Inspektor ochrony danych – miejsce w organizacji, rola i zadania

dr *Gabriela Bar*[1]

Na podstawie nowych przepisów o ochronie danych osobowych, zawartych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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)[2] wsparciem dla administratorów danych i podmiotów przetwarzających mają być inspektorzy ochrony danych (IOD). Ich rolą – podobnie jak poprzednio administratorów bezpieczeństwa informacji (ABI) – jest działanie na rzecz zgodnego z prawem przetwarzania danych osobowych, zarówno w jednostkach administracji publicznej, jak i w sektorze prywatnym. Celem niniejszego opracowania jest wskazanie miejsca IOD w organizacji, jego roli i zadań.

Uwagi wstępne

Koncepcja IOD nie jest w prawie europejskim nowa. Chociaż dyrektywa 95/46/WE[3] nie wprowadzała obowiązku wyznaczenia IOD, to umożliwiała (art. 18 ust. 2 oraz art. 20 ust. 2) powołanie tzw. urzędnika ds. ochrony danych osobowych (ang. *data protection official)*, a ponadto w ciągu wielu lat jej obowiązywania w niektórych państwach członkowskich rozwinęła się praktyka wyznaczania takich inspektorów.

Polska ustawa z 29.8.1997 r. o ochronie danych osobowych[4] także umożliwiała administratorom danych wyznaczenie osoby odpowiedzialnej za ochronę danych osobowych w organizacji, której funkcja została w art. 36a autonomicznie określona mianem „administratora bezpieczeństwa informacji", w skrócie ABI.

Jeszcze przed uchwaleniem i wejściem w życie RODO Grupa Robocza Art. 29 (obecnie Europejska Rada Ochrony Danych) podkreślała, że „wyznaczenie IDO może ułatwiać przestrzeganie przepisów z zakresu ochrony danych osobowych, umożliwiać budowanie przewagi konkurencyjnej na rynku oraz wdrożenie narzędzi rozliczalności (ocena skutków dla zakresie ochrony danych, przeprowadzanie lub ułatwianie audytów w zakresie bezpieczeństwa danych), a także zapewniać lepszą komunikację pomiędzy zainteresowanymi stronami (np. organami nadzoru, podmiotami danych i jednostkami biznesowymi w ramach organizacji)".

Wyznaczenie inspektora ochrony danych

Zgodnie z art. 37 ust. 1 RODO wyznaczenie inspektora ochrony danych (ang. *Data Protection Officer*, *DPO*) jest obowiązkowe w następujących przypadkach[5]:

1) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
2) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub
3) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych[6] albo danych osobowych dotyczących wyroków skazujących i naruszeń prawa.

Ustawodawca unijny nie definiuje „organu lub podmiotu publicznego", jednak pojęcie to zostało sprecyzowane w polskiej ustawie z 10.5.2018 r. o ochronie danych osobowych[7]. W art. 9 wskazuje się, że przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora należy rozumieć:

1) jednostki sektora finansów publicznych;
2) instytuty badawcze;
3) Narodowy Bank Polski.

Pojęcie jednostek sektora finansów publicznych definiuje art. 9 ustawy z 27.8.2009 r. o finansach publicznych[8], wskazując, że sektor ten tworzą: organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej

[1] Autorka jest radcą prawnym, partnerem zarządzającym w Szostek Bar i Partnerzy Kancelarii Prawnej.

[2] Dz.Urz. UE L119, s. 1; dalej jako: RODO.

[3] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.Urz. UE L Nr 281, s. 31.

[4] T,j. Dz.U. z 2016 r. poz. 922 ze zm.

[5] Zgodnie z art. 37(4) RODO przepisy unijne bądź krajowe mogą wymuszać powołanie IOD także w innych przypadkach.

[6] Zgodnie z art. 9 RODO są to dane osobowe ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

[7] Dz.U. poz. 1000 ze zm.; dalej jako: DaneOsobU. Ustawa ta weszła w życie 25.5.2018 r.

[8] T.j. Dz.U. z 2017 r. poz. 2077 ze zm.

i ochrony prawa oraz sądy i trybunały; jednostki samorządu terytorialnego oraz ich związki; związki metropolitalne; jednostki budżetowe; samorządowe zakłady budżetowe; agencje wykonawcze; instytucje gospodarki budżetowej; państwowe fundusze celowe; Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasa Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego; Narodowy Fundusz Zdrowia; samodzielne publiczne zakłady opieki zdrowotnej; uczelnie publiczne; Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne; państwowe i samorządowe instytucje kultury; inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem jednak przedsiębiorstw, instytutów badawczych, banków i spółek prawa handlowego.

