Katalog Praw Przedsiębiorców

Inspektor ochrony danych „IOD”

ZESZYT 8.

Opracowanie: Prof. nadzw. dr hab. Maciej Rogalski
Dworzyński Rogalski Kancelaria Radców Prawnych

Katalog Praw Przedsiębiorców

Inspektor ochrony danych „IOD”

ZESZYT 8.

Opracowanie: Prof. nadzw. dr hab. Maciej Rogalski
Dworzyński Rogalski Kancelaria Radców Prawnych

O KANCELARII

Założycielami Kancelarii są radcowie prawni: prof. nadzw. dr hab. Maciej Rogalski oraz Adrian Dworzyński, prawnicy z ponad dwudziestoletnim doświadczeniem.

Naszym celem jest świadczenie usług prawnych w sposób zapewniający praktyczne i skuteczne rozwiązania, z naciskiem na biznesowe podejście oraz identyfikację i minimalizację ryzyka prawnego i regulacyjnego.

Przez wiele lat kierowaliśmy zespołami prawnymi największych polskich przedsiębiorstw. Łączymy w sposób szczególny umiejętność analizy zagadnień z perspektywy doradcy zewnętrznego oraz zarządzającego sprawami prawnymi firm (ryzykiem prawnym i regulacyjnym).

Nasz zespół tworzą prawnicy z dużym doświadczeniem praktycznym oraz specjalistyczną wiedzą. Współpracujemy także z doświadczonymi prawnikami o uzupełniających się specjalizacjach, w większości współpracujących z nami co najmniej kilka lat.

Szeroka praktyka i różnorodne, wszechstronne doświadczenie umożliwiają, w zależności od potrzeb klientów, pełną obsługę prawną firmy, tj. uwzględniającą wszelkie aspekty prawne jej działalności, skoordynowaną, kompleksową obsługę skomplikowanych projektów, jak również doradztwo i reprezentację przy indywidualnych sprawach, w tym procesach sądowych i postępowaniach administracyjnych.

dworzynskirogalski.pl

1. Wstęp.

Omówimy nowe rozporządzenie o ochronie danych osobowych, w szczególności w kontekście statusu nowego podmiotu zajmującego się ochroną danych osobowych tj. inspektora ochrony danych („IOD"). Podmiot ten zastąpi obecnego administratora bezpieczeństwa informacji („ABI").

Status inspektora ochrony danych jest uregulowany w Rozporządzeniu 2016/679 z 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady UE 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. L Nr 199 z 4 maja 2016 r., s. 1-88) („RODO")

W zakresie wyznaczania IOD uregulowania RODO odbiegają od dotychczasowych uregulowań w ustawie o ochronie danych osobowych („u.o.d.o."). Administrator oraz podmiot przetwarzający wyznaczają inspektora ochrony danych w przypadkach wskazanych w RODO.

Zgodnie z motywem 97 preambuły RODO: *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 niniejszego rozporządzenia administrator lub podmiot przetwarzający powinni być wspomagani przez osobę dysponującą wiedzą fachową na temat prawa i praktyk w dziedzinie ochrony danych. W sektorze prywatnym przetwarzanie danych osobowych jest główną działalnością administratora, jeżeli oznacza jego zasadnicze, a nie poboczne czynności.*

2. Definicja administratora i obowiązek powołania inspektora ochrony danych dla organizacji lub grupy organizacji.

Administrator w rozumieniu art. 4 pkt 7 RODO *oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub* wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Natomiast podmiot przetwarzający w rozumieniu art. 4 pkt 8 RODO *oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.*

Zgodnie z art. 37 ust. 1 RODO istnieje obowiązek wyznaczenia inspektora w trzech przypadkach. Zgodnie z art. 37 ust. 1 RODO, administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:

- *przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;*

- *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*

- *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 skazującychi naruszeń prawa, o czym mowa w art. 10.*

Wytyczne zalecają uwzględnianie następujących czynników przy określaniu, czy przetwarzanie następuje na „dużą skalę":

- liczba osób, których dane dotyczą – konkretna liczba albo procent określonej grupy społeczeństwa;

- zakres przetwarzanych danych osobowych;
- okres, przez jaki dane są przetwarzane;
- zakres geograficzny przetwarzania danych osobowych.

