Małgorzata Durbajło-Mrowiec
Uniwersytet Wrocławski

DOI: 10.23734/23.18.010

Ochrona danych osobowych w rachunkowości

Streszczenie

Od 25 maja 2018 roku kraje członkowskie Unii Europejskiej zostały zobowiązane rozporządzeniem 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 (ogólne rozporządzenie o ochronie danych) do ujednolicenia standardów ochrony danych osobowych. Rachunkowość prowadzona przez komórki wewnętrzne podmiotu lub przez biura rachunkowe również musi zostać dostosowana do nowych wymagań. Więcej wymagań muszą spełnić biura rachunkowe niż działy rachunkowości będące komórkami wewnętrznymi podmiotów-administratorów danych osobowych. Biura rachunkowe są zobowiązane realizować wszystkie obowiązki ciążące na administratorze danych i podmiocie przetwarzającym. Wewnętrzne działy rachunkowości zwykle będą zobowiązane do udziału w realizacji niektórych obowiązków ciążących na całym podmiocie, w swoim zakresie działania, np. sporządzania umów powierzenia, zarządzania czynnościami przetwarzania danych osobowych, przygotowania zgłoszeń naruszenia danych, udziału o ocenie skutków dla ochrony danych. Działy rachunkowości nie będą przekazywały klauzul informacyjnych osobom, których dane będzie przetwarzał administrator danych.

Słowa kluczowe

rachunkowość, biura rachunkowe, ochrona danych osobowych

Wprowadzenie

W 2016 roku Parlament i Rada Unii Europejskiej przyjęły jednolite zasady ochrony danych osób fizycznych, uchwalając 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 (ogólne rozporządzenie o ochronie danych)[1], zwane dalej RODO. W art. 99 ust. 2 zapisano, że rozporządzenie ma zastosowanie we wszystkich krajach Unii od 25 maja 2018 roku. Pozostawiono więc krajom członkowskim Unii Europejskiej dwa lata na dostosowanie środowiska prawnego i funkcjonowania

[1] 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 (ogólne rozporządzenie o ochronie danych), https://sip.legalis.pl/document-full.seam?documentId=mfrxilrtgm2tsnrrguytsltwmvzc4mjxgy3ti [dostęp: 30.06. 2018].

podmiotów publicznych i gospodarczych do stosowania RODO. W przypadku Polski jedyną formą i działaniem dostosowawczym, które zostało zrealizowane do momentu zastosowania RODO jest uchwalenie ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.[2], zwanej dalej Ustawą. Proces legislacyjny Ustawy był pośpieszny, co odbiło się na zawartości i jakości regulacji. Poniżej kalendarz prac nad Ustawą:

- 5.04.2018 Rada Ministrów kieruje projekt do Sejmu,
- 10.05.2018 Sejm uchwala Ustawę,
- 16.05.2018 Senat akceptuje Ustawę bez poprawek,
- 22.05.2018 Prezydent podpisuje Ustawę,
- 24.05.2018 Ustawa zostaje ogłoszona w Dzienniku Ustaw.

Wprowadzona ustawa o ochronie danych osobowych nie reguluje przetwarzania danych osobowych we wszystkich obszarach życia. Poza jej wpływem pozostaje działalność służb mundurowych, które nadal funkcjonują zgodnie z ustawą z 1997 roku[3]. Zasadnicza część Ustawy dotyczy utworzenia organu nadzorczego i zasad jego funkcjonowania, jak również prowadzenia postępowań przed tym organem. Dużo miejsca w nowej ustawie poświęcono wskazaniu administratorów danych centralnych systemów informatycznych i określeniu podmiotów, które mogą korzystać z tych baz danych. Kolejnym istotnym obszarem regulowanym Ustawą jest prowadzenie monitoringu w zakładach pracy, w szkołach oraz w miejscach publicznych. W Polsce nie ma przepisów o monitoringu. Ustawodawca polski w niewielkim zakresie skorzystał z uprawnień, jakie państwom członkowskim Unii pozostawiono w RODO. Stosowne zestawienie ujęto w tabeli 1. Najtrudniejszy do spełnienia przez administratora danych obowiązek informacyjny nie został doprecyzowany. Nie wprowadzono też żadnego ograniczenia w spełnianiu go, mimo wcześniejszych informacji o złagodzeniu tego wymogu, np. Ministerstwa Cyfryzacji wspólnie z Ministerstwem Przedsiębiorczości i Technologii o zwolnieniu z tego obowiązku przedsiębiorstw małych i średnich[4]. Chodzi tu przede wszystkim o obowiązki wynikające z art. 13 RODO dotyczące informacji podawanych przez administratorów danych osobowych w przypadku zbierania danych od osoby, której dane dotyczą. Nawet podmioty finansów publicznych realizujące swoje obowiązki wynikające z przepisów prawa w zakresie zabezpieczenia socjalnego, wypłacania świadczeń rodzinnych czy świadczące usługi zdrowotne nie zostały zwolnione z tego obowiązku, chociażby częściowo.