Status instytutu badawczego oraz NBP jako państwowych osób prawnych regulują odpowiednio: ustawa z 30.4.2010 r. o instytutach badawczych[9] i ustawa z 29.8.1997 r. o Narodowym Banku Polskim[10].

Należy mieć na uwadze, iż wykonywanie zadań w interesie publicznym lub sprawowanie władzy publicznej może być nie tylko domeną organów lub podmiotów publicznych, ale również może być realizowane przez inne osoby fizyczne i prawne podlegające prawu publicznemu lub prywatnemu, w sektorach takich jak np. transport publiczny, dostarczanie wody i energii, infrastruktura drogowa, radiofonia i telewizja, budynki użyteczności publicznej albo organy powołane dla zawodów regulowanych. Grupa Robocza Art. 29 ds. Ochrony Danych (dalej jako: GR Art. 29) w Wytycznych dotyczące inspektorów ochrony danych, WP243, przyjętych 13.12.2016 r. oraz następnie zmienionych i przyjętych 5.4.2017 r. (dalej jako: Wytyczne GR) zaleca w takich przypadkach powołanie IOD w ramach dobrych praktyk, uznając, że sytuacja osób, których dane dotyczą, może być bardzo podobna do sytuacji przetwarzania ich danych przez organy lub podmioty publiczne[11].

Zgodnie z motywem 97 RODO przetwarzanie danych osobowych jest główną działalnością administratora, jeżeli oznacza jego zasadnicze, a nie poboczne czynności. „Główną działalnością" będzie zatem działalność kluczowa z punktu widzenia osiągnięcia celów administratora albo podmiotu przetwarzającego.

O monitorowaniu zachowania osób, których dane dotyczą, ustawodawca unijny wspomina w motywie 24 RODO: „Aby stwierdzić, czy czynność przetwarzania można uznać za »monitorowanie zachowania« osób, których dane dotyczą, należy ustalić, czy osoby fizyczne są obserwowane w Internecie, w tym także czy później potencjalnie stosowane są techniki przetwarzania danych polegające na profilowaniu osoby fizycznej, w szczególności w celu podjęcia decyzji jej dotyczącej lub przeanalizowania lub prognozowania jej osobistych preferencji, zachowań i postaw". Pojęcie to – według Wytycznych GR – obejmuje wszelkie formy śledzenia i profilowania, w tym na potrzeby reklam behawioralnych, przy czym nie jest ograniczone jedynie do środowiska online i śledzenie w sieci powinno być traktowane wyłącznie jako jeden z przykładów monitorowania zachowań osób, których dane dotyczą.

GR Art. 29 definiuje pojęcie „regularne" jako: stałe albo występujące w określonych odstępach czasu przez ustalony okres; cykliczne albo powtarzające się w określonym terminie; odbywające się stale lub okresowo. Z kolei pojęcie „systematyczne" może oznaczać: występujące zgodnie z określonym systemem; zaaranżowane, zorganizowane lub metodyczne; odbywające się w ramach generalnego planu zbierania danych; przeprowadzone w ramach określonej strategii. Do przykładów podanych w Wytycznych GR zaliczają się m.in. profilowanie i ocenianie do celów oceny ryzyka (np. do celów oceny ryzyka kredytowego, ustanawiania składek ubezpieczeniowych, zapobiegania oszustwom, wykrywania zjawisk związanych z praniem pieniędzy), śledzenie lokalizacji (np. przez aplikacje mobilne); programy lojalnościowe; reklama behawioralna; monitorowanie danych dotyczących zdrowia i kondycji fizycznej za pośrednictwem urządzeń przenośnych; monitoring wizyjny[12].

Wskazówki, jak rozumieć pojęcie „dużej skali", można znaleźć w motywie 91 RODO, który stanowi, że operacje przetwarzania o dużej skali to takie, „które służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko". Chodzi tu przy tym nie tylko o liczbę osób, ale także ilość danych i ich kategorii, okres i trwałość czynności przetwarzania oraz geograficzny zakres czynności przetwarzania. Jako przykład przetwarzania danych na dużą skalę Wytyczne GR wskazują: przetwarzanie danych do celów reklamy behawioralnej przez wyszukiwarki, przetwarzanie danych klientów przez banki albo ubezpieczycieli w ramach prowadzonej działalności lub przetwarzanie danych geolokalizacyjnych klientów w czasie rzeczywistym przez wyspecjalizowany podmiot na rzecz międzynarodowej sieci fast food do celów statystycznych[13].