Wytyczne wskazują następujące przykłady „przetwarzania na dużą skalę":

- przetwarzanie danych pacjentów przez szpital w ramach prowadzonej działalności;
- przetwarzanie danych osób korzystających ze środków komunikacji miejskiej;
- przetwarzanie danych geo-lokalizacyjnych w czasie rzeczywistym przed wyspecjalizowany podmiot na rzecz międzynarodowej sieci fast food do celów statystycznych;
- przetwarzanie danych klientów przez banki albo ubezpieczycieli w ramach prowadzonej działalności;
- przetwarzanie danych do celów reklamy behawioralnej przez wyszukiwarki;
- przetwarzanie danych (dotyczących treści, ruchu, lokalizacji) przez dostawców usług telefonicznych lub internetowych.

Wytyczne wskazują także przykłady przetwarzania niemieszczącego się w definicji „dużej skali":

- przetwarzanie danych pacjentów – klientów, dokonywane przez pojedynczego lekarza;

- przetwarzanie danych dotyczących wyroków skazujących lub naruszeń prawa przez adwokata lub radcę prawnego.

Pojęcie „regularnego i systematycznego monitorowania" nie jest zdefiniowane w RODO. „Monitorowanie zachowania osób, których dane dotyczą" wyjaśnia motyw 24 RODO. Pojęcie to obejmuje wszelkie formy śledzenia i profilowania w sieci, w tym na potrzeby reklam behawioralnych (pojęcie nie jest ograniczone do środowiska online; śledzenie w sieci to jeden z przykładów monitorowania zachowań osób, których dane dotyczą).

GR definiuje „regularne" jako jedno lub więcej z następujących pojęć:

- stałe albo występujące w określonych odstępach czasu przez ustalony okres;

- cykliczne albo powtarzające się w określonym terminie;
- odbywające się stale lub okresowo.

GR definiuje także „systematyczne" jako jedno lub więcej z następujących pojęć:

- występujące zgodnie z określonym systemem;
- zaaranżowane, zorganizowane lub metodyczne;
- odbywające się w ramach generalnego planu zbierania danych;
- przeprowadzone w ramach określonej strategii.

Można podać następujące przykłady: świadczenie usług telekomunikacyjnych; profilowanie i ocenianie dla celów oceny ryzyka, na przykład dla celów oceny ryzyka kredytowego, ustanawiania składek ubezpieczeniowych, zapobiegania oszustwom, wykrywania prania pieniędzy; śledzenie lokalizacji, na przykład w aplikacjach telefonicznych; programy lojalnościowe; reklama behawioralna; monitorowanie danych o stanie zdrowia za pośrednictwem urządzeń przenośnych; monitoring wizyjny; urządzenia skomunikowane np. inteligentne liczniki, inteligentne samochody, automatyka domowa, etc. W celu stwierdzenia czy czynność przetwarzania można uznać za „monitorowanie zachowania" osób, których dane dotyczą, należy ustalić, czy osoby fizyczne są obserwowane w internecie.

Przepis art. 37 ust. 4 RODO przewiduje możliwość wyznaczenia inspektora w innych jeszcze przypadkach. Zgodnie z art. 37 ust. 4 RODO, *w przypadkach innych niż te, o których mowa w art. 37 ust. 1, administrator, podmiot przetwarzający, zrzeszenia lub inne podmioty reprezentujące określone kategorie administratorów lub podmiotów przetwarzających mogą wyznaczyć lub jeżeli wymaga tego prawo Unii lub prawo państwa członkowskiego, wyznaczają inspektora ochrony danych. Inspektor ochrony danych może działać w imieniu takich zrzeszeń i innych podmiotów reprezentujących administratorów lub podmioty przetwarzające.*

Grupa Robocza („GR") zaleca administratorom i podmiotom przetwarzającym stworzenie wewnętrznej procedury w celu ustalenia obowiązku bądź braku obowiązku wyznaczenia inspektora.

