zarząd nieruchomością wspólną powierzono, może żądać od właścicieli lokali okazania dokumentów potwierdzających prawo własności lokali. Okazanie dokumentów nie jest tożsame z doręczeniem ich kserokopii, jak również brak jest w powołanym przepisie wyraźnego wskazania, że dokumentem potwierdzającym przedmiotowe prawo jest akt notarialny. Ponadto, przechowywanie przez wspólnotę mieszkaniową aktów notarialnych, w których zawarte są dane osobowe, mogłoby naruszać zasadę adekwatności przetwarzania danych osobowych, o której mowa w art. 26 ust. 1 pkt 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Oznacza ona, że należy przetwarzać (gromadzić i wykorzystywać) dane osobowe tylko w takim zakresie, jaki jest niezbędny dla osiągnięcia zamierzonego celu. Tak stwierdził Wojewódzki Sąd Administracyjny w wyroku z dnia 1 grudnia 2005 r. (sygn. akt II SA/Wa 917/2005). Trudności interpretacyjne co do zakresu przetwarzanych danych nie powinny mieć miejsca, gdy przewidują to wprost przepisy prawa, gdyż w takich sytuacjach to przepisy prawa określające odpowiedni zakres danych osobowych, będą miały zastosowanie. O ile jednak brak jest takich unormowań, to zastosowanie powinna znaleźć wyżej wskazana zasada adekwatności zakresu danych do celu ich przetwarzania.

W związku z powyższym, nie można uznać, iż wspólnota mieszkaniowa ma prawo do gromadzenia i przechowywania aktów notarialnych poszczególnych lokali, w których zawarte są dane osobowe ich właścicieli.

11 Czy spółdzielnia mieszkaniowa może za pośrednictwem dozorców doręczać korespondencję kierowaną do członków tej spółdzielni?

Tak, o ile dozorczy posiadają upoważnienie do doręczania korespondencji nadane przez spółdzielnię (administrатора danych), a korespondencja zabezpieczona jest w taki sposób, by uniemożliwić im zapoznanie się z jej treścią.

Uzasadnienie

Zgodnie z art. 26 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.

Obowiązkiem każdego administratora danych – w tym przypadku spółdzielni – jest wydanie upoważnienia dla każdej osoby, która ma dostęp do przetwarzanych przez administratora danych osobowych. Zatem, o ile dozorczy posiadają upoważnienie do przetwarzania danych członków spółdzielni (w związku z doręczaniem im korespondencji) o tyle nie są upoważnieni do zapoznawania się treścią doręczanych pism.

Kwestie dotyczące zabezpieczenia danych osobowych uregulowane zostały w rozdziale 5 ww. ustawy. Na mocy art. 36 ust. 1 ustawy administrator danych (w tym przypadku spółdzielnia) jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Powyższe oznacza to, że spółdzielnia, jako administrator danych członków spółdzielni obowiązana jest podjąć działania mające na celu ochronę ich danych osobowych zawartych w korespondencji do nich kierowanej, poprzez doręczanie jej w taki sposób, aby tylko adresat miał do niej dostęp, np. w kopertach.

Zabezpieczenie tych danych jest tym bardziej istotne z uwagi na fakt, że zgodnie z art. 51 ust. 1 ustawy, kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. W przypadku, gdy sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku (ust. 2). Przepis ten oznacza, że zachowanie sprawcy przestępstwa polega na stworzeniu możliwości dostępu do danych osobom nieupoważnionym i może być popełnione zarówno przez administrującego zbiorem danych, jak i osobę upoważnioną do przetwarzania danych osobowych przez administratora danych.

Należy również zauważyć, że tajemnica korespondencji, jako jedno z podstawowych dóbr osobistych człowieka, korzysta także z ochrony przewidzianej przepisami prawa cywilnego. W związku z czym za jej naruszenie poszkodowany może domagać się zadośćuczynienia za doznaną krzywdę.

Reasumując, stwierdzić należy, że postępowanie spółdzielni jako administratora danych uznać będzie można za zgodne z prawem, o ile dozorczy posiadają będą upoważnienie do doręczania korespondencji nadane przez administratora danych, a korespondencja zabezpieczona zostanie w taki sposób, by uniemożliwić im zapoznanie się z jej treścią.

12 Czy spółdzielnia mieszkaniowa, która jako zabezpieczenie spłaty kredytu, wskazała przelew wierzytelności wpłat członków spółdzielni na fundusz remontów, może udostępnić bankowi dane osobowe osób dokonujących tych wpłat?

Tak, spółdzielnia może, w ramach umowy zawartej z bankiem, udostępnić dane osobowe swoich członków.

Uzasadnienie

Zgodnie z ustawą o ochronie danych osobowych przetwarzanie danych jest zgodne z prawem, gdy administrator danych wskaże co najmniej jedną z przesłanek zezwalających na przetwarzanie danych (art. 23 ust. 1 ustawy). I tak, przetwarzanie danych jest dopuszczalne m.in. wtedy, gdy przepis szczególny zezwala na przetwarzanie danych (pkt 2) bądź, gdy jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą (pkt 5).

Mając na uwadze powołany wyżej przepis należy uznać, że udostępnienie bankowi przez spółdzielnię danych osobowych jej członków znajduje prawne uzasadnienie w art. 23 ust.1

pkt 2 i 5 ustawy (szczególny przepis prawa zezwalający na przetwarzanie danych oraz, gdy przetwarzanie danych jest niezbędne do wypełnienia prawnie usprawiedliwionych celów). Wskazać należy, że przepisem prawa legalizującym udostępnienie danych osobowych jest art. 509 Kodeksu cywilnego, w myśl którego wierzyciel (spółdzielnia) może bez zgody dłużnika (członków spółdzielni) przenieść wierzytelność na osobę trzecią (bank), chyba że sprzeciwiałoby się to ustawie, zastrzeżeniu umownemu albo właściwości zobowiązania (§ 1). Wraz z wierzytelnością przechodzą na nabywcę wszelkie związane z nią prawa, w szczególności roszczenie o zaległe odsetki (§ 2).

