Annales. Etyka w Życiu Gospodarczym / *Annales. Ethics in Economic Life* 2017
Vol. 20, No. 3, September 2017, 107–119
doi: http://dx.doi.org/10.18778/1899-2226.20.3.08

Arleta Nerka
Kozminski University
e-mail: arletan@kozminski.edu.pl

Powołanie inspektora ochrony danych jako przejaw społecznej odpowiedzialności biznesu

The Appointment of the Inspector General for Data Protection Officer as a sign of corporate social responsibility

The reform of the EU's personal data protection regulations introduces the institution of the Data Protection Officer, assigning it a key role in the new personal data protection system thereto. 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, builds the personal data protection model, wherein the main responsibility for adequate assessment of the risk associated with the processing of personal data and for the implementation of internal procedures to assure compliance of the referenced operations with the personal data protection regulations rests with a database administrator. Simultaneously, a database administrator should be capable of proving that he/she has duly met the requirements under the regulations, thus following the crucial rule for the processing of personal data, i.e. data accountability. The EU regulations describe the means and mechanisms to be used by a data processor to a lesser extent than those in force hitherto, focusing more on ensuring the standard of the protection of individual rights through data controllers' ethical and responsible activities.

The key part in the new personal data protection model will be played by the institution of the Data Protection Officer, intended to become a real guarantor of due observance of the personal data protection regulations. In this context, the appointment of the Data Protection Officer by database administrators, not bound to do so by law, should be judged a sign of the organization's corporate social responsibility for the impact of its decisions and activities on society through transparent and ethical conduct. It is therefore essential to emphasize the important function to be performed, the authority to be had, and the necessary preparatory action to be taken by the Data Protection Officer to that effect. The new regulations should be regarded as a chance to professionalize both the individuals, serving as information security officers and, in the near future, the data controllers, as well as the entire occupational group.

Keywords: Data Protection Officer, personal data protection, personal data administrator, corporate social responsibility

JEL Classification: K29, M14

1. Wprowadzenie

Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jedną z fundamentalnych zasad wyrażonych w art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej[1] oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej[2]. Przepisy te statuują prawo każdego człowieka do ochrony danych osobowych go dotyczących w kategoriach podstawowych praw i wolności. Wobec powszechności przetwarzania danych osobowych, zwłaszcza w cyberprzestrzeni, i związanych z tym zagrożeń dla praw i wolności, oczekiwanie stworzenia efektywnego mechanizmu ochrony praw podmiotów danych jest ze wszech miar uzasadnione. Wychodząc naprzeciw tym wyzwaniom, UE dokonała reformy przepisów o ochronie danych osobowych[3], której celem jest ujednolicenie modelu ochrony tychże danych.

Wśród wielu innowacyjnych rozwiązań służących ochronie prywatności rozporządzenie 2016/679 wprowadza instytucję inspektora ochrony danych (dalej: inspektor, IOD), wyznaczając mu kluczową rolę w nowym systemie ochrony danych osobowych. Inspektor został określony jako w pełni profesjonalny podmiot dysponujący kwalifikacjami zawodowymi, specjalistyczną wiedzą i doświadczeniem, posiadający odpowiednie przymioty osobiste, umiejętności interpersonalne i cechujący się wysokim standardem etycznym. Takie przygotowanie umożliwia skuteczną realizację zadań dotyczących ochrony danych osobowych w sferze działania administratora i podmiotu przetwarzającego. Trzeba zaznaczyć, że nie jest to jednak funkcja nowa – wynikała już z przepisów dyrektywy 95/46/WE[4], w której w art. 18 ust. 2 oraz art. 20 ust. 2 wprowadzono podstawę do ustanowienia tzw. urzędnika ds. ochrony danych osobowych (*Data Protection*

[1] Dz.U.UE.C.2007.303.1 z dnia 14 grudnia 2007 r.
[2] Wersja skonsolidowana: D.Urz.UE C 326 z 26.10.2012.
[3] Rozporządzenie 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*, Dz.Urz.UE L 119 z 4.05.2016, (dalej: rozporządzenie 2016/679 lub RODO); oraz dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.4.2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW*, Dz.Urz. L Nr 119 z 4.5.2016 r., s. 89.
[4] 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. L Nr 281 z 23.11.1995 r., s. 31 ze zm.

Official). Na grunt prawa krajowego fakultatywne powołanie administratora bezpieczeństwa informacji[5] przeniosła ustawa z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych*[6], jednakże od dnia 25 maja 2018 r. będzie stosowane w sposób bezpośredni rozporządzenie 2016/679, które przewiduje wymóg prawny wyznaczania inspektora w niektórych jednostkach.