W art. 37 ust. 1 lit. c) RODO nakłada na administratora obowiązek wyznaczenia IOD, gdy jego główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych z art. 9 ust. 1 RODO lub danych

[9] T.j. Dz.U. z 2018 r. poz. 736 ze zm.
[10] T.j. Dz.U. z 2017 r. poz. 1373 ze zm.
[11] Wytyczne dotyczące inspektorów ochrony danych (DPO), 16/EN WP 243 rew. 01, s. 7.
[12] Wytyczne…, s. 9–10.
[13] Wytyczne…, s. 9.

osobowych dotyczących wyroków skazujących i czynów zabronionych (art. 10 RODO).

Pojęcie „dużej skali" należy rozumieć w odniesieniu do tej przesłanki, podobnie jak zostało to opisane powyżej. Przetwarzanie danych osobowych nie powinno być uznawane za przetwarzanie na dużą skalę, jeżeli dotyczy danych osobowych pacjentów i jest dokonywane przez pojedynczego lekarza lub innego pracownika służby zdrowia (por. motyw 91 RODO).

Poziom wiedzy fachowej i kwalifikacje zawodowe

Artykuł 37(5) RODO stanowi, że „inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39". Niezbędny poziom wiedzy fachowej powinno się zaś ustalać w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają przetwarzane dane osobowe (motyw 97 RODO).

Mając na względzie powyższe przepisy oraz Wytyczne GR, należy uznać, że wiedza fachowa IOD obejmować powinna następujące elementy:

- wiedza z zakresu prawa ochrony danych osobowych: krajowego i europejskiego oraz umiejętność interpretacji przepisów prawa;
- znajomość praktyk w dziedzinie ochrony danych osobowych, w tym praktycznych aspektów wdrażania przepisów prawa w danej organizacji;
- praktyczna znajomość mechanizmów zarządzania ochroną danych (np. monitorowanie, przeprowadzanie kontroli, ocena ryzyka);
- znajomość zagadnień związanych z zastosowaniem technologii informacyjnych w przetwarzaniu danych osobowych, cyberbezpieczeństwem oraz architekturą systemów informatycznych;
- znajomość specyfiki branży, w której działa administrator lub procesor oraz wiedza o dokonywanych u danego administratora lub procesora czynnościach przetwarzania, procesach i systemach IT, w których są przetwarzane dane osobowe, oraz o kontrahentach, którym dane są powierzane do przetwarzania lub którym są przekazywane.

Choć art. 37 ust. 5 RODO nie wskazuje konkretnych kwalifikacji zawodowych, jakie należy brać pod uwagę, wyznaczając IOD, to wydaje się istotne – w świetle powyższych uwag – aby posiadał on wyższe wykształcenie, w szczególności prawnicze lub informatyczne. Przydatna jest też wiedza na temat danego sektora, a zatem w grę może wchodzić również inne wykształcenie kierunkowe.

W przypadku organów i podmiotów publicznych IOD powinien posiadać kwalifikacje w zakresie prawa i postępowania administracyjnego.

Dobrą praktyką może być uwzględnienie wytycznych dla inspektorów ochrony danych w instytucjach EU, w których zalecane jest wymaganie od IOD co najmniej siedmiu lat odpowiedniego doświadczenia, aby dana osoba mogła pełnić funkcję inspektora ochrony danych w instytucji lub organie, w których ochrona danych jest związana z podstawową ich działalnością lub które mają istotny wolumen operacji przetwarzania danych osobowych[14].

Do cech osobowych, jakimi IOD powinien się odznaczać, należą: uczciwość, etyka zawodowa, inicjatywa, dobra organizacja pracy, wytrwałość, dyskrecja, umiejętność radzenia sobie w trudnych sytuacjach, umiejętności interpersonalne: komunikacyjne, negocjacyjne czy umiejętność rozwiązywania konfliktów[15].