[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000).

[3] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r. ze zm.).

[4] *Komunikat Ministerstwa Cyfryzacji i Ministerstwa Przedsiębiorczości i Technologii dotyczący stosowania przepisów unijnego ogólnego rozporządzenia o ochronie danych osobowych (RODO) w stosunku do sektora małych i średnich przedsiębiorstw*, „Gazeta Podatkowa" 29.01.2018, Nr 9 (1466).

Tabela 1. Zestawienie uprawnień państw członkowskich ujętych w RODO z adekwatnymi regulacjami w Ustawie

Art. RODO	Podstawowe zakresy pozostawione do regulacji krajowej	Art. Ustawy
6	Zgodność przetwarzania danych zwykłych – prawo do doprecyzowania	
8	Warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego – prawo do zmiany wieku, min. do 13 lat	
9	Przetwarzanie szczególnych kategorii danych osobowych – prawo do dalszego ograniczenia przetwarzania danych genetycznych, biometrycznych lub dotyczących zdrowia	
23	Ograniczenia – prawo do ograniczenia zakresu obowiązków i praw przewidzianych w art. 12-22 i w art. 34, a także w art. 5 RODO, czyli praw osób, zasad przetwarzania i informowania o naruszeniu danych osobowych	3, 4, 5, ale tylko w zakresie obowiązku informacyjnego, jeśli dotyczy informacji niejawnych albo realizacji zadań publicznych i podanie informacji utrudni realizacje zadania, 6 – wyłączenie stosowania przez jednostki sektora finansów publicznych, jeśli dotyczy to bezpieczeństwa narodowego oraz służb specjalnych
40	Kodeksy postępowania – prawo do zachęcania do sporządzania kodeksów postępowania dla różnych sektorów z uwzględnieniem specyfiki mikro, małych i średnich przedsiębiorstw	Rozdział 6 – obowiązki, które należy spełnić przed Urzędem nadzorczym
42	Certyfikacja – prawo do ustalenia mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych osobowych	Rozdziały 3, 4, 5, ale tylko w zakresie certyfikacji
84	Sankcje – prawo do określenia innych sankcji za naruszenia RODO niż kary administracyjne	Rozdział 10 – odpowiedzialność cywilna 107 – odpowiedzialność karna
85	Przetwarzanie a wolność wypowiedzi i informacji – prawo do określenia zasad pozwalających pogodzić ochronę danych osobowych z wypowiedzią dziennikarską, akademicką, artystyczną i literacką	2
86	Przetwarzanie a publiczny dostęp do dokumentów urzędowych – prawa do pogodzenia tych celów	151 – powtórne wykorzystanie z zachowaniem przepisów o ochronie danych osobowych
87	Przetwarzanie krajowego numeru identyfikacyjnego – prawa do określenia szczególnych zasad	

Art. RODO	Podstawowe zakresy pozostawione do regulacji krajowej	Art. Ustawy
88	Przetwarzanie w kontekście zatrudnienia – prawo do określenia szczególnych zasad	111 – zmiana w kodeksie pracy – zasady stosowania monitoringu
89	Zabezpieczenia i wyjątki mające zastosowanie do przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych albo historycznych lub do celów statystycznych – prawo do ograniczenia w praw osób, których dane dotyczą	
90	Obowiązek zachowania tajemnicy – prawo do regulacji szczególnej w zakresie zawodów zobowiązanych do zachowania tajemnicy zawodowej	115 – NIK uprawnienie do przetwarzania danych zwykłych 126 – zwolnienie częściowe z zachowania tajemnicy dla psychologów 141 – nałożono obowiązek zachowania poufności 147 – obowiązek poufności dla fizjoterapeutów 153 – uprawnienie do zbierania danych osobowych przez Krajową Administrację Skarbową

Źródło: opracowanie własne na podstawie RODO i Ustawy.