Przedmiotem artykułu jest dokonanie charakterystyki obowiązku administratorów danych i podmiotów przetwarzających dotyczącego wyznaczania IOD oraz wskazanie, iż jego prawidłowa realizacja stanowi przejaw społecznej odpowiedzialności biznesu (*Corporate Social Responsibility*, CSR). Wyznaczenie inspektora danych z pewnością bowiem wpisuje się w CSR rozumianą jako przejrzysta oraz etyczna działalność przedsiębiorstwa, która determinuje zrównoważony rozwój i uwzględnia oczekiwania jego interesariuszy. Nie jest moją ambicją analiza koncepcji CSR, ale dla potrzeb niniejszych rozważań należy wskazać, że znajduje ona zastosowanie do wszystkich rodzajów organizacji, niezależnie od ich wielkości i lokalizacji, odnosi się zarówno do organizacji publicznych, prywatnych, jak i *non-profit*[7], jest także rekomendowana przez Komisję Europejską, m.in. poprzez ISO 26000[8]. Na doniosłość roli inspektora w mechanizmach ochrony danych osobowych wskazywała zresztą Komisja Europejska[9]. Dlatego celem opracowania jest dokonanie analizy obowiązku wyznaczenia IOD, ukształtowania jego pozycji w jednostce i ustalenia relacji pomiędzy administratorem danych a IOD w oparciu o wymagania prawne wynikające z RODO.

2. Zakres i charakter obowiązku administratorów i podmiotów przetwarzających wyznaczenia IOD w jednostce

RODO nakłada obowiązek wyznaczenia inspektora nie tylko na administratora[10], lecz również, co jest nowością, na podmiot przetwarzający[11], czyli procesora, pod warunkiem spełnienia określonych kryteriów. Przedmiotowy obowiązek może

[5] Nazwa autonomiczna, zob. szerzej: P. Fajgielski, *Pozycja prawna i zadania administratora bezpieczeństwa informacji po nowelizacji ustawy o ochronie danych osobowych*, „Monitor Prawniczy" 2015, nr 6 (dodatek), s. 3 i n.

[6] Tekst jedn. Dz.U. 2016 r., poz. 922.

[7] T. Gasiński, G. Piskalski, *Zrównoważony biznes. Podręcznik dla małych i średnich przedsiębiorstw*, Ministerstwo Gospodarki, Warszawa 2009, s. 89.

[8] H. Soroka-Potrzebna, *Zysk przedsiębiorstwa ważny, ale nie najważniejszy – społeczna odpowiedzialność biznesu*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2016, nr 419, s. 208 i n.

[9] *Report from the Commission – First Report on the implementation of the Data Protection Directive (95/46/EC)*, COM (2003) 265 Final z 15.5.2003 r., s. 18 i n., http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF (data dostępu 12. 04. 2017).

[10] Zgodnie z art. 4 pkt 7 rozporządzenia „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

[11] Zgodnie z art. 4 pkt 8 rozporządzenia „podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

również zostać rozszerzony na gruncie prawa krajowego na inne podmioty niż wskazane w RODO; taki obowiązek może także zostać wprowadzony prawem Unii. Poszukując podstaw omawianej regulacji, należy uwzględnić treść 97 motywu preambuły rozporządzenia 2016/679, zgodnie z którą:

> *Jeżeli przetwarzania dokonuje organ publiczny z wyjątkiem sądów lub niezależnych organów wymiaru sprawiedliwości w ramach sprawowania wymiaru sprawiedliwości lub jeżeli w sektorze prywatnym przetwarzania dokonuje administrator, którego główna działalność polega na operacjach przetwarzania wymagających regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę, lub jeżeli główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, to w monitorowaniu wewnętrznego przestrzegania RODO administrator lub podmiot przetwarzający powinni być wspomagani przez osobę dysponującą wiedzą fachową na temat prawa i praktyk w dziedzinie ochrony danych.*

W treści art. 37 rozporządzenia 2016/679 wskazano, że wyznaczenie inspektora jest dla administratora lub przetwarzającego obowiązkowe, gdy:

(1) przetwarzania dokonuje 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, o których mowa w art. 9 ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.