Na podstawie umowy o przelew wierzytelności dochodzi do zbycia przez spółdzielnię przedmiotowej wierzytelności na rzecz banku. Zatem zbycie przez spółdzielnię wierzytelności, która przysługuje jej w stosunku do członków będących członkami spółdzielni z tytułu wpłat na fundusz remontowy (a w konsekwencji udostępnienie także danych osobowych członków spółdzielni), mające na celu uzyskanie kredytu na sfinansowanie remontu budynku mieszkalnego stanowi realizację przez administratora (spółdzielnię) prawnie usprawiedliwionego celu, o którym mowa w art. 23 ust. 1 pkt 5 ustawy. Taką podstawą prawną jest pozyskanie danych przez bank.

Biorąc powyższe pod uwagę stwierdzić należy, że spółdzielnia mieszkaniowa, zawierając z bankiem umowę kredytu inwestorskiego w celu sfinansowania kosztów remontu budynku mieszkalnego może w celu zabezpieczenia spłaty tego kredytu udostępnia dane swoich członków.

Na marginesie należy podkreślić, że Generalny Inspektor Ochrony Danych Osobowych nie ma prawa badać kwestii legalności zawarcia przez spółdzielnię umowy z bankiem. Bowiem takie sprawy, zgodnie z art. 1 Kodeksu postępowania cywilnego, są sprawami cywilnymi i powinny być rozpatrywane w postępowaniach prowadzonych przez sądy powszechne. Zatem GIODO może jedynie w ramach przyznanych mu kompetencji badać czy u podstaw udostępnienia przez spółdzielnię i pozyskania przez bank danych osobowych członków spółdzielni znajduje się jedna z określonych w art. 23 ust. 1 ustawy przesłanek legalizujących takie działanie.

13 Czy spółdzielnia mieszkaniowa może publikować na swojej stronie internetowej kierowaną do niej korespondencję zawierającą dane osobowe członka tej spółdzielni?

Nie, gdyż jest to niezgodne z prawem.

Uzasadnienie

Podstawę przetwarzania danych osobowych członków spółdzielni mieszkaniowej przez organy spółdzielni powinny stanowić przepisy ustawy z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych, a w zakresie nie uregulowanym w tych przepisach - ustawy z dnia 16 września 1982 r. Prawo spółdzielcze. W myśl art. 30 ustawy Prawo spółdzielcze, zarząd spółdzielni prowadzi rejestr członków zawierający ich imiona i nazwiska oraz miejsce zamieszkania, do którego dostęp posiadają jedynie wskazane w tym przepisie podmioty, a więc członek spółdzielni, jego małżonek, wierzyciel członka lub spółdzielni. Tym samym opisane powyżej przetwarzanie danych (m.in. ich gromadzenie, przechowywanie, czy udostępnianie) odbywa się w oparciu o przesłankę z art. 23 ust. 1 pkt 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Zgodnie z nią przetwarzanie danych osobowych jest dopuszczalne, gdy zezwala na to szczególny przepis prawa. Odniesienie do ustawy o ochronie danych osobowych jest istotne, z tego względu, że zawiera ona ogólne zasady wykorzystywania (przetwarzania) danych osobowych, których należy przestrzegać. A zatem skoro zezwala ona na wykorzystywanie danych osobowych m.in. wtedy, gdy szczególny (branżowy) przepis prawa o tym stanowi, to jest to działanie legalne.

Jednocześnie spółdzielnia jest – w świetle przepisów ustawy o ochronie danych osobowych – administratorem danych swoich członków, czyli podmiotem odpowiedzialnym za ich właściwe wykorzystywanie i zabezpieczenie m.in. przed nieudostępnianiem osobom nieuprawnionym.

Upublicznienie zatem przez spółdzielnię, na jej stronach internetowych, pisma zawierającego dane osobowe jej członka niewątpliwie wykracza poza zakres uprawnienia spółdzielni. Żaden bowiem przepis prawa, na podstawie którego działają spółdzielnie, nie daje jej prawa do takiego upublicznienia. Ponadto, jako administrator danych spółdzielnia w ten sposób dopuszcza do zapoznania się z upublicznionej informacjami przez osoby nieupoważnione – nieograniczony krąg odbiorców (szeroka rzesza internautów).

W sytuacji upublicznienia danych osobowych bez podstawy prawnej ustawa o ochronie danych osobowych przewiduje odpowiedzialność karną w postaci grzywny, kary ograniczenia wolności albo pozbawienia wolności do lat 2 (art. 51 ust. 1 ustawy).

Dodatkowo informuję, że tajemnica korespondencji pozostaje także pod ochroną przepisów ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny, odnoszących się do ochrony dóbr osobistych (art. 23 i 24).

14 Czy spółdzielnia mieszkaniowa ma prawo udostępnić informacje dotyczące rozliczenia indywidualnych kosztów zużycia ciepła w poszczególnych lokalach?

Tak, o ile informacje o zużyciu ciepła są zawarte w prowadzonym przez spółdzielnię rejestrze członków i udostępnione będą jedynie osobie uprawnionej

Uzasadnienie

Informacje o indywidualnych kosztach ogrzewania danego mieszkania, chociażby w połączeniu z numerem lokalu, będą stanowiły dane osobowe, gdyż na ich podstawie możliwe jest ustalenie tożsamości osoby fizycznej, w tym przypadku właściciela lokalu. I choć zasady wykorzystywania danych osobowych reguluje ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, to wówczas, gdy przepisy odrębne regulują kwestie przetwarzania danych osobowych w określonym sektorze, mają one pierwszeństwo stosowania.