Nowa ustawa o ochronie danych osobowych miała wejść w życie razem z ustawą wprowadzającą, w której miały być ujęte zmiany w innych ustawach (wg szacunku Rządu w ponad 100 aktach), aby doprowadzić polskie przepisy do zgodności z RODO. Projekt ustawy – przepisy wprowadzające ustawę o ochronie danych osobowych nadal jest przedmiotem prac Rady Ministrów. Po wdrożeniu RODO zmieniono nazwę projektowanej ustawy na projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679[5]. W projekcie, w sektorze finansów proponuje się zmiany w następujących przepisach:

1) ustawie z dnia 17 czerwca 1966 o postępowaniu egzekucyjnym w administracji (Dz. U. z 2016 r. poz. 599 ze zm.),
2) ustawie z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników (Dz. U. z 2016 r. poz. 476 ze zm.),
3) ustawie z dnia 29 sierpnia 1997 – Ordynacja podatkowa (Dz. U. z 2017 r. poz. 201 ze zm.),
4) ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2016 r. poz. 1988 ze zm.),

[5] Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679, https://bip.kprm.gov.pl/kpr/form/r7079293730832,Projekt-ustawy-o-zmianie-niektorych-ustaw-w-zwiazku-z-zapewnieniem-stosowania-ro.html [dostęp: 5.07.2018].

5) ustawie z dnia 22 maja 2003 r. o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych (Dz. U. z 2016 r. poz. 2060),
6) ustawie z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz. U. z 2016 r. poz. 1910 ze zm.),
7) ustawie z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2016 r. poz. 1572 ze zm.),
8) ustawie z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz. U. poz. 1844 ze zm.),
9) ustawie z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz. U. poz. 1947 ze zm.),
10) ustawie z dnia 9 marca 2017 r. o wymianie informacji podatkowych z innymi państwami (Dz. U. poz. 648).

Nie przewidziano zmian w przepisach regulujących prowadzenie rachunkowości, np. ustawie o rachunkowości, rozporządzeniu w sprawie szczególnych zasad oraz planów kont dla budżetu państwa, budżetów jednostek samorządu terytorialnego, jednostek budżetowych, samorządowych zakładów budżetowych, państwowych funduszy celowych oraz państwowych jednostek budżetowych mających siedzibę poza granicami Rzeczypospolitej Polskiej czy rozporządzeniu w sprawie prowadzenia podatkowej księgi przychodów i rozchodów.

Celem artykułu jest określenie działań dostosowawczych, jakie muszą zrealizować działy rachunkowości i biura rachunkowe, oraz wskazanie ich obowiązków w związku z wejściem RODO. Nie ulega bowiem wątpliwości, że rachunkowość przy okazji przetwarzania informacji finansowych przetwarza też dane osób fizycznych: dostawców, klientów, pracowników, emerytów, właścicieli spółek.

Publikację poprzedzono badaniami, głównie metodą porównawczą uwarunkowań prawno-organizacyjnych i funkcjonalnych działów księgowości w 18 wybranych pomiotach gospodarczych i sektora finansów publicznych, jak również biur rachunkowych. Przeprowadzono wywiady z osobami odpowiedzialnymi za ochronę informacji w badanych podmiotach, analizę zmian jakościowych oraz analizę dokumentacji z zakresu ochrony danych osobowych. Zbadano również przepisy prawa regulujące obszar badawczy.

Obowiązki administratora danych

Według RODO najważniejszym podmiotem biorącym udział w przetwarzaniu danych osób fizycznych jest administrator danych osobowych. Zgodnie z art. 4 ust. 7 RODO administratorem danych jest każda osoba fizyczna, prawna, prowadząca

działalność gospodarczą, realizująca zadania publiczne bez względu na wielkość, sektor, branżę, w których prowadzi działalność, jeśli określa cele i sposoby przetwarzania danych. Przez przetwarzanie należy rozumieć „operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie" (art. 4 ust. 2 RODO).

Administrator danych może przetwarzać dane osób fizycznych według następujących zasad (art. 5-11 RODO):

1) zgodnie z prawem, rzetelnie, w sposób przejrzysty dla osoby, której dane dotyczą;
2) dla konkretnego, szczegółowego celu (archiwizowanie nie narusza tej zasady), np. zawarcie umowy o pracę i jej realizacja, wydanie zaświadczenia, przeprowadzenie konkursu, ustalenie wymiaru podatku, podpisanie i rozliczenie umowy (ograniczenie celu);
3) tylko w niezbędnym zakresie dostosowanym do celu (minimalizacja danych), najlepiej wprost wynikającego z zapisów prawa, np. art. 22 k.p.;
4) administrator odpowiada za prawidłowe, aktualne dane (ma podjąć rozsądne działania, aby zapewnić spełnienie tej zasady);
5) dane mogą być przetwarzane w ograniczonym okresie czasu, różne dane w różnym czasie, np. dane kontaktowe pracownika do zakończenia pracy, dokumentacja kadrowa wynikająca z przepisów prawa zgodnie z okresem archiwizacji;
6) przetwarzane dane mają charakter poufny, administrator musi zastosować rozwiązania organizacyjne i techniczne w celu ochrony tych danych (zasada integralności);
7) w sposób rozliczalny, tzn. administrator musi wykazać przestrzeganie przepisów prawa i podjęte działania w celu ochrony danych (zasada dokumentowania działań).