Oceniając okoliczności warunkujące konieczność wyznaczenia IOD, należy wskazać, że administrator powinien przede wszystkim wziąć pod uwagę kryterium kategorii przetwarzanych w jednostce danych, cel przetwarzania danych na dużą skalę, publiczny charakter podmiotu[12]. Mylna ocena przesłanek i rezygnacja z wyznaczenia inspektora grozi sankcją w postaci zastosowania przez organ nadzorczy niektórych instrumentów przewidzianych w art. 58 oraz kar pieniężnych na warunkach art. 83 RODO. Z kolei wyznaczenie IOD może być wzięte pod uwagę przy ustalaniu wysokości kary jako przejaw działania mającego na celu minimalizację ryzyka naruszenia przepisów prawa.

Zgodnie ze wskazaniami ujętymi w pierwszej przesłance, wyznaczenie inspektora jest powinnością organów władzy publicznej i innych podmiotów publicznych, z wyłączeniem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości. Oznacza to, że sądy są objęte obowiązkiem wyznaczenia inspektora, przy czym z zakresu jego zadań jest wyłączone monitorowanie przestrzega-

[12] *Unijna reforma ochrony danych osobowych. Analiza zmian*, red. A. Dmochowska, M. Zadrożny, Wydawnictwo C.H. Beck, Warszawa 2016, s. 36.

nia przepisów w odniesieniu do danych przetwarzanych w ramach czynności orzeczniczych sądu, np. danych zawartych w aktach sądowych lub bazach służących do wspomagania czynności orzeczniczych.

Pozostałe przesłanki konieczności wyznaczenia inspektora są dość niejednoznaczne z uwagi na posługiwanie się pojęciami o niedookreślonej treści, wymagającymi odrębnej refleksji. Przede wszystkim należy dokonać interpretacji użytego tam sformułowania „główna działalność". Motyw nr 97 preambuły rozporządzenia 2016/679 odnosi się do tego pojęcia, wskazując, iż: (…) *w sektorze prywatnym przetwarzanie danych osobowych jest główną działalnością administratora, jeżeli oznacza jego zasadnicze, a nie poboczne czynności*, co można również interpretować w taki sposób, że przetwarzanie danych jest koniecznym elementem funkcjonowania podmiotu i prowadzenia przez niego działalności w obrocie gospodarczym. Zgodnie z wytycznymi przyjętymi dnia 13.12.2016 r. przez Grupę Roboczą Art. 29[13] „główną działalnością" będzie działalność kluczowa z punktu widzenia osiągnięcia celów administratora albo podmiotu przetwarzającego dane. Jednocześnie pojęcia „głównej działalności" nie należy interpretować w sposób wyłączający działalność w zakresie przetwarzania danych nierozerwalnie związaną z działalnością główną administratora lub podmiotu przetwarzającego. Na przykład działalnością główną szpitali będzie zapewnianie opieki medycznej, natomiast prowadzenie efektywnej opieki medycznej nie byłoby możliwe bez przetwarzania danych medycznych, jak np. historii choroby pacjenta. W związku z tym czynności polegające na przetwarzaniu historii choroby pacjenta również powinny zostać zaklasyfikowane jako działalność główna, co oznacza, że szpitale będą miały obowiązek powołania IOD. Z drugiej strony wszystkie podmioty, spółki i inne organizacje prowadzą określone działania wspierające, np. sporządzając listę płac albo korzystając ze standardowej obsługi IT. Są to przykłady niezbędnych postępowań wspomagających prowadzenie działalności głównej. Mimo że są one konieczne lub niezbędne, zazwyczaj uznawane są raczej za działania dodatkowe niż za główną działalność[14].

Z kolei art. 37 ust. 1 pkt b) i c) uzależnia obowiązek powołania inspektora od przetwarzania danych osobowych na „dużą skalę". W treści rozporządzenia 2016/679 nie zdefiniowano tego pojęcia, a podpowiedzi interpretacyjne znajdują się w motywie 91 preambuły odnoszącym się do oceny skutków ryzyka, ale wskazującym jednocześnie, że:

> *Operacje przetwarzania o dużej skali – 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, na przykład (ze względu na swój szczególny charakter) gdy zgodnie ze stanem wiedzy technicznej stosowana jest na dużą skalę nowa technologia – oraz do innych operacji przetwarzania powodujących wyso-*

[13] *Wytyczne dotyczące inspektorów ochrony danych (DPO) przyjęte w dniu 13 grudnia 2016 r. przez Grupę Roboczą Art. 29 ds. Ochrony Danych*, WP 243 rew. 01, www.giodo.gov.pl (data dostępu: 28.04. 2016).

[14] Cf. K. Syska, *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań*, „Monitor Prawniczy" 2016, nr 20, dodatek, s. 76.

kie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, w szczególności gdy operacje te utrudniają osobom, których dane dotyczą, wykonywanie przysługujących im praw (…).