Wykonywanie zadań w sposób niezależny i brak konfliktu interesów

Artykuł 38 ust. 3 RODO wyznacza pewien zakres gwarancji, których celem jest umożliwianie IOD wykonywania obowiązków z odpowiednim stopniem niezależności w ramach organizacji. Administrator lub podmiot przetwarzający mają w szczególności zapewnić, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Motyw 97 RODO uzupełnia to o stwierdzenie, iż „inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny".

IOD ma wprawdzie możliwość wykonywania innych zadań i obowiązków w ramach współpracy z danym podmiotem, jednak „administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów" (art. 38 ust. 6 RODO).

W strukturze organizacyjnej IOD musi być tak umiejscowiony, aby był niezależny i aby nie dochodziło do konfliktu interesów z interesami jednostki (działu, zespołu, departamentu), w której on funkcjonuje. Rozwiązaniem zgodnym w RODO jest podleganie IOD bezpośrednio najwyższemu kierownictwu administratora lub podmiotu przetwarzającego (art. 38 ust. 3 zd. ostatnie RODO). Takie rozwiązanie jest rekomendowane także przez stowarzyszenie IOD (*Network of IODs*) dla instytucji i organów UE[16]. Wytyczne te stanowią, że jedną z najlepszych praktyk pomagającą zapewnić

[14] Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 z 14.10.2010 r., https://edps.europa.eu/sites/edp/files/publication/10-10-14_IOD_standards_en.pdf (dostęp z 18.5.2018 r.).

[15] *Ibidem*.

[16] *Ibidem*.

niezależność IOD jest zapewnienie, aby raportował on bezpośrednio do szefa instytucji lub organu, który powinien być odpowiedzialny za weryfikację wykonywania obowiązków przez inspektora ochrony danych zgodnie z rozporządzeniem. Bezpośrednia podległość zapewnia najwyższemu kierownictwu wiedzę na temat porad i zaleceń IOD w ramach wypełniania przez niego zadania informowania i doradzania administratorowi lub podmiotowi przetwarzającemu. W sytuacji podjęcia przez administratora lub podmiot przetwarzający decyzji niezgodnej z przepisami RODO i zaleceniami IOD ten powinien mieć możliwość jasnego przedstawienia swojej odrębnej opinii najwyższemu kierownictwu i osobom podejmującym decyzję.

W przypadku osób prawnych, w szczególności spółek prawa handlowego, najwyższym kierownictwem administratora lub procesora będzie zarząd.

IOD nie może otrzymywać instrukcji dotyczących sposobu rozpoznania sprawy, środków, jakie mają zostać podjęte, celu, jaki powinien zostać osiągnięty, czy też faktu, czy należy skontaktować się z organem nadzorczym. IOD nie może być obligowany do przyjęcia określonego stanowiska w sprawie z zakresu prawa ochrony danych, np. określonej wykładni przepisów.

Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny, co oznacza, że IOD nie może zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych. Stanowiska niekompatybilne z funkcją IOD (powodujące konflikt interesów) to m.in.: stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT), jak również niższe stanowiska, jeśli biorą udział w określaniu celów i sposobów przetwarzania danych[17].

Zadania IOD i zapewnienie możliwości ich realizacji

Zgodnie z art. 39 RODO do zadań IOD należą:

1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o ich obowiązkach wynikających z przepisów o ochronie danych osobowych i doradzanie im w tej sprawie;
2) monitorowanie przestrzegania obowiązujących przepisów o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
4) współpraca z organem nadzorczym oraz wypełnianie funkcji punktu kontaktowego dla organu nadzorczego.

IOD powinien – zgodnie z opracowanym planem swoich działań – informować, doradzać i rekomendować określone działania administratorowi lub procesorowi.

Artykuł 39 ust. 1 lit. a RODO nie tylko dotyczy obowiązków ochrony danych określonych przepisami RODO, lecz także wskazuje, iż obowiązki te mogą wynikać z przepisów odrębnych ustaw. W rezultacie w sytuacji, gdy organizacja funkcjonuje w sektorze dodatkowo regulowanym (np. banki), to należy uwzględnić odrębne przepisy regulujące ochronę danych osobowych i bezpieczeństwo informacji w ogóle.

W ramach monitorowania przestrzegania przepisów IOD powinien m.in.:

- zbierać informacje w celu identyfikacji procesów przetwarzania;
- analizować i sprawdzać zgodność tego przetwarzania z RODO i innymi odnośnymi przepisami prawa;
- przeprowadzać kontrole w zakresie prawidłowości przetwarzania danych w organizacji;
- rekomendować określone działania;
- przeprowadzać szkolenia personelu uczestniczącego w operacjach przetwarzania.