Z zasad przetwarzania danych i praw osób, których dane dotyczą, wynikają obowiązki administratora danych. Zadania administratora danych zostały zapisane wprost w RODO w następujących artykułach:

- art. 13-18 i art. 34 **obowiązek komunikowania się (informowania),** w tym o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania, ale tylko odbiorców danych oraz o naruszeniu danych;
- art. 24 ust 1 **obowiązek wdrożenia środków organizacyjnych i technicznych** adekwatnych do ryzyka przetwarzania danych, aby przetwarzanie było zgodne

z RODO i aby móc to wykazać, środki te w razie potrzeby należy poddawać przeglądom i uaktualniać;

- art. 24 ust 2 **obowiązek opracowania i wdrożenia Polityki przetwarzania danych** osobowych, jeśli taki środek zostanie uznany za adekwatny do czynności przetwarzania;
- art. 25 uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych – wdraża odpowiednie środki techniczne i organizacyjne, aby **domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne** (np. szyfrowanie, pseudoanonimizację);
- art. 30 **rejestrowanie czynności przetwarzania**;
- art. 35 **ocena skutków dla ochrony danych podstawą doboru środków ochrony danych i zapewnienia bezpieczeństwa danych.** Konsultacje z organem nadzorczym przed rozpoczęciem przetwarzania, jeśli ryzyko naruszenia ochrony danych jest duże, a administrator nie może zabezpieczyć danych (art. 36);
- art. 31 **współpraca z organem nadzorczym**, np. wykonywanie sprawdzeń przez Inspektora ochrony danych na zlecenie Urzędu;
- art. 33 **zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu**;
- art. 37 **wyznaczenie inspektora ochrony danych w podmiotach publicznych** i innych, które systematycznie i regularnie monitorują osoby na dużą skalę lub przetwarzają dane wrażliwe.

Drugą, rozległą grupą zadań administratora danych jest realizacja praw osób, których dane przetwarza. Pierwszym z nich jest prawo osoby do bycia właściwie poinformowaną. Aby zrealizować to prawo, administrator jest zobowiązany do przekazania osobie w czasie pozyskiwania danych albo w czasie ujawnienia tzw. klauzuli informacyjnej. Zawartość tej klauzuli powinna się zmieniać w zależności od sposobu pozyskania danych, źródła danych, celu, do którego dane są zbierane, zakresu przetwarzania i podstawy prawnej przetwarzania (art. 13 i 14 RODO). Kolejne prawa osób fizycznych to prawo dostępu do danych, ich sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia, wniesienia sprzeciwu. Należy pamiętać, że zakres praw przysługujący osobie, której dane dotyczą, zależy od przyjętej podstawy prawnej przetwarzania. Osobie, która wyraziła zgodę na przetwarzanie danych osobowych, przysługuje pełny wachlarz praw zagwarantowanych w RODO. Spośród podstaw mających najczęstsze zastosowanie, czyli: za zgodą osoby, w celu przygotowania i realizacji umowy, której stroną jest osoba lub w celu spełnienia obowiązku prawnego ciążącego na administratorze danych, najwęższy zakres praw przysługuje osobie, której dane są przetwarzane na podstawie ostatniej z wymienionych przesłanek, czyli realizacji obowiązku zapisanego w prawie

UE lub prawie państwa członkowskiego. Realizacja tej grupy praw wymaga od administratora danych przyjęcia szeregu rozwiązań organizacyjnych, np. powierzenia adekwatnych zadań pracownikowi, określenia sposobu kontaktu z osobami chcącymi skorzystać ze swoich praw, ustalania zasad realizacji tych praw, np. kiedy, od jakiej liczby kopii danych pobierana będzie opłata, w jak sposób, użytkując systemy komputerowe o ograniczonych możliwościach raportowania, przykazywać dane osób fizycznych w powszechnie stosowanych formatach, sposoby aktualizacji danych, kryteria, po spełnieniu których osoba nie będzie identyfikowana itp. Osoba fizyczna, która poniesie szkodę majątkową lub niemajątkową w wyniku naruszenia RODO, ma prawo uzyskać od administratora odszkodowanie za poniesioną szkodę. Administrator ponosi więc również odpowiedzialność finansową.