W opinii Grupy Roboczej Art. 29 nie jest możliwe wskazanie konkretnego rozmiaru zbioru danych czy liczby osób, których dane dotyczą, które determinowałyby „dużą skalę". Nie wyklucza to sytuacji, w której, wraz z rozwojem praktyki, ukształtują się standardy umożliwiające szczegółowe (np. ilościowe) zidentyfikowanie „dużej skali" w odniesieniu do określonych rodzajów przetwarzania. Grupa Robocza Art. 29 zaleca uwzględnianie następujących czynników przy określaniu, czy przetwarzanie następuje na „dużą skalę":

(1) liczba osób, których dane dotyczą – konkretna liczba albo procent określonej grupy społeczeństwa,
(2) zakres przetwarzanych danych osobowych,
(3) okres, przez jaki dane są przetwarzane,
(4) zakres geograficzny przetwarzania danych osobowych.

Innym niejasnym elementem przesłanki powołania inspektora z art. 37 ust. 1 lit. b) RODO jest przetwarzanie wymagające, ze względu na swój charakter, zakres lub cele, regularnego i systematycznego monitorowania osób, których dane dotyczą. Należy to rozumieć jako obserwację osób (poprzez przetwarzanie ich danych osobowych), następującą w regularnych odstępach lub w sposób ciągły oraz przeprowadzaną w oparciu o jakiś system, metodologię lub plan[15]. Grupa Robocza Art. 29 wskazuje jako przykłady „przetwarzania na dużą skalę", przetwarzanie danych:

(1) pacjentów w ramach standardowej działalności szpitala,
(2) osób korzystających z miejskiego systemu transportu publicznego,
(3) geolokalizacyjnych klientów międzynarodowej sieci restauracji typu *fast food*, do celów statystycznych, przez podmiot przetwarzający specjalizujący się w świadczeniu takich usług,
(4) klientów w ramach działalności firmy ubezpieczeniowej lub banku,
(5) za pomocą wyszukiwarki na potrzeby reklamy behawioralnej,
(6) przez dostawców usług telefonicznych lub internetowych.

Podsumowując, drugą przesłankę obowiązkowego wyznaczenia inspektora należałoby rozumieć w ten sposób, że konieczne jest jego powołanie w przypadku, gdy niezbędnym elementem głównej działalności podmiotu jest przetwarzanie danych osobowych na dużą skalę, a zarazem przetwarzanie to wymaga systematycznego monitorowania (obserwowania) osób. Jako przykłady podmiotów, które będą musiały wyznaczyć inspektora na podstawie tej przesłanki, wskazuje się np. sektor usług finansowych i ubezpieczeniowych, sektor usług IT, sektor usług transportu lotniczego[16].

Ostatnią, trzecią grupą jednostek zobowiązanych do wyznaczenia inspektora są podmioty, których główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o jakich mowa w art. 9 ust. 1 RODO,

[15] Ibidem.
[16] R. Heimes, S. Pfeifle, *Study: At least 28,000 DPOs needed to meet GDPR requirements*, https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/ (data dostępu 29.04.2017).

oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO (art. 37 ust. 1 lit. c). „Szczególne kategorie danych", zgodnie z art. 9 ust. 1 RODO, to dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej. W związku z tym wyznaczenie inspektora będzie obowiązkowe dla podmiotów świadczących usługi medyczne, np. prywatne centra medyczne, firmy ubezpieczeniowe świadczące usługi w zakresie ubezpieczeń na życie lub ubezpieczeń zdrowotnych, przedsiębiorcy z branży farmaceutycznej, a także podmioty przetwarzające dane o skazaniach.

Art. 37 ust. 2 i 3 RODO pozwala na wyznaczenie jednego inspektora przez grupę przedsiębiorstw lub przez kilka organów administracji publicznej. Jednak warunkiem wyznaczenia wspólnego inspektora przez kilka podmiotów jest to, aby można było z nim łatwo nawiązać kontakt z każdej jednostki organizacyjnej grupy. Natomiast przesłanką wyznaczenia jednego inspektora przez kilka organów administracji jest uwzględnienie ich struktury organizacyjnej i wielkości.

