Emilia Szczęsna https://orcid.org/0000-0002-8159-5928
Akademia Humanistyczno-Ekonomiczna w Łodzi, Wydział Zamiejscowy w Sieradzu

Unijne przepisy o ochronie danych osobowych w jednostkach samorządu terytorialnego

Wprowadzenie

Zatrudnienie inspektora ochrony danych osobowych, pozyskiwanie zgody na przetwarzanie danych, obowiązkowe zgłaszanie naruszeń i powiadomienie podmiotu zainteresowanego, uściślenie obowiązków podmiotów przetwarzających dane oraz korzystanie ze zmienionych przepisów odnoszących się do międzynarodowego przekazywania danych osobowych to kilka nowych zasad, z którymi pół roku temu musiały się zmierzyć między innymi jednostki samorządu terytorialnego na mocy unijnego Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO). Nowe regulacje dotknęły wszystkich dziedzin działalności jednostek samorządowych, dla których gromadzenie i przetwarzanie danych osobowych jest niezbędne do realizacji wyznaczonych celów i zadań. Najbardziej odczuwalne zmiany to te, które są związane z zaplanowaniem dodatkowych środków w budżecie, a do nich niewątpliwie należy instytucja inspektora ochrony danych osobowych (dalej: IODO). Liczba inspektorów w danej gminie jest uzależniona od liczby jednostek podlegających pod dany urząd, a jeden inspektor może być odpowiedzialny za nie więcej niż dziewięć podmiotów. Zatem im większa gmina, tym więcej instytucji oraz potrzeba większej liczby inspektorów i środków w budżecie. Z finansami jest również związana odpowiedzialność za nieprawidłowe przetwarzanie danych osobowych. Za naruszenie art. 25 RODO (zasada *privacy by design* oraz *privacy by default*)[1], art. 29 (przetwarzanie

[1] Zarówno unijny, jak i polski ustawodawca nie wydał żadnego aktu, w którym istniałaby definicja zasady prywatności w fazie projektowania (ang. *privacy by design*) oraz zasady prywatności w ustawieniach

z upoważnienia administratora lub podmiotu przetwarzającego), art. 30 (rejestr czynności przetwarzania), art. 31 (współpraca z organem nadzorczym) oraz za naruszenie postanowień art. 32 (bezpieczeństwo przetwarzania) grozi kara do 10 mln euro, a w przypadku przedsiębiorstwa – kara w wysokości 2 procent jego całkowitego, rocznego światowego obrotu z poprzedniego roku obrotowego[2]. Natomiast za naruszenie zasad wynikających z art. 5, art. 7 (zgoda na przetwarzanie), art. 15 (prawo dostępu przysługującego osobie, której dane dotyczą) oraz art. 16 (prawo do sprostowania i usuwania danych) grozi kara w wysokości do 20 mln euro, a w przypadku przedsiębiorstwa w wysokości 4 procent jego całkowitego, rocznego światowego obrotu z poprzedniego roku obrotowego[3].

Generowaniem dodatkowych kosztów było również wprowadzenie do obiegu nowych formularzy mających swoje umocowanie w uchwałach, instrukcjach i regulaminach odpowiadających nowym przepisom o ochronie danych osobowych.

ISO 27001 jako wsparcie dla samorządów w procesie wdrażania RODO

Posiadanie certyfikatu międzynarodowej normy technicznej ISO z grupy 27001 dla wielu jednostek samorządu terytorialnego stało się bardzo pomocne podczas wdrażania nowych przepisów. Celem wskazanej procedury jest zagwarantowanie podstawowych zasad dotyczących zarządzania zbiorami zawierającymi dane osobowe oraz określenie reguł udostępniania danych osobowych. Jest to norma „określająca wymagania dla ustanowienia, wdrażania, zarządzania, monitorowania i przeglądu udokumentowanego systemu zarządzania bezpieczeństwem informacji w organizacji”[4]. ISO 27001 wymaga przeprowadzenia oceny ryzyka, co ma chronić przed ujawnieniem danych w jednostce organizacyjnej. Podobny obowiązek wynika z RODO z tą różnicą, że tutaj administrator musi ocenić skutki dla ochrony danych (ang. *private impact assessment*, PIA), zanim rozpocznie przetwarzanie. Kolejnym elementem wynikającym z normy technicznej i jednocześnie wspierającym procedurę wdrażania nowych przepisów jest zarządzanie incydentami bezpieczeństwa informacji. Na mocy art. 33 ust. 1 RODO nie później niż w terminie 72 godzin od stwierdzenia naruszenia administrator ma obowiązek powiadomić organ ochrony danych osobowych o incydencie skutkującym ryzykiem naruszenia praw i wolności danej osoby fizycznej. Analogiczny mechanizm jest narzucony w ramach ISO 27001. Jeżeli dana jednostka wdrożyła wcześniej międzynarodowe normy, które odnoszą się między innymi do outsourcingu danych, to kwestia powierzania przetwarzania danych podmiotom trzecim nie stanowi na przykład dla gmin