Rachunkowość wewnętrzna

Ustawa o rachunkowości umożliwia prowadzenie rachunkowości we własnym zakresie albo w ramach outsourcingu. Rachunkowość wewnętrzna prowadzona jest przez wyodrębnione w strukturze organizacyjnej podmiotu wyspecjalizowane działy. W drugim przypadku mamy do czynienia z usługowym prowadzeniem ksiąg rachunkowych przez biura rachunkowe (art. 76a ustawy o rachunkowości[6]).

Działy rachunkowości w podmiocie są elementem składowym administratora danych osobowych, którym jest najczęściej osoba prawna (przedsiębiorstwo państwowe, spółka, spółdzielnia) lub organ publiczny np. gmina, jednostka samorządu terytorialnego (np. ośrodek pomocy społecznej), stowarzyszenie, fundacja. Zatem wskazane w poprzednim punkcie obowiązki administratora danych nie są wprost obowiązkami działów rachunkowości. Aby jednak administrator mógł wywiązać się ze swoich zadań, również tych w zakresie ochrony danych osobowych, każda wewnętrzna komórka organizacyjna musi uczestniczyć w ich wykonaniu w sposób i w zakresie właściwym dla swojej specyfiki. Zadaniem działów rachunkowości jest odzwierciedlenie procesów, zdarzeń zachodzących w sferze realnej w mierniku finansowym, uporządkowanie zebranych informacji finansowych i ich przekształcenie w sprawozdania finansowe. Rachunkowość pozyskuje i przetwarza dane o sytuacji majątkowej, finansowej i o wynikach finansowych podmiotu. W rozdziale 8 ustawy o rachunkowości określono zasady ochrony danych ujętych w dokumentacji księgowej i sprawozdaniach finansowych. W art. 71 ust. 1 zapisano, że dokumentację należy „przechowywać w należyty sposób i chronić przed niedozwolonymi zmianami, nieupoważnionym rozpowszechnianiem, uszkodzeniem lub zniszczeniem". W ust. 2 tego artykułu dodano „Przy prowadzeniu ksiąg rachunkowych

[6] Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2018 r. poz. 395 ze zm.).

przy użyciu komputera ochrona danych powinna polegać na stosowaniu odpornych na zagrożenia nośników danych, na doborze stosownych środków ochrony zewnętrznej, na systematycznym tworzeniu rezerwowych kopii zbiorów danych zapisanych na informatycznych nośnikach danych, pod warunkiem zapewnienia trwałości zapisu informacji systemu rachunkowości, przez czas nie krótszy od wymaganego do przechowywania ksiąg rachunkowych, oraz na zapewnieniu ochrony programów komputerowych i danych systemu informatycznego rachunkowości, poprzez stosowanie odpowiednich rozwiązań programowych i organizacyjnych, chroniących przed nieupoważnionym dostępem lub zniszczeniem".

Powyższe zapisy ustawowe zobowiązują działy rachunkowości do stosowania rozwiązań organizacyjnych i technicznych wystarczających do zapewnienia nienaruszalności danych osobowych[7], np. przed ich utratą w wyniku pożaru, nieuprawnioną modyfikacją danych. Można przyjąć, że zarówno w celu ochrony informacji finansowych, jak i ochrony danych osobowych podmioty będą dobierały zabezpieczenia adekwatnie do występującego ryzyka naruszenia informacji. Takie podejście należy uznać za logicznie uzasadnione. Taki sposób postępowania narzuca RODO. W podstawowym dokumencie organizacyjnym rachunkowości – Polityce rachunkowości – raczej trudno znaleźć opis zastosowanych środków ochrony. W takiej sytuacji jedynym źródłem informacji o środkach ochrony będzie powszechnie stosowana „Polityka ochrony danych osobowych". Dokument ten powinien regulować następujące zagadnienia:

- ogólne zasady bezpieczeństwa informacji, np. zasady ochrony budynków, szaf,
- spełnianie obowiązku informacyjnego,
- realizację praw osób fizycznych,
- wydawanie upoważnień do przetwarzania danych osobowych,
- tworzenie kopii zapasowych i utrzymanie ciągłości działania,
- ochronę przed szkodliwym oprogramowaniem,
- zabezpieczenie urządzeń mobilnych i zasady pracy zdalnej,
- powierzenie przetwarzania danych,
- zarządzanie ruchem sieciowym i bezpieczeństwem komunikacji,
- ocenę skutków przetwarzania dla ochrony danych,
- szacowanie ryzyka związanego z bezpieczeństwem informacji,
- zgłaszanie naruszeń do organu nadzorczego,
- wyznaczenie Inspektora Ochrony Danych.

[7] Art. 4 ust. 9 RODO „naruszenie ochrony danych osobowych" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób.