Podsumowując ten wątek rozważań, należy stwierdzić, że wyznaczenie inspektora zostało potraktowane jako obowiązkowe dla jednostek spełniających określone kryteria podmiotowe, natomiast w przypadku pozostałych pozostawiono to do ich uznania. Kryteria podmiotowe słusznie odnoszą się do rodzaju głównej działalności administratora lub podmiotu przetwarzającego, jednakże duży stopień ogólności ich sformułowania w praktyce może stanowić problem przy ustalaniu, które podmioty powinny inspektora wyznaczyć. Zgodnie z art. 37 ust. 4 rozporządzenia 2016/679 konieczność powołania IOD mogą przewidywać inne przepisy unijne lub krajowe, co ustawodawcy krajowemu otwiera drogę do rozszerzenia obowiązku wyznaczenia IOD bądź doprecyzowania przepisów RODO wprowadzających obligatoryjność jego powołania.

3. Warunki selekcyjne wyznaczenia inspektora ochrony danych

Rozporządzenie 2016/679 w art. 37 ust. 5 stawia wobec kandydata na inspektora przede wszystkim wymagania merytoryczne dotyczące 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. Oceny spełnienia wskazanych wymagań zawodowych dokonuje jednostka wyznaczająca. W pierwszym rzędzie IOD musi legitymować się posiadaniem pogłębionej wiedzy w obszarze europejskich i krajowych przepisów dotyczących ochrony danych osobowych. Zgodnie z motywem 97 preambuły odpowiedni poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez administratora lub podmiot przetwarzający. Grupa Robocza Art. 29 opisuje wy-

magany poziom wiedzy w zakresie współmiernym do charakteru, skomplikowania i liczby danych przetwarzanych w ramach jednostki. Wynika stąd, że RODO kładzie duży nacisk na praktyczne przygotowanie inspektora do pracy, co wydaje się słuszne z uwagi na brak świadomości lub dość niski poziom wiedzy dotyczącej ochrony danych osobowych reprezentowany przez osoby zarządzające jednostkami organizacyjnymi. Wiedza w tym obszarze jest niezbędna dla prawidłowej oceny ryzyka naruszenia prywatności przy podejmowaniu decyzji biznesowych i organizacyjnych wiążących się z przetwarzaniem danych. Inspektor ma służyć profesjonalnym wsparciem, a ono wymaga nie tylko wiedzy, lecz i praktycznego przygotowania popartego doświadczeniem zawodowym. W związku z tym selekcja IOD powinna być dokonana z zachowaniem należytej staranności i uwzględniać okoliczności dotyczące jednostki, w szczególności charakter przetwarzania danych w ramach podmiotu.

Z kolei warunek możliwości wypełniania zadań powinien być interpretowany zarówno przez pryzmat właściwości osobowych i umiejętności DPO, np. komunikacji, przekazywania wiedzy i prowadzenia szkoleń, jak również jego pozycji w strukturach jednostki. Wymagania dotyczące cech osobowych powinny dotyczyć profesjonalnego podejścia do pracy i wysokiego poziomu etyki zawodowej, niezbędnego przy wykonywaniu zawodu IOD.

4. Charakterystyka zadań inspektora w świetle rozporządzenia 2016/679

Zadania inspektora wyszczególnione zostały przede wszystkim w art. 39 ust. 1 RODO, jednakże inne jego obowiązki można wyinterpretować z treści innych przepisów. Nawet pobieżna ich lektura nasuwa wniosek, iż część zadań jest ukierunkowana na działania wewnątrz jednostki, a część wiąże się z jej reprezentacją na zewnątrz – głównie wobec organu nadzorczego i podmiotów danych.

W pierwszym rzędzie zostały wymienione obowiązki o charakterze edukacyjnym i doradczym, polegające na informowaniu administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o powinnościach spoczywających na nich na mocy rozporządzenia 2016/679 oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzaniu im w tej sprawie. Wskazują one na rolę, jaką prawodawca przypisuje inspektorowi w relacjach z jednostką wyznaczającą, mianowicie informatora i doradcy, co przekłada się na swoiste „bycie" źródłem wiedzy (biegłym) i wsparcia praktycznego przy realizacji zadań wynikających z RODO.

Kolejny obowiązek związany jest z monitorowaniem przestrzegania przepisów dotyczących ochrony danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych. W jego ramach mieszczą się podział zadań, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty. Tak określone czynności można zakwalifikować jako szeroko pojęty nadzór nad zgod-