domyślnych (ang. *privacy by default*). Ich treść wynika z funkcji, jakie powinny spełniać programy służące przetwarzaniu danych osobowych. Koncepcja tych pojęć miała być odpowiedzią na trudności związane z zabezpieczeniem prywatności w związku z postępem technologicznym i rozwojem społeczeństwa informacyjnego.

[2] Zob. art. 83 ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).

[3] Zob. tamże, art. 83 ust. 5.

[4] E. Wolska, *Audyt zgodności z normą ISO – IEC 27001:27005*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki” 2012, nr 7, s. 80.

większych trudności[5]. Samorządy coraz chętniej sięgają po nowoczesne metody służące poprawie jakości usług i jak się okazuje, tam, gdzie wcześniej były wdrożone normy ISO, spokojniej przebiegał proces dostosowania danej jednostki do RODO i funkcjonowania w niej nowych przepisów.

Tabela 1. Związek ISO 20071 z wymaganiami RODO

27001	Polityka bezpieczeństwa	art. 24 ust. 2	Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora **odpowiednich polityk ochrony danych**.
	Kontrola dostępu	art. 5 ust. 1f	Dane osobowe muszą być […] przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed **niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą**, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").
	Zarządzanie ciągłością działania	art. 32 ust. 2	Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności **ryzyko** wiążące się z przetwarzaniem, w szczególności wynikające z **przypadkowego** lub niezgodnego z prawem **zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu** do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
	Zarządzanie incydentami związanymi z bezpieczeństwem informacji	motyw 49	Przetwarzanie danych osobowych w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji […] oraz bezpieczeństwa związanych z nimi usług oferowanych lub udostępnianych poprzez te sieci i systemy przez organy publiczne, zespoły reagowania na zagrożenia komputerowe, zespoły reagowania na **komputerowe incydenty naruszające bezpieczeństwo**, dostawców sieci i usług łączności elektronicznej oraz dostawców technologii i usług w zakresie bezpieczeństwa jest prawnie uzasadnionym interesem administratora, którego sprawa dotyczy.

Źródło: S. Stefaniak, H. Suszek-Borowska, O. Budziszewska, *Zabezpieczanie i analizowanie ryzyk przetwarzania danych osobowych*, [w:] P. Sikorski (red.), *Ochrona danych osobowych – poradnik dla małych i średnich przedsiębiorców*, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2017, s. 87.

RODO w zamówieniach publicznych realizowanych przez jednostki samorządowe

Gmina (jako zamawiający) przetwarza dane wykonawców na przykład ujawnione w ofertach, dane osób reprezentujących, dane dotyczące realizacji obowiązku zatrudnienia na podstawie umowy o pracę czy też dane osobowe zawarte w KRS, KRK, wykazach usług, robót budowlanych itp., które są dostarczane na wezwanie. Gmina również ujawnia dane osób fizycznych i wtedy to wykonawcy stają się podmiotami przetwarzającymi, na przykład gdy gmina udostępnia nazwiska członków komisji przetargowej, dane osób, z którymi należy się kontaktować w sprawie ogłoszonego przetargu, czy też dane niezbędne do realizacji umowy przy zamówieniach na ochronę, budowę systemów informatycznych, zamówienia archiwizacyjne itp. RODO ma znaczący wpływ na relację samorząd–przedsiębiorca w od-

[5] Zob. A. Popowicz-Pazdej, *Ochrona danych osobowych: Wdrożenie ISO 27001 pomoże przy implementacji RODO, ale nie zastąpi analizy indywidualnych uwarunkowań*, https://prawo.gazetaprawna.pl/artykuly/1076816,rodo-ochrona-danych-osobowych-wdrozenie-iso-27001.html [dostęp: 10.11.2018].

niesieniu do zamówień publicznych, gdzie zarówno na zamawiającego, jak i wykonawcę zostały nałożone nowe obowiązki.