Uprawnienia i obowiązki organów oraz członków spółdzielni mieszkaniowej określone zostały w ustawie z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych, a w zakresie w niej uregulowanym zastosowanie znajdują rozwiązania przewidziane w ustawie z dnia 16 września 1982 r. Prawo spółdzielcze, a także w statucie spółdzielni i sporządzonym na jego podstawie regulaminie bądź w uchwałach podejmowanych przez organy spółdzielni mieszkaniowych.

Powołane przepisy stanowią m.in. (art. 30 Prawa spółdzielczego), że w prowadzonym przez spółdzielnię mieszkaniową rejestrze członków znajdują się ich imiona i nazwiska oraz miejsce zamieszkania (w odniesieniu do członków będących osobami prawnymi - ich nazwę i siedzibę), wysokość zadeklarowanych i wniesionych udziałów, wysokość wniesionych wkładów, ich rodzaj, jeżeli są to wkłady niepieniężne, zmiany tych danych, data przyjęcia w poczet członków, data wypowiedzenia członkostwa i jego ustania, a także inne dane przewidziane w statucie. Rejestr członków spółdzielni, obok informacji wyraźnie wskazanych w powołanym przepisie, może zawierać także „inne dane przewidziane w statucie”. Zatem - o ile statut tak stanowi - w rejestrze mogą się znaleźć informacje dotyczące rozliczania kosztów ogrzewania poszczególnych lokali.

Stwierdzić jednak należy, że wgląd do danych zawartych w rejestrze spółdzielni mają jedynie członek spółdzielni, jego małżonek oraz wierzyciel członka lub spółdzielni. To te osoby – jako uprawnione do przeglądania rejestru – wymienia art. 30 Prawa spółdzielczego. Jednocześnie stanowi on podstawę prawną legalizującą przetwarzanie danych osobowych, które w tym przypadku polega na ich udostępnieniu (tym samym spełniona jest przesłanka wskazana

w art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych, czyli istnienie zezwalającego na to szczególnego przepisu prawa, który ma pierwszeństwo stosowania przed ustawą o ochronie danych osobowych).

15 Czy w statucie spółdzielni można wskazać, że w rejestrze członków odnotowywane będą informacje o zaległościach z tytułu wydatków związanych z członkostwem wraz z imieniem i nazwiskiem oraz adresem zamieszkania zadłużonego członka?

Tak, takie działanie spółdzielni będzie zgodne z przepisami prawa.

Uzasadnienie

Podstawą przetwarzania danych osobowych członków spółdzielni przez organy spółdzielni są przepisy o spółdzielniach mieszkaniowych, a w zakresie nieuregulowanym w tych przepisach w ustawie prawo spółdzielcze oraz w statucie i sporządzonych w oparciu o statut regulaminach i uchwałach podejmowanych przez te organy. W kwestii majątku spółdzielni stwierdzić należy, że spółdzielnia jest dobrowolnym zrzeszeniem nieograniczonej liczby osób, o zmiennym składzie osobowym i zmiennym funduszu udziałowym, które w interesie swoich członków prowadzi wspólną działalność gospodarczą (art. 1 § 1 prawa spółdzielczego). Majątek spółdzielni jest prywatną własnością jej członków. Informacje o zadłużeniach czynszowych członków spółdzielni mieszkaniowej są informacjami bezpośrednio dotyczącymi majątku członków spółdzielni (art. 3 prawa spółdzielczego).

Posiadają oni zatem interes faktyczny w uzyskaniu informacji dotyczących tego majątku, zaś uprawnienie członków spółdzielni mieszkaniowej do dostępu do informacji o zadłużeniu czynszowym innych członków spółdzielni wynika z cytowanych z przepisów. Tryb i forma udostępniania tych informacji powinna być szczegółowo uregulowana w statucie spółdzielni. Możliwe jest bowiem umieszczenie informacji o zadłużeniach czynszowych wraz z danymi osobowymi osób zadłużonych, w rejestrze członków spółdzielni.

Zgodnie z art. 30 prawa spółdzielczego, rejestr członków spółdzielni, obok wyraźnie wskazanych w tym przepisie informacji, może zawierać także „inne dane przewidziane w statucie” (art. 30 prawa spółdzielczego). Do statutu spółdzielni mogą być zatem wprowadzone postanowienia, stosownie do których informacje o zaległościach z tytułu wydatków związanych z członkostwem w spółdzielni, zamieszczane będą w rejestrze jej członków. Należy zaznaczyć, iż w tej sytuacji dostęp do tych danych będą mieć jedynie osoby uprawnione do przeglądania rejestru, a są nimi – zgodnie z przepisami prawa członek spółdzielni, jego małżonek i wierzyciel członka lub spółdzielni.

Zatem, podstawą prawną do udostępnienia danych zawartych w rejestrze członków spółdzielni jest – o ile zostaną spełnione powyższe warunki - przepis prawa, który stanowi jedną z podstaw przetwarzania danych wynikających z ustawy o ochronie danych osobowych (czyli art. 23 ust. 1 pkt 2 ustawy o ochronie danych osobowych).

16 Czy Straż Miejska ma prawo pozyskać, na potrzeby skierowania do sądu wniosku o ukaranie, informacje o dochodach, stanie majątkowym czy też liczbie osób pozostających na utrzymaniu osoby, która popełniła wykroczenie?

Tak, Straż Miejska ma prawo pozyskiwać ww. dane na potrzeby skierowania do sądu wniosku o ukaranie.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych określa jedynie ogólne zasady przetwarzania danych osobowych, zaś ich skonkretyzowanie znajduje się w innych przepisach prawa. W związku z tym opisywaną sprawę należy rozpatrywać m.in. w oparciu

o ustawę o strażach gminnych, ustawę o ruchu drogowym czy też kodeksu postępowania w sprawach o wykroczenia.

I tak, zgodnie z art. 10a ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych, straż w celu realizacji ustawowych zadań może przetwarzać dane osobowe, z wyłączeniem danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, bez wiedzy i zgody osoby, której dane te dotyczą, uzyskane: w wyniku wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia; z rejestrów, ewidencji i zbiorów, do których straż posiada dostęp na podstawie odrębnych przepisów.