Wskazany dokument wydaje Administrator danych osobowych i zarządzeniem wdraża go do stosowania, w tym w działach rachunkowości.

Działy rachunkowości mogą brać udział w spełnianiu następujących obowiązków administratora:

- realizowaniu praw osób fizycznych, np. poprzez przygotowanie kopii danych osobowych, aktualizowanie danych osobowych w obsługiwanych systemach informatycznych, usuwanie danych wskazanych osób z systemów, usuwanie dokumentacji papierowej, zanonimizowanie dokumentacji udostępnianej innym osobom, szyfrowaniu zbiorów danych przekazywanych do naprawy,
- zgłaszaniu zapotrzebowania na wydanie upoważnień do przetwarzania danych osobowych pracownikom zatrudnionym w działach rachunkowości,
- sporządzaniu umów powierzenia do umów głównych zawieranych przez dział rachunkowości, np. z doradcą podatkowym,
- udział w sporządzeniu zgłoszenia do organu nadzorczego w przypadku naruszenia danych osobowych w działach rachunkowości,
- udział w szacowaniu ryzyka ochrony danych osobowych w zakresie rachunkowości.

Z powyższego wynika, że wprowadzenie RODO będzie skutkowało w działach rachunkowości zwiększeniem poufności przetwarzania danych i stosowaniem dodatkowych zabezpieczeń organizacyjnych (upoważnień do przetwarzania, umów powierzenia przetwarzania).

Upoważnienie do przetwarzania danych jest wydawane przez administratora danych w celu kontroli dostępu do danych osobowych przetwarzanych w podmiocie. Przed wydaniem upoważnienia osoba upoważniana powinna podpisać oświadczenie o zachowaniu w tajemnicy przetwarzanych danych oraz sposobów ich ochrony przyjętych w pomiocie. Aby upoważnienie spełniło cel, do realizacji którego jest wydawane, powinno wskazywać: do jakiego zbioru danych jest wystawiane, do jakiego rodzaju przetwarzania, np. tylko do przeglądu danych, jakie zostało nadane upoważnienie w systemie informatycznym, na jaki okres zostało wydane.

Sporządzając umowę powierzenia przetwarzania danych, której wzór zgodny z RODO najprawdopodobniej przygotuje specjalista z zakresu ochrony danych osobowych, działy rachunkowości powinny zwrócić uwagę na obszary nieuregulowane przez RODO, a mianowicie:

– zakres powierzanych danych, np. imię i nazwisko i PESEL, oraz kategorię osób, których dane będą powierzone, np. dane klientów,
– określenie miejsca, w którym będą przetwarzane dane, aby w przypadku skorzystania z prawa do kontroli było znane miejsce, do którego należy się udać,

– określenie podmiotu wydającego upoważnienia do przetwarzania danych osobowych,
– zwrot kar, odszkodowań w przypadku ich poniesienia przez administratora danych z powodu nieprzestrzegania RODO przez podmiot przetwarzający,
– zabezpieczenie danych osobowych po zakończeniu lub zerwaniu umowy o przetwarzanie danych, np. warunki ich zwrotu, obowiązek trwałego usunięcia z systemów informatycznych,
– obowiązki podmiotu przetwarzającego w przypadku konieczności zgłoszenia naruszenia danych do organu nadzorczego.

Księgowość na zlecenie – biuro rachunkowe

W przeciwieństwie do działów rachunkowości w podmiotach biura rachunkowe prowadzące usługowo rachunkowość są samodzielnymi administratorami danych osobowych i jednocześnie podmiotami przetwarzającymi dane osobowe powierzone przez inne podmioty. Muszą więc realizować wszystkie obowiązki ciążące na administratorze danych wskazane we wcześniejszym punkcie, w tym ten najtrudniejszy – informowanie osób fizycznych, których dane przetwarzają. Biura rachunkowe przetwarzają dane osób fizycznych szerszych kategorii niż rachunkowość wewnętrzna, mianowicie: właścicieli, klientów, dostawców, pracowników i emerytów, darczyńców, ale także osób niezwiązanych finansowo z biurem, np. gości. Biura jako samodzielni administratorzy danych są więc zobowiązani do przekazania klauzul informacyjnych wskazanym osobom, a w niektórych przypadkach do pozyskania zgód na przetwarzanie danych osobowych. Zgody w formie oświadczeń[8] woli będą wymagane zawsze w ramach działań marketingowych i promocyjnych biura. Zasady udzielania zgody określono w art. 7 i 8 RODO. Zdecydowanie częściej biura rachunkowe będą przekazywać informacje o przetwarzaniu danych osobowych, pozyskanych od osoby, której dane dotyczą[9]. W takiej informacji biuro jest zobowiązane podać:

1) kto jest administratorem danych;
2) w jakim celu będą wykorzystane dane, np. prowadzenia spraw kadrowo-płacowych;
3) podstawy upoważniającej biuro do przetwarzania danych, np. przetwarzanie jest niezbędne do wykonania umowy, gdzie stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem

[8] Zgodnie z definicją zgody wprowadzoną w RODO jest nią nie tylko oświadczenie woli, ale także wyraźne działanie potwierdzające wyrażenie zgody (art. 4 ust. 8 RODO), czyli np. przekazanie wniosku, przedstawienie się w czasie rozmowy telefonicznej, dostarczenie danych do podpisania umowy.