RODO chroni dane osób fizycznych, a zatem wydawać by się mogło, że nie w każdym postępowaniu o udzielenie zamówienia powinny znaleźć zastosowanie nowe regulacje prawne, albowiem większość zamówień jest udzielana osobom prawnym. Nic bardziej mylnego! Należy pamiętać, że nawet jeśli wykonawcą nie jest osoba fizyczna prowadząca działalność gospodarczą, to zamawiający i tak otrzymuje dane osób fizycznych, które są zatrudnione przez daną osobę prawną, a zatem stosowanie przepisów RODO w zamówieniach publicznych jest niezbędne, by prowadzić procedurę zamówieniową zgodnie z prawem na wszystkich jej etapach.

W początkowym okresie wdrażania rozporządzania kłopotliwe dla stron postępowania o udzielenie zamówienia było to, czy nowe przepisy odnoszą się do postępowań już wszczętych, czy wyłącznie do tych, które dopiero będą się rozpoczynały i przede wszystkim to, w jaki sposób chronić dane osób i podmiotów biorących udział w przetargu. Naprzeciw tym wątpliwościom wyszedł Urząd Zamówień Publicznych, który wskazał, że nowe przepisy odnoszą się do postępowań zarówno rozpoczętych z dniem 25 maja 2018 roku, jak i postępowań wszczętych wcześniej, pod warunkiem że toczyły się nadal po wejściu w życie rozporządzenia, tj. po 25 maja 2018 roku. W takich przypadkach zamawiający miał obowiązek uwzględnić nowe przepisy przy pierwszej czynności podejmowanej z wykonawcą, którą zwykle jest wymiana korespondencji[6].

Obowiązek informacyjny ciążący na gminie jako administratorze danych osobowych

Administratorem danych osobowych pozyskiwanych w związku z ogłaszanym przez urząd gminy konkursem ofert na udzielenie zamówienia jest gmina, albowiem to ona występuje w charakterze zamawiającego. Zgodnie z art. 7 pkt 4 Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[7] (dalej: u.o.d.o.) za administratora danych uznaje się organ, jednostkę organizacyjną bądź podmiot lub osobę, do której odnoszą się przepisy ustawy decydujące o celach i środkach przetwarzania danych osobowych. Jak stanowi art. 13 RODO, jednym z podstawowych obowiązków administratora jest obowiązek informacyjny wobec osób fizycznych, których dane gmina pozyskuje i przetwarza. Rozporządzenie przewiduje spełnienie obowiązku informacyjnego w trzech formach: pisemnej, elektronicznej lub ustnej. Te dwie pierwsze są najbezpieczniejsze w kontekście zasady rozliczalności, ponieważ w razie konieczności wykazania, że obowiązek informacyjny został spełniony, administrator będzie miał dowody na piśmie[8]. Dlatego też w przypadku zamówienia publicznego to admi-

[6] Zob. J. Rek-Pawłowska, *RODO w zamówieniach publicznych – 5 najważniejszych wskazówek UZP*, https://www.portalzp.pl/nowosci/rodo-w-zamowieniach-publicznych-5-najwazniejszych-wskazowek-uzp-8682.html [dostęp: 10.11.2018].

[7] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. 2018, poz. 1000.

[8] Zob. B. Mendyk, *Przedmiot ochrony – podstawowe pojęcia*, [w:] P. Sikorski (red.), *Ochrona danych osobowych – poradnik dla małych i średnich przedsiębiorców*, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2017, s. 32.

nistrator powinien zamieścić w Specyfikacji Istotnych Warunków Zamówienia, ogłoszeniu o zamówieniu, konkursie lub w regulaminie klauzulę informacyjną, z której będzie wynikało między innymi to, jaki podmiot przetwarza dane, po co są przetwarzane i jak długo będą w posiadaniu administratora. Jeżeli gmina nie zrobiła tego na etapie ogłoszenia przetargu, powinna niezwłocznie tego obowiązku dopełnić na przykład za pośrednictwem korespondencji z wykonawcami, którzy złożyli swoje oferty.