W sytuacji w której podmiot dobrowolnie decyduje się na wyznaczenie inspektora, wymagania wskazane w artykule 37 i 39 RODO stosuje się odpowiednio do jego wyznaczenia, statusu i zadań, tak jakby wyznaczenie było obowiązkowe. W takiej sytuacji konieczne jest wyznaczenie pracownika (zatrudnienie zewnętrznego konsultanta) do wypełniania zadań związanych z ochroną danych osobowych. Nazwa stanowiska, status pracownika, pozycja i zadania nie mogą wprowadzać w błąd. Wskazane jest poinformowanie pracowników organizacji, jak również organów ochrony danych, osób, których dane dotyczą, i ogółu społeczeństwa, iż osoba zatrudniona nie jest inspektorem w świetle przepisów RODO.

Przepis art. 37 ust. 2 i 3 RODO przewiduje możliwość wyznaczenia inspektora dla grupy przedsiębiorstw oraz organów lub podmiotów publicznych. *Grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej* (art. 37 ust. 2 RODO). Wyznaczony inspektor będzie musiał wykonywać swoje zadania we wszystkich tych jednostkach.

Pojęcie łatwości kontaktu odnosi się do zadań inspektora związanych z komunikacją z osobami, których dane dotyczą i obowiązkami punktu kontaktowego dla organu nadzorczego, jak również funkcjonowaniem wewnątrz podmiotu. Do zadań inspektora należy informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO.

W celu zapewnienia możliwości łatwego kontaktu z inspektorem istnieje konieczność udostępnienia jego danych kontaktowych zgodnie z wymogami RODO. Inspektor powinien mieć możliwość sprawnego komunikowania się z osobami, których dane dotyczą i współpracy z organem nadzorczym. Komunikacja musi odbywać się w języku lub językach używanych przez organy nadzorcze i danych osoby, których dane dotyczą. *Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych* (art. 37 ust. 3 RODO).

Wyznaczenie jednego inspektora będzie tylko możliwe w przypadkach, gdy inspektor będzie w stanie wypełniać prawidłowo wszystkie swoje obowiązki.

Zgodnie z art. 36a ust. 6 u.o.d.o. istnieje możliwość powołania zastępców ABI. *Administrator danych może powołać zastępców administratora bezpieczeństwa informacji, którzy spełniają warunki określone w art. 36a ust. 5 u.o.d.o.* (art. 36a ust. 6 u.o.d.o.). Brak regulacji w tym zakresie w RODO ale nie ma przeszkód aby zgodnie z RODO powołać zastępców inspektora.

3. Kwalifikacje zawodowe do pełnienia funkcji inspektora.

Postanowienia art. 37 ust. 5 RODO wskazują następujące kwalifikacje zawodowe do pełnienia funkcji inspektora (w szczególności):

- posiadanie wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych;
- umiejętność wypełnienia zadań, o których mowa w art. 39 RODO.

Przepis RODO wymagają dodatkowo posiadanie umiejętności w zakresie wykonywania zadań inspektora. Brak natomiast wymogów dotyczących niekaralności oraz zdolności do czynności prawnych i korzystania z praw publicznych.

Zgodnie z motywem 97 preambuły RODO, *Niezbędny 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. Tacy inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny.* Wymagany poziom wiedzy fachowej nie jest nigdzie jednoznacznie określony.

Musi być współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w ramach jednostki.

Artykuł 37 ust. 5 RODO nie wskazuje konkretnych kwalifikacji zawodowych, jakie należy brać pod uwagę wyznaczając inspektora. Inspektor powinien posiadać odpowiednią wiedzę z zakresu krajowych i europejskich przepisów o ochronie danych osobowych i praktyk, w szczególności RODO. Postanowienia art. 37 ust. 5 RODO: *Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39.* Zalecana jest wiedza fachowa i sektorowa dotycząca administratora. Inspektor powinien również posiadać odpowiednią wiedzę na temat procesów przetwarzania danych, systemów informatycznych oraz zabezpieczeń stosowanych u administratora i jego potrzeb w zakresie ochrony danych.

W przypadku organów i podmiotów publicznych inspektor powinien posiadać wiedzę w zakresie procedur administracyjnych i funkcjonowania jednostki. Możliwość wykonywania zadań ciążących na inspektorze powinna być interpretowana zarówno przez pryzmat cech i kwalifikacji inspektora, jak również jego pozycji w strukturach podmiotu. Do cech osobowych zaliczyć można rzetelne podejście i wysoki poziom etyki zawodowej.