nością działań administratora z przepisami dotyczącymi ochrony danych oraz z przyjętą polityką ochrony danych (tzw. „monitorowanie"). Z obowiązkiem tym jest skorelowany kolejny, polegający na udzielaniu na żądanie zaleceń co do oceny skutków dla ochrony danych[17] oraz monitorowanie ich wykonania zgodnie z art. 35. Przepis ten wskazuje, że konieczność dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych jeszcze przed rozpoczęciem przetwarzania zachodzi, gdy dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Powinność ta stanowi nową jakość w obszarze przetwarzania danych osobowych, którą ocenia się jako kluczowe zadanie administratorów danych, a wykonanie go jest z kolei niezbędne dla zapewnienia realizacji rozliczalności danych[18] przez ich administratora. Konsultacja z inspektorem, o ile został przez administratora powołany, jest obowiązkowa w przypadku przeprowadzania oceny skutków, przy czym przepis nie egzemplifikuje konkretnych obowiązków inspektora. Natomiast charakter szacowania ryzyka wskazuje, że powinny one polegać na analizie projektowanych czynności i mechanizmów przetwarzania danych oraz dokonaniu ich oceny z punktu widzenia przepisów o ochronie danych. W oparciu o poczynione ustalenia inspektor powinien zaproponować rekomendacje co do planowanych operacji przetwarzania danych, mając na uwadze eliminację lub zmniejszenie ryzyka naruszenia praw lub wolności osób, których dane dotyczą.

W sferze reprezentacji zewnętrznej inspektor realizuje zadania polegające na współpracy z organem nadzorczym oraz pełnieniu funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenia konsultacji we wszelkich innych sprawach. Można z tego wnioskować, że inspektor powinien odpowiadać na wszelkie pytania organu nadzoru dotyczące przetwarzania danych w organizacji.

Inne zadania IOD wynikają chociażby z art. 38 ust. 4 rozporządzenia 2016/679 – zgodnie z nim osoby, których dane są przetwarzane, mogą się kontaktować z inspektorem we wszystkich sprawach dotyczących przetwarzania ich danych. Tak określonemu prawu podmiotów danych odpowiada ciążący na inspektorze obowiązek w postaci udzielania odpowiedzi na ich wątpliwości. Realizacja tego zadania wymaga odpowiedniego przygotowania merytorycznego i praktycznego poprzez opracowanie procedury obsługi wniosków. Administrator lub podmiot przetwarzający mogą powierzyć inspektorowi wykonywanie innych zadań związanych z ochroną danych, chociażby prowadzenie rejestru czynności

[17] A. Mednis, *Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych*, „Monitor Prawniczy" 2016, nr 20 (dodatek), s. 29 i n.

[18] Art. 5 ust. 2 rozporządzenia statuuje zasadę rozliczalności, zgodnie z którą administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 (określającego zasady dotyczące przetwarzania danych osobowych) i musi być w stanie wykazać ich przestrzeganie.

przetwarzania danych osobowych, o którym mowa w art. 30 RODO. Poza tym, zgodnie z art. 38 ust. 6 RODO, inspektor może wykonywać inne obowiązki, przy czym podmiot go wyznaczający musi zapewnić, aby nie powodowało to konfliktu interesów.

Rozbudowane obowiązki nałożone na inspektora oraz ich charakter jednoznacznie w moim przekonaniu wskazują, iż nastąpił wzrost znaczenia IOD w systemie ochrony danych osobowych. Bezspornie wniosek taki uzasadnia powierzenie inspektorowi nadzoru nad zgodnością działań administratora i podmiotu przetwarzającego z obowiązującymi przepisami.

5. Status inspektora ochrony danych w jednostce

Wyznaczenie IOD wiąże się z podjęciem przez administratora danych decyzji o formie jego zatrudnienia – czy ma być nim pracownik zatrudniony w jednostce, czy osoba zewnętrzna. Decydując się na inspektora wewnętrznego, administrator danych ma wybór w zakresie zatrudnienia pracowniczego, podporządkowanego przepisom prawa pracy, bądź zatrudnienia cywilnoprawnego ze wskazaniem na umowę-zlecenie. Korzystając z możliwości powierzenia funkcji inspektora osobie zewnętrznej, zawiera umowę o świadczeniu usług w ramach outsourcingu. Podjęcie decyzji w tym zakresie wymaga zdefiniowania potrzeb jednostki związanych z ochroną danych osobowych, uwzględnienia przyjętych zasad polityki kadrowej, analizy kosztów zatrudnienia oraz kwestii odpowiedzialności prawnej, itp. W mojej ocenie kryteriami podstawowymi wyboru inspektora powinny być jego profesjonalizm i etyka w wykonywaniu zadań. Nie bez znaczenia będzie tutaj świadomość administratora, że niezależnie od wyboru podstawy zatrudnienia nie istnieje prawna możliwość przeniesienia odpowiedzialności spoczywającej z mocy prawa na administratorze na inspektora, nawet pełniącego funkcję zewnętrznie.