Wykonując swoje zadania strażnik – na podstawie art. 12 ust. 1 pkt 5 ustawy strażach gminnych - ma prawo do dokonywania czynności wyjaśniających, kierowania wniosków o ukaranie do sądu, oskarżania przed sądem i wnoszenia środków odwoławczych - w trybie i zakresie określonych w ustawie z dnia 24 sierpnia 2001 r. - Kodeks postępowania w sprawach o wykroczenia. Zgodnie z art. 57 § 2 Kodeksu postępowania w sprawach o wykroczenia, wniosek o ukaranie powinien zawierać: imię i nazwisko oraz adres obwinionego, a także inne dane niezbędne do ustalenia jego tożsamości; określenie zarzucanego obwinionemu czynu ze wskazaniem miejsca, czasu, sposobu i okoliczności jego popełnienia; wskazanie dowodów; imię i nazwisko oraz podpis sporządzającego wniosek, a także adres gdy wniosek pochodzi od pokrzywdzonego.

Zgodnie natomiast z art. 57 § 3 Kodeksu postępowania w sprawach o wykroczenia, wniosek o ukaranie składany przez oskarżyciela publicznego powinien ponadto zawierać wskazanie: przepisów, pod które zarzucany czyn podpada; miejsca zatrudnienia obwinionego oraz, w miarę możliwości, danych o jego warunkach materialnych, rodzinnych i osobistych; pokrzywdzonych, o ile takich ujawniono; wysokości wyrządzonej szkody; stanowiska osoby sporządzającej wniosek; sądu właściwego do rozpoznania sprawy; danych dotyczących uprzedniego skazania obwinionego za podobne przestępstwo lub wykroczenie, jeżeli oskarżyciel powołuje się na tę okoliczność.

Wyżej wskazane przepisy prawa precyzują więc, jaki zakres danych i informacji o osobie fizycznej może być przetwarzany przez straż gminną (miejską). Instytucja ta jest zatem uprawniona do przetwarzania danych osobowych w ww. zakresie. Jednakże, wskazać należy, że informacje o warunkach materialnych, rodzinnych i osobistych osoby podejrzanej o popełnienie wykroczenia powinny być zawarte we wniosku o ukaranie wyłącznie „w miarę możliwości” tj. o ile uda się je pozyskać. Odmowa zaś przyjęcia mandatu karnego powoduje konieczność ustalenia przez straż gminną (miejską) informacji niezbędnych dla sporządzenia wniosku o ukaranie i następnie skierowanie przedmiotowej sprawy na drogę postępowania sądowego.

17 Czy dane osobowe przetwarzane przez straż miejską, zawarte w dokumentach papierowych, takich jak notatniki służbowe, notatki urzędowe, czy wypełnione blankiety mandatów karnych stanowią odrębne, od zarejestrowanych u GODO, zbiory danych w rozumieniu ustawy o ochronie danych osobowych?

To zależy od kryterium podziału, jaki przyjmie straż miejska, jako administrator danych.

Uzasadnienie

Jako administrator danych, straż miejska, ma obowiązek zarejestrować zbiory danych u Generalnego Inspektora Ochrony Danych Osobowych, gdyż nie zachodzi żadna z okoliczności wskazanych w art. 43 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwalniających ją z tego obowiązku. Przykładowo, zarejestrowanymi

u Generalnego Inspektora Ochrony Danych Osobowych w jawnym rejestrze zbiorów danych osobowych, prowadzonymi przez straż miejską zbiorami są: zbiór danych osobowych przetwarzanych w postępowaniu mandatowym, skargowym i interwencjach oraz zbiór danych osobowych właścicieli lub posiadaczy pojazdów usuniętych z drogi na podstawie art. 130a lub 50a ustawy Prawo o ruchu drogowym.

W rozumieniu zaś art. 7 pkt 1 ustawy o ochronie danych osobowych zbiorem danych jest zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. Nie jest zatem istotne, czy zestaw ten jest scentralizowany czy rozproszony, jednolity lub podzielony funkcjonalnie. Ważne jest natomiast, aby w tym zestawie można było odszukać dane osobowe na podstawie określonych kryteriów, np. alfabetycznego czy chronologicznego. Przykładem rozproszonego zbioru danych jest zestaw informacji o pracownikach, zgromadzony w związku z ich zatrudnieniem i świadczeniem przez nich pracy, wykorzystywany przez różne komórki organizacyjne pracodawcy, zarówno w systemach informatycznych, jak i w formie papierowej.

Straż miejska, zgodnie z art. 10a ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych, przetwarza dane osobowe sprawców wykroczeń, uzyskując je od osoby, której one dotyczą w wyniku wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia oraz z rejestrów, ewidencji i zbiorów, do których straż posiada dostęp na podstawie odrębnych przepisów, np. z Centralnej Ewidencji Ludności. Dane te, oprócz tego, że są zapisywane w systemie informatycznym, są wprowadzane do różnych dokumentów papierowych, np. notatników służbowych, notatek służbowych, wypełnionych blankietów mandatów karnych.

Zatem, w świetle ustawy o ochronie danych osobowych, zbiór danych mogą tworzyć dane osobowe przetwarzane jednocześnie w systemach informatycznych, jak i w postaci dokumentów papierowych. W każdym przypadku przetwarzania danych osobowych ich administrator powinien dokonać oceny, czy dane osobowe tworzą samodzielny zbiór, czy też ze względu na funkcjonalną organizację zastosowaną przez administratora danych stanowią część istniejącego zbioru danych. Tym samym straż miejska, gromadząc dane np. w notatnikach strażników miejskich, może stworzyć odrębny zbiór takich danych lub też przetwarzać te dane w zbiorach zgłoszonych do rejestracji GIODO.