Priorytetem inspektora powinno być zapewnienie przestrzegania RODO. Wytworzenie polityki ochrony danych osobowych w organizacji zależy w dużej mierze od działalności inspektora, do jego obowiązków należeć będzie również wsparcie w implementacji RODO, w tym zasad przetwarzania danych osobowych, praw osób, których dane dotyczą, ochrony danych w fazie projektowania oraz domyślnej ochrony danych, rejestru czynności przetwarzania, wymogów bezpieczeństwa przetwarzania i zgłoszenia naruszeń. Dostępność inspektora (fizycznie w miejscu pracy, telefonicznie czy przy wykorzystaniu innych bezpiecznych środków komunikacji) jest kluczowa dla zapewnienia kontaktu z inspektorem.

Przepis art. 37 ust. 6 RODO reguluje sposób zatrudnienia inspektora:

- umowa o pracę;
- umowa o świadczenie usług.

W przypadku funkcji inspektora pełnionej na podstawie umowy o świadczenie usług zawartej z osobą fizyczną lub innym podmiotem spoza organizacji administratora/podmiotu przetwarzającego konieczne jest, aby każdy członek podmiotu sprawującego funkcję inspektora spełniał wszystkie istotne wymogi pozwalające mu np. na unikanie konfliktu interesów.

Każda z tych osób powinna być pod ochroną przewidzianą w przepisach RODO aby zapobiec np. nieuzasadnionemu rozwiązaniu umowy o świadczenie usług w zakresie pełnienia funkcji inspektora, ale również aby nie miało miejsca niezgodne z prawem zwolnienie osoby będącej członkiem podmiotu realizującego zadania inspektora. W celu zapewnienia przejrzystości prawnej i dobrej organizacji zalecany jest wyraźny podział zadań w ramach zespołu inspektora oraz wyznaczenie jednej osoby jako wiodącej osoby kontaktowej i osoby odpowiedzialnej za każdego klienta. Wskazane jest określenie tych kwestii w umowie o świadczenie usług.

Przepis art. 37 ust. 7 RODO przewiduje obowiązek zapewnienia, aby osoby, których dane dotyczą (zarówno wewnątrz jak i spoza organizacji) oraz organy nadzorcze mogły mieć łatwy, bezpośredni i poufny kontakt z inspektorem, bez konieczności kontaktowania się z innymi jednostkami podmiotu. Dane kontaktowe inspektora powinny zawierać dane umożliwiające osobom, których dane dotyczą, i organom nadzorczym nawiązanie kontaktu w łatwy sposób (adres korespondencyjny, telefon kontaktowy, dedykowany adres email). Powinny również zostać udostępnione inne środki komunikacji dla ogółu społeczeństwa, np. dedykowania infolinia, formularz kontaktowy z inspektorem na stronie internetowej organizacji. Przepis artykułu 37 ust. 7 RODO nie wymaga publikowania imienia i nazwiska inspektora. Informacja taka powinna zostać wskazana w ramach dobrej praktyki. Decyzja w tym zakresie zależy od administratora i inspektora.

4. Dobre praktyki i obowiązki kadry zarządzającej w związku ze współpracą z inspektorem ochrony danych osobowych

W ramach dobrej praktyki GR zaleca poinformowanie organu nadzorczego i pracowników organizacji o imieniu, nazwisku i danych kontaktowych inspektora. Dane te mogą zostać udostępnione wewnętrznie np. poprzez intranet, w wewnętrznej książce telefonicznej albo w ramach rozpisanej struktury organizacyjnej. Wyznaczony inspektor będzie punktem kontaktowym dla osób, których dane są przetwarzane. W sprawach wymienionych w art. 15-18 RODO, w szczególności w realizacji praw: dostępu do informacji na temat przetwarzania danych, sprostowania danych, usunięcia danych (prawo do bycia zapomnianym) oraz ograniczenia przetwarzania danych.