[9] Zgodnie z art. 13 i 14 RODO informacja o przetwarzaniu danych osobowych powinna być zróżnicowana w zależności od źródła danych: od osoby, której dane dotyczą, lub z innego źródła.

umowy i spełnienia obowiązku prawnego ciążącego na administratorze (art. 6 lub 9 RODO);
4) czy dane będą przekazywane odbiorcom danych, np. spółce partnerskiej;
5) przez jaki okres będą przetwarzane dane, np. do zakończenia zatrudnienia, a w zakresie obowiązku archiwizacji przez okres przewidziany przepisami prawa;
6) jakie prawa przysługują osobie fizycznej, np. w przypadku przetwarzania celem spełnienia obowiązku prawnego ciążącego na administratorze:
   a) żądania od administratora dostępu do swoich danych osobowych, ich sprostowania, ograniczenia przetwarzania, a także przenoszenia danych,
   b) wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych;
7) czy podanie danych jest dobrowolne, czy wynika z przepisów prawa, np. prawa pracy;
8) wskazanie, jakie będą przyczyny niepodania danych, np. niepodanie danych uniemożliwi podpisanie i realizację umowy;
9) czy podane dane będą podlegać zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.

Jako podmiot przetwarzający dane powierzone przez innych administratorów biuro działa wyłącznie na polecenie administratora. Do zadań biura w tym obszarze należy wspomaganie administratora w realizowaniu jego obowiązków (art. 26 RODO). Podstawą powierzenia danych może być zgodnie z RODO umowa powierzenia albo inny akt prawny. Określenie wzajemnych relacji między administratorem danych a biurem można jedynie określić w umowie, stąd też, mimo że w ustawie o rachunkowości jest dopuszczone usługowe prowadzenie rachunkowości, to podstawą prawną powierzenia danych przez biuro rachunkowe powinna być umowa powierzenia. Umowa ta jest organizacyjnym środkiem zabezpieczającym administratora danych przed naruszeniem RODO. Stąd też biura rachunkowe powinny skupić swoje wysiłki w tym obszarze na wynegocjowaniu zapisów, które nie będą je nadmiernie obciążały. W skrajnym przypadku administratorzy danych mogą podejmować próby przeniesienia na podmiot przetwarzający wielu swoich obowiązków. Na dziewięć zbadanych umów powierzenia zawartych przez podmioty o różnym statusie prawnym, własnościowym, reprezentujących zróżnicowane sfery i branże działalności oraz o różnej specyfice działalności zawartych z:

– kancelarią prawną,
– przychodnią w zakresie medycyny pracy,
– dostawcą systemu informatycznego, w tym finansowo-księgowego,
– pomiotem obsługującym płatną strefę parkowania,
– podmiotem obsługującym monitoring miejski,
– biurem rachunkowym,

– podmiotem świadczącym usługi marketingowe,
– podmiotem świadczącym usługi w zakresie bhp,
– firmą brokerską,

większość umów powierzenia miała charakter ogólny, zawarte w nich zapisy były powtórzeniem regulacji RODO albo jeszcze ustawy o ochronie danych osobowych z 1997 roku. W jednej administrator danych zawarł zapisy przenoszące obowiązek udzielania odpowiedzi osobom fizycznym na podmiot przetwarzający. W kolejnej administrator danych zrezygnował z prawa kontroli, ale zobowiązał podmiot przetwarzający do udzielania wielu informacji o prowadzonym przetwarzaniu w formie pisemnej na żądanie administratora. W pięciu zapisano prawo podmiotu przetwarzającego do podpowierzenia przetwarzania danych. Wszystkie zawierały obowiązek usunięcia danych w systemach informatycznych i przekazania dokumentacji papierowej po zakończeniu przetwarzania. Tylko jedna zawierała wszystkie pożądane elementy wymienione wyżej.