18 Czy zgodne z prawem jest działanie jednostek Straży Miejskiej polegające na wykonywaniu fotografii osobom zatrzymanym w celu doprowadzenia tych osób do izby wytrzeźwień?

Nie, bowiem takie działanie jednostek Straży Miejskiej nie ma podstaw prawnych.

Uzasadnienie:

Wizerunek człowieka, jako jego dobro osobiste, chroniony jest przepisami ustawy z 23 kwietnia 1964 r. Kodeks cywilny, w szczególności jej art. 23 i 24, zaś w kwestii ewentualnego naruszenia dóbr osobistych orzekają sądy cywilne w trybie wynikającym z przepisów ustawy z 17 listopada 1964 r. Kodeks postępowania cywilnego.

Rozważając zatem możliwość wykonywania przez Straż Miejską zdjęć osobom zatrzymanym w celu doprowadzenia do izby wytrzeźwień należy mieć na uwadze, iż działanie takie - nie poprzedzone zgodą osoby, której zdjęcie zostało wykonane - może narazić administratora danych (czyli w tym przypadku Straż Miejską) na zarzut naruszenia prawnie chronionych dóbr osobistych.

Jednocześnie dodać trzeba, że jest to również niezgodne z punktu widzenia przepisów ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych. Bowiem na gruncie ustawy o ochronie danych osobowych dopuszczalność przetwarzania danych osobowych tzw. zwykłych (jak np. imię, nazwisko, adres zamieszkania) uzależniona jest od spełnienia jednej z przesłanek

wymienionych w art. 23 ust. 1 pkt 1 - 5 ustawy. Natomiast przetwarzanie danych szczególnie chronionych, do których - zgodnie z art. 27 ust. 1 ustawy - należą m. in. dane ujawniające pochodzenie rasowe lub etniczne, dane o stanie zdrowia, czy nałogach jest - co do zasady - zakazane. Wyjątki od ogólnego zakazu ich przetwarzania zostały natomiast określone w ust. 2 powołanego przepisu (art. 27 ust. 2 pkt 1 - 10).

Zgodnie natomiast z zasadą legalności i adekwatności (wyrażoną w art. 26 ust. 1 pkt 1 i 3 cytowanej ustawy) administrator danych powinien przetwarzać w zgodzie z obowiązującym prawem tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na cel zbierania danych. W myśl powołanych przepisów art. 26 ustawy, administrator jest obowiązany zapewnić, aby dane te były przetwarzane zgodnie z prawem, oraz aby były one merytorycznie poprawne i adekwatne w stosunku do celu przetwarzania. Zasada legalnego przetwarzania danych osobowych oznacza konieczność niewykraczania poza odpowiednie regulacje ustawowe, czy wynikające z innych źródeł prawa. Adekwatność danych w stosunku do celu ich przetwarzania powinna być natomiast rozumiana jako równowaga pomiędzy dobrem osoby, której dane dotyczą a interesem administratora danych. Oznacza to, że administrator danych nie może przetwarzać danych w zakresie szerszym niż niezbędny dla osiągnięcia zamierzonego celu, jak również danych o większym, niż uzasadniony tym celem, stopniu szczegółowości. Równowaga będzie zachowana, jeżeli administrator zażąda danych tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane (wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 1 grudnia 2005 r. (sygn. akt II SA/Wa 917/2005).

Dlatego pozyskiwanie danych osób zatrzymywanych celem ich doprowadzenia do izby wytrzeźwień, poprzez wykonywanie im fotografii nie jest adekwatne dla celów realizacji ustawowo określonych zadań straży gminnych (miejskich).

Ponadto, art. 10a ustawy z 29 sierpnia 1997 r. o strażach gminnych stanowi, iż straż w celu realizacji ustawowych zadań może przetwarzać dane osobowe, z wyłączeniem danych (szczególnie chronionych) ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym. Powyższe dane (prócz ww. danych szczególnie chronionych) mogą być przetwarzane bez wiedzy i zgody osoby, której dane te dotyczą. Uzyskane mogą zostać w wyniku: 1) wykonywania czynności podejmowanych w postępowaniu w sprawach o wykroczenia, 2) z rejestru, ewidencji i zbiorów, do których straż posiada dostęp na podstawie odrębnych przepisów.

Biorąc zatem pod uwagę, iż wizerunek osób zatrzymywanych w celu doprowadzenia do izby wytrzeźwień może prowadzić do ujawnienia pochodzenia rasowego lub etnicznego tych osób, jak również w niektórych przypadkach danych o ich stanie zdrowia, czy nałogach, uznać należy, że przetwarzanie takich danych przez straż miejską może nastąpić jedynie za wiedzą i zgodą tych osób.

19 Czy stráže miejskie są upoważnione do pozyskiwania - poprzez "protokoły przesłuchania podejrzanego o popełnienie wykroczenia";- od osób podejrzanых o popełnienie wykroczenia, danych o stanie ich zdrowia?

Jak wynika ze skarg, wpływających do Biura Generalnego Inspektora Ochrony Danych Osobowych, stráže miejskie pozyskują - poprzez "protokoły przesłuchania podejrzanego o popełnienie wykroczenia"- od osób podejrzanых o popełnienie wykroczenia, dane o stanie ich zdrowia. Wśród zebranych w ten sposób danych znajdują się w szczególności informacje o "wadach psychicznych i fizycznych, ułomnościach". Dane te umieszczane są następnie we wnioskach o ukaranie - kierowanych przez stráže miejskie, występujące jako oskarżyciele publiczni, do sądów grodzkich.

OCHRONA DANYCH OSOBOWYCH

Z dokonanych przez Generalnego Inspektora ustaleń wynika, iż straże miejskie wykorzystują do gromadzenia danych formularze (druki) stosowane przez Policję (są one "pobierane" przez straże miejskie bezpośrednio od współpracujących z nimi komend Policji), bądź też formularze (druki) wzorowane na tych stosowanych przez Policję.