Zgodnie z art. 38 ust. 1 RODO istnieje obowiązek właściwego i niezwłocznego włączania inspektora we wszystkie sprawy dotyczące ochrony danych osobowych. Inspektor powinien być zaangażowany na wczesnym etapie we wszystkie kwestie związane z przetwarzaniem danych osobowych. Przy ocenie skutków dla ochrony danych RODO wskazuje na zaangażowanie inspektora i stanowi, że administrator powinien konsultować się z inspektorem przy okazji dokonywania takiej oceny. Angażowanie inspektora powinno być standardową procedurą w organizacji. Inspektor powinien być postrzegany jako partner w dyskusji i włączany w prace grup roboczych poświęconych procesom związanym z przetwarzaniem danych osobowych w ramach organizacji.

W związku z tym organizacja powinna zapewnić między innymi:

- udział inspektora w spotkaniach przedstawicieli wyższego i średniego szczebla organizacji;

- uczestnictwo inspektora przy podejmowaniu decyzji dotyczących przetwarzania danych osobowych (informacje powinny zostać udostępnione inspektorowi wcześniej, umożliwiając wypracowanie stanowiska);

- stanowisko inspektora powinno być uwzględnianie w procesie decyzyjnym. GR zaleca, w ramach dobrych praktyk, dokumentowanie przypadków i powodów postępowania niezgodnego z zaleceniem inspektora;

- w przypadku stwierdzenia naruszenia albo innego zdarzenia związanego z danymi osobowymi należy natychmiast skonsultować się z inspektorem.

W określonych przypadkach administrator lub podmiot przetwarzający powinni stworzyć wytyczne ochrony danych osobowych, które wskazywały przypadki wymagające konsultacji z inspektorem.

Zgodnie z art. 38 ust. 2 RODO powinno być zapewnione wsparcie inspektora w wykonywaniu przez niego zadań, poprzez zapewnienie:

- zasobów niezbędnych do wykonywania zadań (m.in. odpowiednie wsparcie finansowe, infrastrukturalne);

- dostępu do danych osobowych i operacji przetwarzania (m.in. umożliwienie dostępu do innych działów organizacji, np. HR, działu prawnego, IT, ochrony, celem stworzenia przepływu informacji między tymi jednostkami a inspektorem);

- zasobów niezbędnych do utrzymania jego fachowej wiedzy (m.in. szkolenia, warsztaty, udział w konferencjach poświęconych ochronie danych osobowych).

5. Obowiązki inspektora ochrony danych.

Przepis art. 38 ust. 3 zd. 3 RODO przewiduje podległość inspektora pod administratora danych. Administrator oraz podmiot przetwarzający muszą zapewnić, aby inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego (art. 38 ust. 3 RODO). Motyw 97 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."*

W ramach wypełniania zadań z art. 39 inspektor nie może otrzymywać instrukcji dotyczących sposobu rozpoznania sprawy, środków jakie mają zostać podjęte czy celu jaki powinien zostać osiągnięty, czy też faktu, czy należy skontaktować się z organem nadzorczym (zgodnie z art. 38 ust. 3 zd. 1 RODO *„Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań"*). Inspektor nie może również zostać zobligowany do przyjęcia określonego stanowiska w sprawie z zakresu prawa ochrony danych, np. określonej wykładni przepisów.

Administrator i podmiot przetwarzający są odpowiedzialni za przestrzeganie przepisów dotyczących ochrony danych i muszą być w stanie wykazać ich przestrzeganie. W sytuacji podjęcia przez administratora lub podmiot przetwarzający decyzji niezgodnej z przepisami RODO i zaleceniami inspektora, inspektor powinien mieć możliwość jasnego przedstawienia swojego stanowiska osobom podejmującym decyzję.

Zgodnie z artykułem 38 ust. 3 zd. 2 RODO stanowi, że inspektor „nie jest odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań." Zapewnienie niezależności inspektora i zapewnienie możliwości wykonywania zadań w niezależny i odpowiednio chroniony sposób.

Kary w świetle RODO są niedozwolone tylko w przypadkach, gdy są nałożone w związku z wypełnianiem przez inspektora swoich zadań. Kary mogą przybrać szereg form i mogą być bezpośrednie albo pośrednie. Mogą polegać na braku albo opóźnieniu awansu, utrudnieniu rozwoju zawodowego, ograniczeniu dostępu do korzyści oferowanych pozostałym pracownikom. Nieistotny jest przy tym fakt nałożenia kary, gdyż sama możliwość jej wykonania i obawa z tym związana może być wystarczająca do utrudnienia inspektorowi wykonywania zadań. Zgodnie z przepisami karnymi i prawa pracy, jak w przypadku każdego innego pracownika, inspektor może zostać odwołany w uzasadnionych sytuacjach z przyczyn innych niż wykonywanie obowiązków inspektora.