Podsumowanie

RODO jest kolejnym aktem prawym regulującym ochronę danych osobowych w Polsce. Poprzedni miał zasięg krajowy. Ustawa, o której mowa, zawierała w wielu obszarach identyczne albo podobne zapisy, np. w zakresie definicji pojęć, obowiązku informacyjnego, powierzania przetwarzania danych, wyznaczania administratora bezpieczeństwa informacji. Nowościami wprowadzonymi przez RODO są: bezpośrednia odpowiedzialność administratora danych za naruszenie przepisów wraz z odpowiedzialnością finansową, nawet do 20 mln euro lub 4% rocznego obrotu, zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu, nowe i rozszerzone prawa osób, których dane są przetwarzane, wyznaczanie inspektora danych z innym zakresem obowiązków niż administrator bezpieczeństwa informacji, rozszerzony obowiązek dokumentacyjny dla realizacji zasady rozliczalności, rozszerzony obowiązek informacyjny, nowe wymagania, które musi spełniać zgoda na przetwarzanie danych osobowych, obowiązek wykonania oceny skutków w zakresie ochrony danych. Przebadane podmioty w większości przypadków nie przestrzegały ustawy o ochronie danych osobowych. Ich działania w tym obszarze ograniczały się do wdrożenia Polityki bezpieczeństwa z instrukcją zarządzania systemami informatycznymi i wydania upoważnień do przetwarzania danych swoim pracownikom. W momencie wejścia w życie RODO stanęły przed problemem nie tyle modyfikacji stosowanych rozwiązań, co przed wdrożeniem niestosowanych dotychczas środków i zasad w wersji bardziej wymagającej niż dotychczas oraz przed wdrożeniem nowości. Działy rachunkowości w podmiotach, podobnie jak wszystkie inne komórki organizacyjne, muszą więc obecnie nauczyć się przetwarzać dane

osób fizycznych w sposób bardziej odpowiedzialny, świadomy zagrożeń i poufny. Zadania działów rachunkowości w porównaniu z komórkami merytorycznymi podmiotów nie obejmują spełniania obowiązku informacyjnego. Zgodnie z zapisami art. 14 ust. 4 RODO administrator danych, a w jego imieniu bezpośredni wykonawca ma obowiązek informować osoby o przetwarzaniu danych osobowych podczas ich pozyskiwania lub najpóźniej w momencie ujawnienia danych. Tymi bezpośrednimi wykonawcami będą głównie komórki merytoryczne, tj. dział sprzedaży, zaopatrzenia, organizacyjny, sekretariat.

Biura rachunkowe pełniące jednocześnie funkcję administratora danych dla „własnych" danych i podmiotu przetwarzającego dla danych powierzonych są zobowiązane do samodzielnego stosowania i przestrzegania wszystkich regulacji zawartych w RODO i nowej ustawie.

Bibliografia

Źródła

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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119/1 z 4.5.2016 r.)

Ustawa z dnia 29 września 1994 r. o rachunkowości **(**Dz. U. z 2018 r. poz. 395 ze zm.)

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r. ze zm.)

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

Literatura

Komunikat Ministerstwa Cyfryzacji i Ministerstwa Przedsiębiorczości i Technologii dotyczący stosowania przepisów unijnego ogólnego rozporządzenia o ochronie danych osobowych (RODO) w stosunku do sektora małych i średnich przedsiębiorstw, „Gazeta Podatkowa" 29.01.2018, Nr 9 (1466)

Internet

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 (ogólne rozporządzenie o ochronie danych) https://sip.legalis.pl/document-full.seam?documentId=mfrxilrtgm2tsnrrguytsltwmvzc4mjxgy3ti [dostęp 30.06-7.07. 2018]

Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679, https://bip.kprm.gov.pl/kpr/form/r7079293730832,Projekt-ustawy-o-zmianie-niektorych-ustaw-w-zwiazku-z-zapewnieniem-stosowania-ro.html [dostęp 5.07.2018]

Personal Data Protection in Accountancy

Summary

From 25th May 2018 all the members of European Union were committed to the General Data Protection Regulation (EU) 2016/679 from 27th April 2016 on data protection and privacy for all individuals, free flow of such data and on superseding the Data Protection Directive 95/46/EC to normalize standards on personal data protection. Accountancy led by internal units of an entity or by accounting offices must be adjusted to new requirements. More requirements must be met by accounting offices than by accounting departments which are internal parts of entities-administrators of personal data. Accounting offices are obliged to fulfil requirements of personal data administrators and processing entity. Internal accounting departments will be obliged to fulfil the requirements of the whole entity in the area of composing entrustment agreement, managing personal data processing etc. Accounting departments will not forward informative provisions to a person whose data will be processed by a data administrator.

Keywords

accountancy, accounting offices, personal data protection