Wprawdzie do obowiązków administratora, a nie IOD, należy przeprowadzanie w określonych przypadkach oceny skutków dla ochrony danych, jednak art. 35 ust. 2 RODO nakłada na administratora obowiązek konsultowania się z IOD przy jej dokonywaniu. Natomiast w art. 39 ust. 1 lit. c) RODO określono obowiązek IOD udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych zgodnie z art. 35 RODO. Wobec tego administrator powinien konsultować z IOD co najmniej:

- fakt, czy należy przeprowadzić ocenę skutków dla ochrony danych;
- metodologię przeprowadzenia oceny skutków dla ochrony danych;
- fakt, czy należy przeprowadzić wewnętrzną ocenę skutków dla ochrony danych czy też zlecić ją podmiotowi zewnętrznemu;
- zastosowania konkretnych zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą;
- prawidłowość przeprowadzonej oceny skutków dla ochrony danych i zgodność jej wyników z wymogami ochrony danych.

[17] Wytyczne..., s. 17.

IOD ma pełnić funkcję punktu kontaktowego, by umożliwić organowi nadzorczemu dostęp do dokumentów i informacji w celu realizacji zadań, o których mowa w art. 57 RODO, jak również wykonywania uprawnień w zakresie prowadzonych postępowań, uprawnień naprawczych, uprawnień w zakresie wydawania zezwoleń oraz uprawnień doradczych, zgodnie z art. 58 RODO.

Wprawdzie IOD związany jest tajemnicą i poufnością dotyczącą wykonywania zadań IOD, ale zakaz ten nie wyłącza możliwości kontaktowania się IOD z organem nadzoru w celu uzyskania porady co do właściwej ścieżki postępowania w danych okolicznościach (art. 39 ust. 1 lit. e) RODO).

Należy zwrócić uwagę, że art. 39 ust. 1 RODO w wersji angielskiej stanowi, że IOD „*shall have »at least« the following tasks*" („do obowiązków IOD należy co najmniej"). W związku z tym zakres obowiązków IOD może być szerszy lub bardziej szczegółowo opisany, niż ma to miejsce w art. 39 ust. 1 RODO. W szczególności należy uznać za praktyczne rozwiązanie, aby IOD:

- stanowił punkt kontaktowy dla podmiotów danych – w sprawach związanych z realizacją ich praw;
- prowadził rejestr czynności przetwarzania lub rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora (art. 30 ust. 1 i 2 RODO);
- prowadził rejestr naruszeń i dokumentację wymaganą art. 33 ust. 5 RODO.

W związku z powyższymi zadaniami administrator lub procesor powinni zapewnić udział IOD we wszystkich zagadnieniach związanych z ochroną danych osobowych (art. 38 RODO), np. poprzez:

- udział w spotkaniach kadry kierowniczej (wyższego i średniego szczebla),
- udział w procesach decyzyjnych – otrzymywanie istotnych informacji w wyprzedzeniem,
- uwzględnianie opinii IOD na etapie projektowania procesów i w toku przetwarzania danych,
- konsultacje z IOD w przypadku stwierdzenia naruszenia albo innego incydentu związanego z danymi osobowymi.

Zespół wspierający IOD

W zależności od rozmiaru i struktury organizacji przydatne może być powołanie zespołu inspektora ochrony danych[18]. Wskazanie pozytywnego katalogu wszystkich możliwych zadań nakładanych na IOD oraz kierowany przez niego zespół nie jest możliwe, gdyż w dużej mierze zależeć on będzie od decyzji administratora lub procesora. Zadania te można jednak podzielić na trzy grupy:

1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o konkretnych obowiązkach spoczywających na nich na podstawie RODO i in. przepisów regulujących kwestie bezpieczeństwa przetwarzania danych osobowych;
2) merytoryczne wsparcie administratora danych, podmiotu przetwarzającego oraz pracowników w podejmowaniu działań zmierzających do zapewnienia zgodnego z prawem przetwarzania danych;
3) egzekwowanie przestrzegania zasad ochrony danych.