Przepis art. 38 ust. 4 RODO przewiduje możliwość kontaktowania się osób, których dane dotyczą z inspektorem. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia (art. 38 ust. 4 RODO).

Przepis art. 38 ust. 5 RODO zobowiązuje inspektora do zachowania tajemnicy i poufności w zakresie wykonywanych przez niego zadań - zgodnie z prawem Unii lub prawem państwa członkowskiego.

Przepis art. 38 ust. 6 RODO przewiduje możliwość wykonywania przez inspektora innych zadań i obowiązków. Konieczne jest jednak zapewnienie aby takie zadania i obowiązki nie powodowały konfliktu interesów. Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny. Inspektor nie może zajmować w organizacji stanowiska powodującego alokację zasobów przeznaczonych na przetwarzanie danych. Zależnie od rodzaju działalności, rozmiaru i struktury organizacji, dobrą praktyką dla administratorów i podmiotów przetwarzających powinno być:

- zidentyfikowanie stanowisk niekompatybilnych z funkcją inspektora;

- opracowanie wewnętrznej polityki zapobiegającej łączeniu stanowisk będących w konflikcie interesów;

- z zasady można uznać, że konflikt interesów mogą powodować stanowiska kierownicze np. dyrektor generalny, dyrektor ds. operacyjnych, dyrektor ds. marketingu, dyrektor HR, dyrektor IT, ale również niższe stanowiska, jeśli biorą udział w określaniu celów i sposobów przetwarzania danych;

- stwierdzenie, że nie ma konfliktu interesów w funkcjonowaniu obecnego inspektora w celu zwiększenia świadomości na temat tego wymogu;

- wprowadzenie odpowiednich zabezpieczeń do wewnętrznych zasad organizacji w celu zapewnienia, aby ogłoszenia o rekrutacji na stanowisko inspektora było jasne, precyzyjne i niwelowały ryzyko powstania konfliktu interesów.

Postanowienia art. 39 ust. 1 RODO określają zadania inspektora ochrony danych. Przepis art. 39 RODO nie określa precyzyjnie trybu realizacji tych zadań. Pomocne są więc wytyczne Grupy Roboczej. Doprecyzowanie realizacji zadań powinno się znaleźć w odpowiednich kodeksach postępowania zatwierdzonych na podstawie art. 40 ust. 5 lub 9 RODO.

Przepis art. 39 ust. 1 lit. a) RODO nakazuje informowanie osób, które przetwarzają dane osobowe, o obowiązkach spoczywających na nich na podstawie RODO oraz postanowień innych przepisów o ochronie danych osobowych UE lub państwa członkowskiego i doradzanie w tym zakresie. Przepis RODO wprowadzają dodatkowy obowiązek w postaci doradzania w sprawach ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty. RODO, odmiennie niż u.o.d.o. nie określa trybu i sposobu wykonywania tego zadania. Istnieje możliwość określenia tych kwestii w kodeksach postępowania.

Motyw 97 RODO doprecyzowuje, iż *„w monitorowaniu wewnętrznego przestrzegania niniejszego rozporządzenia administrator lub podmiot przetwarzający powinni być wspomagani przez osobę dysponującą wiedzą fachową na temat prawa i praktyk w dziedzinie ochrony danych."* Powinny być prowadzone działania podnoszące poziom świadomości, w tym szkolenia pracowników dopuszczonych do przetwarzania danych oraz przeprowadzanie

audytów dotyczących ochrony danych osobowych. W ramach monitorowania inspektorzy mogą między innymi:

- zbierać informacje w celu identyfikacji procesów przetwarzania;

- analizować i sprawdzać zgodność tego przetwarzania;

- informować, doradzać i rekomendować określone działania administratorowi.

Monitorowanie nie oznacza odpowiedzialności inspektora w przypadkach naruszenia RODO (administrator, a nie inspektor *„wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać"* art. 24 ust. 1 RODO).