Wyznaczenie IOD nie ma charakteru kadencyjnego, czas trwania nawiązanego stosunku prawnego jest uzależniony od woli stron, przy czym nie jest wykluczone przyjęcie w tym zakresie odrębnych regulacji na gruncie prawa krajowego. Rozporządzenie 2016/679 nie wypowiada się również na temat zagadnień odwołania IOD ze stanowiska, wskazując jedynie w art. 38 ust. 3, że inspektor nie może być odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. W rozporządzeniu 2016/679 wprost nie jest wskazany obowiązek zawiadomienia organu nadzoru o odwołaniu inspektora, jednak należy uznać, że skoro inspektor ma pełnić funkcję punktu kontaktowego dla organu nadzoru, to organ ten musi mieć aktualną informację co do niego.

Niezbędnym warunkiem prawidłowości wykonywania zadań przez IOD jest zagwarantowanie mu w tym zakresie niezależności. Wyrazem jej zapewnienia jest wymóg wyrażony w art. 38 ust. 3 RODO, polegający na bezpośredniej podległości inspektora najwyższemu kierownictwu administratora lub podmiotu przetwarzającego (dyrektor, zarząd itp.). Wysokie umiejscowienie w strukturze jednostki jest

warunkiem podstawowym dla faktycznej możliwości realizacji obowiązków przez IOD. Poza tym charakter i rozległość zadań inspektora uzasadniają powinności osób zarządzających jednostką w zakresie:

(1) zapewnienia, by inspektor był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych (art. 38 ust. 1 RODO),
(2) wspierania inspektora w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej (art. 38 ust. 2 RODO),
(3) zapewnienia, by inspektor nie otrzymywał instrukcji dotyczących wykonywania tych zadań (art. 38 ust. 3 RODO).

Inspektor nie może być także odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań (art. 38 ust. 3 RODO). Artykuł 38 ust. 5 RODO wprowadza obowiązek zachowania przez inspektora tajemnicy lub poufności w zakresie wykonywania swojej pracy. Obowiązek ten może być doprecyzowany zgodnie z prawem Unii lub prawem państwa członkowskiego.

Zgodnie z art. 37 ust. 7 rozporządzenia 2016/679 administrator lub podmiot przetwarzający zawiadamiają organ nadzorczy o danych kontaktowych inspektora, a tym samym o jego wyznaczeniu. Z RODO nie wynika, jakie konkretnie dane powinny być przekazane organowi nadzorczemu[19], jednakże oczywiste wydaje się, że „dane kontaktowe" obejmują informacje pozwalające na nawiązanie kontaktu, np. nr telefonu, adres e-mail, adres korespondencyjny. Poza tym administrator w ramach wypełniania obowiązku informacyjnego powinien przekazać osobie, której dane dotyczą, dane kontaktowe inspektora, o ile ten został wyznaczony.

6. Podsumowanie

Rozporządzenie 2016/679 buduje model ochrony danych osobowych, w którym to przede wszystkim na ich administratorze ciąży odpowiedzialność za właściwą ocenę ryzyka związanego z przetwarzaniem danych osobowych i wdrożenie wewnętrznych procedur zapewniających zgodność takich operacji z przepisami. Jednocześnie administrator danych powinien być w stanie wykazać, że właściwie spełnił wymogi określone przepisami, realizując w ten sposób wiodącą zasadę przetwarzania danych – rozliczalność danych. Przepisy UE, w mniejszym stopniu niż dotychczas obowiązujące, charakteryzują środki i mechanizmy podlegające zastosowaniu przez podmioty przetwarzające, koncentrując się raczej na zapewnieniu standardu ochrony praw jednostki poprzez odpowiedzialne i etyczne działanie administratorów danych. Takie rozwiązanie wzmaga prawną i etyczną odpowiedzialność administratorów za niebezpieczeństwo naruszenia prywatności człowieka, w świetle czego wspomożenie się zatrudnieniem profesjonalisty, czyli inspektora, należy postrzegać w kategoriach CSR. Można przyjąć, że adresatem,

[19] P. Fajgielski, *Ogólne rozporządzenie o ochronie danych – co nas czeka?* „ABI EXPERT" 2016, nr 1, s. 11.

a zarazem beneficjentem unormowań RODO jest osoba fizyczna, a w szerszym ujęciu – społeczeństwo. Paralelnie do niego na znaczeniu zyskują działania podejmowane przez odpowiedzialną firmę. Może ona pomnażać kapitał społecznego zaufania poprzez konsekwentnie prowadzoną politykę odpowiedzialnego zarządzania danymi osobowymi.