W przepisach prawa lub wytycznych GR Art. 29 nie zostały wskazane żadne ograniczenia co do tego, w jakim zakresie IOD może delegować swoje kompetencje na pracowników zespołu. Nie ulega jednak wątpliwości, iż w stosunkach zewnętrznych związanych z pełnioną przez IOD funkcją, zawsze powinien on występować osobiście. Podobnie rzecz ma się z podejmowaniem decyzji, co do przeprowadzenia kontroli w kwestii zgodności z RODO przetwarzania danych osobowych oraz wyrażania opinii co do działań rekomendowanych administratorowi. Szczegółowy podział kompetencji i obowiązków powinien określać regulamin zespołu IOD lub inne wewnętrzne regulacje w danej organizacji.

Zawiadomienie o wyznaczeniu IOD i publikowanie jego danych

Przepis art. 10 DaneOsobU wprowadza obowiązek zawiadomienia o wyznaczeniu IOD Prezesa Urzędu Ochrony Danych Osobowych, który prowadzi wewnętrzną ewidencję zawiadomień. Obowiązek ten spoczywa na podmiocie wyznaczającym: administratorze lub procesorze i powinien być spełniony w terminie 14 dni od dnia wyznaczenia IOD. Zawiadomienie obejmuje: imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora. O każdej zmianie danych należy zawiadomić w terminie 14 dni od dnia zaistnienia zmiany.

Zawiadomienia można dokonać wyłącznie w postaci elektronicznej – wymaga ono jednak opatrzenia kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

Oprócz konieczności zawiadomienia organu administrator i procesor są zobowiązani opublikować na swojej stronie internetowej – niezwłocznie po wyznaczeniu inspektora – następujące dane IOD: imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora (art. 11 DaneOsobU). Jeśli dany podmiot nie prowadzi własnej strony internetowej, to takiej publikacji powinien dokonać w sposób ogólnie dostępny w miejscu prowadzenia działalności.

Rozwiązanie to wydaje się niezgodne z RODO. Artykuł 37 ust. 7 RODO nie wymaga bowiem publikowania imienia i nazwiska inspektora, a jedynie podania jego danych kontaktowych, czyli np. adresu korespondencyjnego, numeru telefonu kontaktowego lub dedykowanego adresu e-mail. Zgodnie

[18] Wytyczne…, s. 15.

z Wytycznymi GR wskazanie dodatkowych informacji może być dobrą praktyką, ale decyzja o tym, czy w określonych okolicznościach udostępnienie tych danych może być konieczne lub pomocne, zależeć powinno od administratora lub podmiotu przetwarzającego i IOD[19].

Podsumowanie

Należy pamiętać, iż wyznaczenie IOD jest jednym z wielu działań, które organizacja powinna lub może podjąć, aby funkcjonować w zgodzie z przepisami z zakresu ochrony danych osobowych. Pomimo istotnej roli IOD i wagi wypełnianych przez niego zadań IOD nie jest osobiście odpowiedzialny za przestrzeganie tych przepisów przez podmiot, w ramach struktury którego działa. W każdym wypadku to administrator lub podmiot przetwarzający jest zobowiązany zapewnić i być w stanie wykazać, że przetwarzanie odbywa się zgodnie z RODO lub innymi odnośnymi przepisami prawa (art. 24 ust. 1 RODO).

[19] Wytyczne…, s. 14.

Słowa kluczowe: inspektor ochrony danych, IOD, DPO, RODO, GDPR, dane osobowe, przetwarzanie danych osobowych, podmioty danych, naruszenia danych osobowych, niezależność inspektora ochrony danych, konflikt interesów, zawiadomienie Prezesa Urzędu Ochrony Danych Osobowych.

Data Protection Supervisor – place in the organization, role and duties

Based on new regulations on personal data protection included in the regulation of the European Parliament and of the Council 2016/679 of 27.4.2016, in the matter of protection of natural persons in regard to processing of personal data and in the matter of free movement of such data and repealing the directive 95/46/EC (general data protection regulation), the support for data administrators and entities processing data are going to be data protection supervisors (DPS). The role of those supervisors – just like before with information security administrators (ISA) – is to act in the interest of processing data protection in accordance with law, both in public administration units, and in the private sector. The aim of the present study is to show the place of DPS in an organization, their roles and duties.

Keywords: data protection supervisor, DPS, GDPR, personal data, processing of personal data, subjects of data, violating personal data, independence of data protection supervisor, conflict of interest, notifying the President of Personal Data Protection Office.