Warto podkreślić, że o ile podmiot przystępujący do postępowania posiada prawo dostępu do swoich danych (art. 15 RODO), prawo do ich sprostowania (art. 16 RODO) oraz żądania od administratora ograniczenia przetwarzania danych poza sytuacjami, w których dane są przechowywane w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego (art. 18 ust. 2 RODO), a także posiada prawo do wniesienia skargi do prezesa Urzędu Ochrony Danych Osobowych, o tyle jest pozbawiony prawa do usunięcia danych osobowych w imię przepisów zawartych w art. 17 ust. 3 lit. b, d lub e RODO. Istnieje kilka okoliczności ujętych w zamkniętym katalogu, które wyłączają prawo do bycia zapomnianym – jest to między innymi sytuacja, w której administrator przetwarza dane w związku z ciążącym na nim ustawowym obowiązkiem prawnym oraz gdy wykonywane zadanie jest w interesie publicznym lub w ramach władzy publicznej powierzonej administratorowi[9]. Poza tym wykonawca nie ma prawa do przenoszenia danych osobowych, do czego nawiązuje art. 20 RODO oraz nie może podnieść sprzeciwu wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania danych osobowych przez gminę jest art. 6 ust. 1 lit. c RODO, który stanowi, że „przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze", o czym podmiot zainteresowany zostaje poinformowany za pośrednictwem przygotowanej przez daną jednostkę organizacyjną klauzuli informacyjnej. Trzeba też dodać, że jeżeli wykonawca chciałby skorzystać z przysługującego mu prawa do sprostowania swoich danych, to czynność ta nie może mieć wpływu na wynik postępowania o udzielenie zamówienia ani też nie może skutkować zmianą postanowień umowy w zakresie, którego p.z.p. nie przewiduje.

Dane osobowe zamieszczane w Biuletynie Zamówień Publicznych

Ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych[10] (dalej: p.z.p.) nie reguluje kwestii związanych z przetwarzaniem danych osobowych w Biuletynie Zamówień Publicznych, przez co wykonawcy często poddają pod wątpliwość zakres informacji podawanych do publicznej wiadomości w związku z nowymi przepisami o ochronie danych osobowych. Jak wspomniano wcześniej, zakres przedmiotowy ustawy o ochronie danych osobowych oraz unijnego rozporządzenia dotyczy danych osób fizycznych. Wszelkiego rodzaju ograniczenia wynikające z regulacji odnoszących się do danych osobowych nie mają

[9] Zob. B. Mendyk, *Prawa osób, których dane dotyczą*, *czyli inne obowiązki administratora*, [w:] P. Sikorski (red.), *Ochrona danych osobowych – poradnik dla małych i średnich przedsiębiorców*, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2017, s. 56–57.

[10] Ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych, Dz. U. 2018, poz. 1986.

zastosowania do podmiotów posiadających osobowość prawną lub jednostek organizacyjnych nieposiadających tej osobowości czy też podmiotów działających w oparciu o przepisy Ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej[11]. Zatem jeżeli zamówienie publiczne zostanie udzielone przedsiębiorcy będącemu osobą fizyczną, którego dane osobowe jednocześnie są danymi identyfikującymi jego firmę, to nie może jako osoba fizyczna żądać od gminy nieujawnienia tych danych na przykład w Biuletynie Zamówień Publicznych. Naczelny Sąd Administracyjny w wyroku z dnia 28 listopada 2002 r., który dotyczył przetwarzania informacji o charakterze osobowym osób prowadzących działalność gospodarczą, podkreślił, że osoba decydująca się na działalność gospodarczą godzi się na ograniczenie swojego prawa prywatności w większym zakresie niż osoba fizyczna, która takiej działalności nie podejmuje. Jeżeli informacje zawarte w umowie są przez kontrahenta nadużywane do innych celów, aniżeli przewiduje treść zawartej umowy, wtedy podniesienie sprzeciwu byłoby zasadne[12]. Ponieważ w zamówieniach publicznych obowiązuje zasada jawności postępowania (art. 8 p.z.p.), to na mocy przepisów odnoszących się do ogłoszeń zamieszczanych w Biuletynie Zamówień Publicznych gwarantuje się dostępność pewnych informacji (w tym danych osobowych) innym zainteresowanym. Każdy uczestnik postępowania, w tym również osoby fizyczne prowadzące działalność gospodarczą, przystępując do przetargu, już przez sam fakt zadeklarowania swojego uczestnictwa godzą się na upublicznienie treści zawierających ich dane osobowe, jeżeli zamówienie zostanie im udzielone, a w przypadku negocjacji bez ogłoszenia i zamówień z wolnej ręki godzą się na ujawnienie swoich danych jeszcze przed udzieleniem zamówienia[13]. Urząd Zamówień Publicznych jest administratorem danych, które są umieszczane przez zamawiających za pośrednictwem odpowiednich formularzy elektronicznych, ale nie posiada uprawnień do zmiany ich treści. Przepisy p.z.p. są przepisami szczególnymi w stosunku do u.o.d.o. Art. 23 ust. 1 wskazanej ustawy dopuszcza przetwarzanie danych, jeżeli jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Urząd Zamówień Publicznych posiada zatem kompetencje do przetwarzania danych osobowych, ponieważ realizuje obowiązki wynikające z przepisów p.z.p. oraz aktów wykonawczych tejże ustawy[14].