Tymczasem, zbieranie danych o stanie zdrowia fizycznego i psychicznego osób podejrzanych o popełnienie wykroczenia, będące wynikiem wykorzystywania powyższych formularzy (druków) przez straże miejskie, wydaje się nieuprawnione ze względu na brzmienie art. 10a ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. Nr 123, poz. 779 z późn. zm.).

Stosownie do treści tego przepisu, straż miejska w celu realizacji swoich ustawowych zadań może przetwarzać dane osobowe, z wyłączeniem danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, bez wiedzy i zgody osoby, której dane dotyczą, uzyskane w wyniku czynności podejmowanych w postępowaniu w sprawach o wykroczenia.

Zauważyć ponadto należy, iż art. 57 § 2 i 3 ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia (Dz. U. Nr 106, poz. 1148 z późn. zm.), określający warunki formalne, jakim musi odpowiadać wniosek o ukaranie nie przewiduje, aby we wniosku zamieszczane były informacje o stanie zdrowia obwinionego. W art. 57 § 3 pkt 2 tej ustawy wskazuje się bowiem wyłącznie, iż we wniosku powinny znaleźć się informacje dotyczące miejsca zatrudnienia obwinionego oraz, w miarę możliwości, danych o jego warunkach materialnych, rodzinnych i osobistych. Brak jest więc wymogu umieszczania danych o stanie zdrowia. Nawet gdyby uznać, iż - jak w wyjaśnieniach podnoszą komendanci straży miejskich - "jednym z warunków osobistych sprawcy ['element' wniosku o ukaranie określony w ww. art. 57 § 3 pkt 2 kpw] jest jego stan zdrowia", to o niedopuszczalności pozyskiwania przez straże miejskie tej kategorii danych przesądza ww. przepis art. 10a ustawy o strażach gminnych. (Podkreślenia przy tym wymaga, iż brak we wniosku danych o stanie zdrowia podejrzanego, przy wątpliwym założeniu, że jest to kategoria mieszcząca się w pojęciu "warunków osobistych sprawcy", nie powinien, ze względu na brzmienie art. 57 § 3 pkt 2 kpw, skutkować zwróceniem wniosku o ukaranie oskarżycielowi publicznemu (straży miejskiej) na podstawie art. 59 § 1 kpw, czyli ze względu na braki formalne. Zauważyć bowiem należy, iż informacje o warunkach materialnych, rodzinnych i osobistych osoby podejrzanego o popełnienie wykroczenia powinny zostać zawarte we wniosku wyłącznie "w miarę możliwości". Umieszczenie we wniosku tego rodzaju informacji nie jest więc niezbędne.)

Istotne znaczenie ma również fakt, iż regułą jest, że z przekazywanej do sądów dokumentacji (wniosków o ukaranie) straże miejskie sporządzają kopie "do własnego użytku". Oznacza to, iż straże miejskie łamią przepis art. 10a ustawy o strażach gminnych nie tylko pozyskując dane o stanie zdrowia celem wykorzystania w związku ze skierowaniem stosownego wniosku do sądu, ale również przechowując tego rodzaju dane we własnych zbiorach (np. "zbiorach wtórników wniosków o ukaranie osób podejrzanych o popełnienie wykroczeń").

Niezależnie od powyższego wskazać należy, iż o ile w stosowanych przez straże miejskie formularzach wniosków o ukaranie, stosownie do treści art. 57 § 3 pkt 7 1 kpw, znajduje się rubryka "Uprzednie kary za podobne przestępstwa lub wykroczenia", o tyle już w formularzach protokołów przesłuchania osoby podejrzanego o popełnienie wykroczenia częstokroć znajduje się rubryka - "Karalność i dane odbycia kary". Konsekwencją zastosowania tego rodzaju ogólnego (nieprecyzyjnego) zapisu może być pozyskiwanie od podejrzanych o popełnienie wykroczenia danych w zbyt szerokim zakresie, niż wynika to z ww. przepisu art. 57 § 3 pkt 7 kpw, a mianowicie danych na temat wszelkich skazań za popełnione przez osobę przesłuchiwaną przestępstwa lub wykroczenia.

W związku z powyższym, Generalny Inspektor Ochrony Danych Osobowych, zasygnalizował

ww. problem Ministrowi Spraw Wewnętrznych i Administracji. Zwrócił się również do Generalnego Inspektora, Komendanta Głównego Policji, jako sprawującego na podstawie art. 9 ust. 1 ustawy o strażach gminnych fachowy nadzór nad działalnością straży miejskich (gminnych), z prośbą o podjęcie działań skutkujących wyeliminowaniem opisanej powyżej praktyki zbierania przez strażę danych osób podejrzanych o popełnienie wykroczenia, w zakresie szerszym, niż przewidziany przepisami ustawy o strażach gminnych oraz ustawy Kodeks postępowania w sprawach o wykroczenia, w szczególności zaś o rozważenie zasadności wprowadzenia, zgodnych z przepisami ww. ustaw, jednolitych formularzy (druków) "protokołów przesłuchania osoby podejrzanej o popełnienie wykroczenia" oraz wniosków o ukaranie, którymi w swojej działalności posługiwałyby się strażę miejskie.

20 Czy od rodziców zapisujących dziecko do świetlicy szkolnej można żądać podania takich danych, jak ich miejsce zatrudnienia, stanowisko oraz wynagrodzenie?

Nie, gdyż przepisy, na podstawie których działają placówki oświatowe, nie dają podstawy do pozyskiwania takich informacji, a poza tym byłyby one zbędne dla realizacji celu, jakim jest zapisanie dziecka do świetlicy szkolnej.

Uzasadnienie

Przetwarzanie danych osobowych przez placówki oświatowe odbywa się przede wszystkim na podstawie przepisów szczególnych w stosunku do ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, zwłaszcza zaś ustawy z dnia 7 września 1991 r. o systemie oświaty oraz wydanych na jej podstawie aktów wykonawczych, m.in. rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji.