Instytucja IOD będzie odgrywała kluczową rolę w nowym modelu ochrony danych osobowych, ponieważ została zaprojektowana jako swoisty gwarant właściwego przestrzegania przepisów o ochronie danych osobowych. Celowi temu służą stawiane mu wymagania dotyczące kwalifikacji zawodowych, wiedzy, doświadczenia, umiejętności, warunku ustawicznego uczenia się, kompetencji społecznych i spełniania standardów etycznych. Istotne jest zatem podkreślenie ważnej roli, jaką pełnić ma IOD, kompetencji, które ma posiadać, oraz niezbędnych działań, aby do tego się przygotować. Nowe przepisy należy oceniać jako szansę na profesjonalizację przyszłych inspektorów ochrony danych, jak również całej grupy zawodowej.

RODO nie wprowadza bezwzględnego obowiązku wyznaczenia inspektora przez wszystkich administratorów danych lub podmioty przetwarzające występujące w obrocie, przyjmując jako zasadę fakultatywność wyznaczenia IOD. Jednakże na negatywną ocenę zasługuje posługiwanie się nieostrymi pojęciami w przesłankach obligatoryjnego wyznaczenia inspektora. Nie jest bowiem oczywiste, w jakich okolicznościach inspektor powinien zostać powołany i w związku z tym, kiedy jego niewyznaczenie może skutkować odpowiedzialnością administracyjną i finansową egzekwowaną przez organ nadzorczy. Przesłanki wyznaczenia inspektora powinny więc być doprecyzowane na poziomie ustawodawstwa krajowego bądź we wskazówkach i opiniach organów ochrony danych.

Oceniając przyjęte rozwiązania, należy stwierdzić, że RODO realizuje założenie upowszechnienia powoływania inspektorów, co daje asumpt do stwierdzenia, iż wyznaczenie IOD stanowi przejaw społecznej odpowiedzialności biznesu. Rozwiązania RODO zostały podyktowane potrzebą zapewnienia efektywnej ochrony danych osobowych podmiotów danych w obrocie gospodarczym w obliczu zagrożeń dla prywatności człowieka.

Bibliografia

Fajgielski P., *Ogólne rozporządzenie o ochronie danych – co nas czeka?*, „ABI EXPERT" 2016, nr 1.

Fajgielski P., *Pozycja prawna i zadania administratora bezpieczeństwa informacji po nowelizacji ustawy o ochronie danych osobowych*, „Monitor Prawniczy" 2015, nr 6 (dodatek).

Gasiński T., G. Piskalski, *Zrównoważony biznes. Podręcznik dla małych i średnich przedsiębiorstw*, Ministerstwo Gospodarki, Warszawa 2009.

Heimes R., S. Pfeifle, *Study: At least 28,000 DPOs needed to meet GDPR requirements*, https://iapp.org/news/a/study-at-least-28000-dpos-needed-to-meet-gdpr-requirements/.

Mednis A., *Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych*, „Monitor Prawniczy" 2016, nr 20 (dodatek).

Report from the Commission – First Report on the implementation of the Data Protection Directive (95/46/EC), COM (2003) 265 Final z 15.5.2003 r., http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF.

Soroka-Potrzebna H., *Zysk przedsiębiorstwa ważny, ale nie najważniejszy – społeczna odpowiedzialność biznesu*, Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu 2016, nr 419.

Syska K., *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań*, „Monitor Prawniczy" 2016, nr 20, dodatek.

Unijna reforma ochrony danych osobowych. Analiza zmian, red. A. Dmochowska, M. Zadrożny, Wydawnictwo C.H. Beck, Warszawa 2016.

Wytyczne dotyczące inspektorów ochrony danych (DPO) przyjęte w dniu 13 grudnia 2016 r. przez Grupę Roboczą Art. 29 ds. Ochrony Danych, WP 243 rew.01, www.giodo.gov.pl.

Akty prawne

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.4.2016 r. *w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW, Dz.Urz. L Nr 119 z 4.5.2016 r.*

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. L Nr 281 z 23.11.1995 r., s. 31 ze zm.*

Karta praw podstawowych Unii Europejskiej, Dz.U. UE.C.2007.303.1 z dnia 14 grudnia 2007 r.

Rozporządzenie 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, Dz.Urz. UE L 119 z 4.05.2016.*

Traktat o funkcjonowaniu Unii Europejskiej, wersja skonsolidowana, D.Urz. UE C 326 z 26.10.2012.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Tekst jedn. Dz.U. z 2016 r., poz. 922.