Podsumowanie

Mimo licznych trudności i zdarzających się pomyłek wynikających z niewłaściwego interpretowania przepisów RODO można uznać, że administracja publiczna radzi sobie niekiedy lepiej z nowymi przepisami aniżeli przedsiębiorcy, czego przykładem jest sprawa o przywrócenie terminu rozpatrywana przez Wojewódzki Sąd Administracyjny

[11] Ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, Dz.U. 2013, poz. 672.

[12] Zob. Wyrok NSA z dnia 28 listopada 2002 r., sygn. akt II SA 3389/01.

[13] Zob. *Dane osobowe wykonawców zamieszczane w Biuletynie Zamówień Publicznych*, Urząd Zamówień Publicznych, https://www.uzp.gov.pl/baza-wiedzy/interpretacja-przepisow/opinie-dotyczace-ustawy-pzp/inne/dane-osobowe-wykonawcow-zamieszczane-w-biuletynie-zamowien-publicznych [dostęp: 8.11.2018].

[14] Zob. tamże.

we Wrocławiu. Jedna ze stron przez reorganizację związaną z RODO zagubiła bardzo ważne dokumenty, przez co nie wywiązała się w terminie ze swojego zobowiązania. Sąd w swoim postanowieniu ocenił, że strona składająca wniosek o przywrócenie terminu dołożyła wszelkiej staranności, aby zaginioną dokumentację odnaleźć, a mimo to użycie wysiłku w danych warunkach nie usunęło przeszkody[15]. Z treści postanowienia można wysnuć wniosek, że skład orzekający miał świadomość, iż kompleksowe wdrażanie nowych przepisów może w danej jednostce być źródłem chaosu skutkującego niewywiązaniem się ze swoich zadań w terminie. Eksperci oceniają, że upłynęło zbyt mało czasu, aby wyciągać daleko idące wnioski, ale na pewno daje się już zauważyć, że najwięcej pytań i trudności w samorządach pojawiło się na etapie zawierania umów powierzenia przetwarzania danych osobowych z innymi podmiotami. Rozbieżne interpretacje przepisów odnoszące się na przykład do zasadności podpisywania takich umów wprowadzają jednostki w błąd. Samorządy musiały się zmierzyć z oceną dotychczasowego systemu przetwarzania danych, a zakres zgromadzonych informacji zweryfikować pod kątem celowości i zasady minimalizmu. Niewątpliwie wiele wysiłku kosztowała weryfikacja treści uchwał, instrukcji, wniosków i regulaminów w kontekście unijnego rozporządzenia, ale samorządy, mając wsparcie IODO, dobrze sobie z tym radzą. Ponieważ rozporządzenie w swojej treści często wyznacza wyłącznie cel (bez wskazania środków do jego realizacji), dla wielu jednostek samorządu terytorialnego bardzo pomocne stały się mechanizmy norm z zakresu zarządzania bezpieczeństwem informacji (ISO z grupy 27001 – systemy zarządzania bezpieczeństwem informacji, 27002 – zasady zarządzania bezpieczeństwem informacji, 27005 – zarządzanie ryzykiem).