Powołane rozporządzenie stanowi, jakiego rodzaju dokumentację prowadzi szkoła i jakie dane osobowe ona zawiera.

Do księgi ewidencji dzieci podlegających obowiązkowi przygotowania przedszkolnego i obowiązkowi szkolnemu, zamieszkałych w obwodzie szkoły, wpisuje się np., według roku urodzenia, imię (imiona) i nazwisko, datę i miejsce urodzenia, numer PESEL oraz adres zamieszkania dziecka, a także imiona i nazwiska rodziców (prawnych opiekunów) oraz adresy ich zamieszkania (§ 3a ust. 1 i 2 pkt 1, § 3b ust. 1 i 2).

Z kolei do księgi uczniów wpisuje się imię (imiona) i nazwisko, datę i miejsce urodzenia, numer PESEL oraz adres zamieszkania ucznia, imiona i nazwiska rodziców (prawnych opiekunów) i adresy ich zamieszkania, a także datę przyjęcia ucznia do szkoły oraz klasę, do której go przyjęto. Odnotowuje się w niej również datę ukończenia szkoły albo datę i przyczynę opuszczenia szkoły przez ucznia (§ 4 ust. 1 i 2).

Omawiane rozporządzenie stanowi też, jakie dane powinny być zawarte w dzienniku lekcyjnym (zgodnie z § 7 ust. 1 są to m.in.: nazwiska i imiona uczniów, daty i miejsca urodzenia oraz adresy ich zamieszkania, imiona i nazwiska rodziców lub prawnych opiekunów i adresy ich zamieszkania), a jakie w dzienniku zajęć w świetlicy (są to m.in. takie informacje, jak: imiona i nazwiska uczniów korzystających ze świetlicy, klasa, do której uczęszczają czy obecność uczniów na poszczególnych godzinach zajęć).

Z przytoczonych powyżej przepisów nie wynika, by placówka oświatowa na potrzeby zapisania dziecka do świetlicy szkolnej mogła żądać od rodziców takich danych, jak ich miejsce zatrudnienia, stanowisko oraz wynagrodzenie. Tym samym brak jest podstawy prawnej do przetwarzania (m.in. gromadzenia) takich danych osobowych. Ich pozyskiwanie może zaś prowadzić do naruszenia art. 26 ustawy o ochronie danych osobowych, zgodnie z którym, administrator danych (w tym przypadku szkoła) przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą,

a w szczególności jest obowiązany zapewnić, aby dane te były: przetwarzane zgodnie z prawem (pkt 1), zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami (pkt 2), merytorycznie poprawne i adekwatne do celów, w jakich są przetwarzane (pkt 3).

Na konieczność stosowania przy przetwarzaniu danych osobowych tzw. zasady adekwatności, wskazał również Wojewódzki Sąd Administracyjny, który w wyroku z 1 grudnia 2005 r. (sygn. akt II SA/Wa 917/2005) orzekł, iż *„Adekwatność danych w stosunku do celu ich przetwarzania powinna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swymi danymi a interesem administratora danych. Równowaga będzie zachowana, jeżeli administrator zażąda danych tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane”*.

21 Czy placówki oświatowe są zobowiązane do zawarcia pisemnej umowy powierzenia przetwarzania danych osobowych z przedsiębiorcą, który udostępnia im system informatyczny do prowadzenia e-dzienników?

Tak, gdyż ustawa o ochronie danych osobowych wymaga, aby umowa powierzenia przetwarzania danych zawarta była w formie pisemnej.

Uzasadnienie

Na podstawie art. 31 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, administrator danych (w tym np. placówka oświatowa) może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Niezbędnymi elementami tej umowy jest określenie celu, w jakim podmiot, któremu powierzono przetwarzanie danych może je przetwarzać oraz zakresu powierzonych do przetwarzania danych. Podmiot ten może bowiem przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Powierzenie przetwarzania danych na podstawie umowy, o której stanowi art. 31 ustawy, w określonym w niej celu, jest działaniem prawnie dopuszczalnym i nie stanowi nieuprawnionego udostępnienia danych przez ich administratora innemu podmiotowi.

Placówki oświatowe mogą prowadzić dzienniki elektroniczne (e-dzienniki) na podstawie rozporządzenia Ministra Edukacji Narodowej i Sportu z dnia 19 lutego 2002 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji. Jeśli placówka oświatowa korzysta z oferowanego jej przez przedsiębiorcę systemu informatycznego w celu prowadzenia elektronicznych dzienników, w których przetwarzane są dane osobowe uczniów, ich przedstawicieli ustawowych oraz nauczycieli, powinna zawrzeć z nim pisemną umowę powierzenia przetwarzania danych osobowych. Nie spełnia wymogów z art. 31 ustawy o ochronie danych osobowych umowa udzielenia licencji na korzystanie z systemu informatycznego zawarta z chwilą otrzymania przez placówkę oświatową kodu dostępu do systemu informatycznego. Mimo, że placówka oświatowa powierza przedsiębiorstwu przetwarzanie danych osobowych w celu wykonania umowy to brak formy pisemnej dyskwalifikuje ją jako umowę powierzenia z art. 31 ww. ustawy. Nie wystarczy także pisemna umowa hostingowa, jeśli nie zawiera ona postanowień, z których wynikałoby iż na ich podstawie powierzono przetwarzanie danych osobowych w celu wykonania tej umowy.

W związku z powyższym placówki oświatowe są zobowiązane do podpisania umowy powierzenia przetwarzania danych z przedsiębiorcą, który udostępnia im system informatyczny do prowadzenia e-dzienników.

22 Czy mogę uzyskać od operatora telekomunikacyjnego wykaz rozmów przychodzących na mój telefon?

Nie, gdyż nie ma podstaw prawnych do pozyskania takiego wykazu.