Bibliografia

Mendyk B., *Prawa osób, których dane dotyczą*, *czyli inne obowiązki administratora*, [w:] P. Sikorski (red.), *Ochrona danych osobowych – poradnik dla małych i średnich przedsiębiorców*, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2017.

Mendyk B., *Przedmiot ochrony – podstawowe pojęcia*, [w:] P. Sikorski (red.), *Ochrona danych osobowych – poradnik dla małych i średnich przedsiębiorców*, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2017.

Popowicz-Pazdej A., *Ochrona danych osobowych: Wdrożenie ISO 27001 pomoże przy implementacji RODO, ale nie zastąpi analizy indywidualnych uwarunkowań*, https://prawo.gazetaprawna.pl/artykuly/1076816,rodo-ochrona-danych-osobowych-wdrozenie-iso-27001.html [dostęp: 10.11.2018].

Rek-Pawłowska J., *RODO w zamówieniach publicznych – 5 najważniejszych wskazówek UZP*, https://www.portalzp.pl/nowosci/rodo-w-zamowieniach-publicznych-5-najwazniejszych-wskazowek-uzp-8682.html [dostęp: 10.11.2018].

Stefaniak S., Suszek-Borowska H., Budziszewska O., *Zabezpieczanie i analizowanie ryzyk przetwarzania danych osobowych*, [w:] P. Sikorski (red.), *Ochrona danych osobowych – poradnik dla małych i średnich przedsiębiorców*, Polska Agencja Rozwoju Przedsiębiorczości, Warszawa 2017.

[15] Zob. Postanowienie WSA we Wrocławiu z dnia 12 września 2018 r., sygn. akt II SA/Wr 493/18.

Dane osobowe wykonawców zamieszczane w Biuletynie Zamówień Publicznych, Urząd Zamówień Publicznych, https://www.uzp.gov.pl/baza-wiedzy/interpretacja-przepisow/opinie-dotyczace-ustawy-pzp/inne/dane-osobowe-wykonawcow-zamieszczane-w-biuletynie-zamowien-publicznych [dostęp: 8.11.2018].

Wolska E., *Audyt zgodności z normą ISO – IEC 27001:27005*, „Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki" 2012, nr 7.

Akty prawne

Postanowienie WSA we Wrocławiu z dnia 12 września 2018 r., sygn. akt II SA/Wr 493/18.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).

Ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych, Dz.U. 2018, poz. 1986.

Ustawa z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, Dz.U. 2013, poz. 672.

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. 2018, poz. 1000.

Wyrok NSA z dnia 28 listopada 2002 r., sygn. akt II SA 3389/01.

Streszczenie
Unijne przepisy o ochronie danych osobowych w jednostkach samorządu terytorialnego

Zatrudnienie inspektora ochrony danych osobowych, pozyskiwanie zgody na przetwarzanie danych, obowiązkowe zgłaszanie naruszeń i powiadomienie podmiotu zainteresowanego, uściślenie obowiązków podmiotów przetwarzających dane oraz korzystanie ze zmienionych przepisów odnoszących się do międzynarodowego przekazywania danych osobowych to nowe zasady, z wdrożeniem których niedawno musiały się zmierzyć m.in. jednostki samorządu terytorialnego na mocy unijnego Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO). Istotne zmiany zaszły na poziomie zamówień publicznych realizowanych przez samorządy, gdzie wykonawca jest pozbawiony prawa do usunięcia danych, ich przenoszenia oraz nie może podnieść sprzeciwu wobec ich przetwarzania.

Słowa kluczowe: samorząd terytorialny, ochrona danych osobowych, obowiązek informacyjny, administrator danych, zamówienia publiczne

Summary
EU regulations on the protection of personal data in local government units

The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) imposed new duties on local self-government units commencing on May 2018. Employing a Personal Data Protection Officer, obtaining consent to data processing, mandatory reporting of violations and notifying the interested party, detailing of the duties of data processors and the application of amended provisions regarding international data transfers constituted the new rules which had to be implemented. Major changes have occurred on the level of public contracts performed by local governments, whereby the contractor no longer has the right to remove data, transfer data, and cannot object against the processing of the data.

Keywords: local government, personal data protection, disclosure requirements, data controller, public contracts