Uzasadnienie

Ustawa o ochronie danych osobowych zawiera jedynie ogólne zasady przetwarzania danych osobowych, zaś ich skonkretyzowanie znajduje się w szczególnych przepisach, które mają pierwszeństwo stosowania.

Wobec powyższego w tej sytuacji znajdują zastosowanie przepisy ustawy z 16 lipca 2004r. Prawo telekomunikacyjne.

I tak, zgodnie z art. 80 ust. 1 prawa telekomunikacyjnego, dostawca publicznie dostępnych usług telekomunikacyjnych dostarcza abonentowi nieodpłatnie z każdą fakturą podstawowy wykaz wykonanych usług telekomunikacyjnych zawierający informację o zrealizowanych płatnych połączeniach z podaniem, dla każdego typu połączeń, ilości jednostek rozliczeniowych odpowiadającej wartości zrealizowanych przez abonenta połączeń.

Ponadto, dostawca publicznie dostępnych usług telekomunikacyjnych dostarcza na żądanie abonenta szczegółowy wykaz wykonanych usług telekomunikacyjnych, za który może być pobierana opłata w wysokości określonej w cenniku (ust. 2). Szczegółowy wykaz wykonanych usług telekomunikacyjnych powinien zawierać informację o zrealizowanych płatnych połączeniach, z podaniem, dla każdego połączenia: numeru wywoływanego, daty oraz godziny rozpoczęcia połączenia, czasu jego trwania oraz wysokości opłaty za połączenie z wyszczególnieniem ceny brutto i netto (ust. 3).

Powyższy przepis wskazuje zatem zakres danych, które muszą być udostępniane abonentowi przez dostawcę usług telekomunikacyjnych jak i mogą być udostępnione na jego żądanie. Zwrócić jednocześnie należy uwagę, iż ww. informacje zostały ujęte w katalogu zamkniętym, a tym samym ustawodawca nie przewidział możliwości udostępnienia abonentowi danych dotyczących połączeń przychodzących.

Ponadto zwrócić należy również uwagę, na art. 159 ust. 1 Prawa telekomunikacyjnego, który stanowi, że tajemnica komunikowania obejmuje m.in. dane dotyczące użytkownika, treść indywidualnych komunikatów, dane transmisyjne, dane o lokalizacji czy dane o próbach uzyskania połączenia między zakończeniami sieci. Natomiast art. 180d tej samej ustawy, wskazuje, że przedsiębiorcy telekomunikacyjni są obowiązani m.in. do utrwalania oraz do udostępniania powyższych danych uprawnionym podmiotom (m.in. Policji, Straży Granicznej czy Agencji Bezpieczeństwa Wewnętrznego) na własny koszt, a także sądowi i prokuratorowi, na zasadach i przy zachowaniu procedur określonych w przepisach odrębnych.

Z powyższych przepisów wynika uprawnienie abonenta do uzyskania od operatora telekomunikacyjnego wykazu jego rozmów wychodzących wykonywanych z danego numeru telefonicznego, natomiast w odniesieniu do połączeń przychodzących uznać należy, iż wszelkie informacje z nimi związane będzie mogła uzyskać osoba wykonująca te połączenia, jak również podmioty uprawnione na mocy przepisów ustawowych w ściśle określonym celu i zakresie. Odmienne traktowane są sytuacje, o których mowa w art. 171 (szczególnie ust. 7 i 9) Prawa telekomunikacyjnego.

23 Czy zgoda abonenta na umieszczenie jego danych osobowych w książce telefonicznej może być wyrażona w każdym czasie?

Nie, gdyż, zgodnie z ustawą Prawo telekomunikacyjne, wyraźna zgoda abonenta powinna być wyrażona wyłącznie przed dokonaniem czynności zamieszczenia danych osobowych w książce telefonicznej, natomiast może być w każdym czasie cofnięta.

Uzasadnienie

Kwestię związaną z zamieszczaniem i udostępnianiem (są to formy przetwarzania) danych osobowych abonentów w książkach telefonicznych, zarówno w formie papierowej, jak i elektronicznej, regulują szczególne wobec ustawy o ochronie danych osobowych przepisy

OCHRONA DANYCH OSOBOWYCH

ustawy – Prawo telekomunikacyjne. Ustawa o ochronie danych osobowych zawiera bowiem jedynie ogólne zapisy odnoszące się m.in. do tego, jakie warunki należy spełnić, aby wykorzystywanie danych osobowych było legalne. W sytuacji natomiast, gdy są szczególne przepisy prawa regulujące dane zagadnienie, należy się do nich odwołać.

Przepisy Prawa telekomunikacyjnego jednoznacznie wskazują, że zamieszczenie w spisie danych identyfikujących abonenta będącego osobą fizyczną może nastąpić wyłącznie po uprzednim wyrażeniu przez niego zgody na dokonanie tych czynności (art. 169 ust. 3). Tym samym niedopuszczalna jest sytuacja, w której operator telekomunikacyjny w pierwszej kolejności zamieści dane abonenta w spisie danych powszechnie dostępnych, a później poprosi o jego zgodę. Ponadto, zgoda abonenta nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści (art. 174 pkt 1), co oznacza, że powinna być wyrażona świadomie i wyraźnie. Istnieje również możliwość wyrażenia zgody drogą elektroniczną, pod warunkiem jej utrwalenia i potwierdzenia przez użytkownika. Operator telekomunikacyjny powinien bowiem dla celów dowodowych posiadać zgodę abonenta utrwaloną w taki sposób, iż okoliczność jej wyrażenia nie budziłaby wątpliwości - np. dopuszczalna jest sytuacja, w której operator przedstawi nagranie rozmowy telefonicznej z abonentem, z którego wynika wprost, iż zgoda taka została wyrażona. Warto zauważyć, iż raz wyrażona przez abonenta zgoda na umieszczenie danych w powszechnym spisie może być wycofana w każdym czasie, w sposób prosty i wolny od opłat – stosownie do art. 174 pkt 3 Prawa telekomunikacyjnego.