Przepis art. 39 ust. 1 lit. c) RODO przewiduje obowiązek inspektora udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO. GR zaleca administratorowi konsultowanie z inspektorem m.in. następujących kwestii:

- czy należy przeprowadzić ocenę skutków dla ochrony danych;

- metodologii przeprowadzenia oceny skutków dla ochrony danych;

- czy należy przeprowadzić wewnętrzną ocenę czy też zlecić ją podmiotowi zewnętrznemu;

- zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą;

- prawidłowości przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie czy też nie oraz jakie zabezpieczenia należy zastosować).

W przypadku, gdy administrator nie zgadza się z zaleceniami inspektora, dokumentacja oceny skutków dla ochrony danych powinna zawierać pisemne uzasadnienie nieuwzględnienia tych zaleceń. GR rekomenduje aby administrator jasno, np. w umowie z inspektorem, ale również w informacjach przekazywanych pracownikom, kierownikom i innym, wskazał zakres obowiązków inspektora w danej organizacji, w szczególności w kontekście przeprowadzania oceny skutków dla ochrony danych.

Zgodnie z artykułem 35 ust. 1 RODO do obowiązków administratora, a nie inspektora, należy przeprowadzanie
w określonych przypadkach oceny skutków dla ochrony danych. Inspektor może jednak odgrywać istotną rolę i wspierać administratora przy przeprowadzaniu takiej oceny. Zgodnie z zasadą ochrony danych w fazie projektowania, art. 35 ust. 2 RODO nakłada na administratora obowiązek konsultowania się z inspektorem przy dokonywaniu oceny skutków dla ochrony danych.

Przepis art. 39 ust. 1 lit. c) RODO reguluje obowiązek udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania. Konieczne jest ustalenie przez inspektora priorytetów w swojej pracy i koncentrowania się na aspektach pociągających za sobą większe ryzyko. Pragmatyczne podejście powinno ułatwić inspektorowi doradzenie administratorowi, jaką metodologię należy zastosować przy przeprowadzeniu oceny skutków dla ochrony danych, które obszary powinny zostać poddane wewnętrznemu albo zewnętrznemu audytowi, jakie szkolenia wewnętrzne przeprowadzić dla pracowników lub kierowników odpowiedzialnych za przetwarzanie danych i na które operacje przetwarzania u przeznaczyć więcej czasu i zasobów.

Konieczne jest stosowania się inspektora do przyjętych przez administratora lub podmiot przetwarzający zasad związanych z analizą ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze naruszenia (art. 32 RODO).

Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania (art. 39 ust. 2 RODO). Inspektor w praktyce będzie musiał sam określić takie zasady, opierając się na dostępnych normach lub kodeksach postępowania (art. 40 RODO).

W RODO przewidziany jest obowiązek prowadzenia przez administratora danych oraz podmiot przetwarzający rejestrów czynności przetwarzania danych, który jest zbliżony pod względem zakresu do rejestru zbiorów prowadzonego przez ABI.

Zgodnie z artykułem 30 ust. 1 i 2 RODO do administratora albo podmiotu przetwarzającego należy obowiązek prowadzenia rejestru „czynności przetwarzania danych osobowych, za które odpowiadają" albo „wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora". Zgodnie z art. 38 ust. 6 RODO zadania te można powierzyć inspektorowi.

W praktyce często to inspektor tworzy i prowadzi powyższe rejestry w oparciu o dane otrzymane od pozostałych komórek organizacji. Taka procedura została ustalona na mocy wielu obowiązujących przepisów państw członkowskich i przepisów o ochronie danych osobowych mających zastosowanie do instytucji i organów UE.

Artykuł 39 ust. 1 RODO określa minimalną listę zakresu obowiązków inspektora aby inspektor prowadził, w imieniu administratora, rejestr czynności przetwarzania danych. Rejestr ten powinien być uznany za jeden ze sposobów monitorowania przestrzegania RODO, informowania administratora lub podmiotu przetwarzającego i doradzania im. Rejestr prowadzony zgodnie z art. 30 RODO powinien umożliwić administratorowi i organowi nadzorczemu (na wniosek) kontrolę wszystkich procesów przetwarzania danych w danej organizacji. Stanowi warunek zapewnienia zgodności i jest przydatnym narzędziem przy rozliczalności.

Przepis art. 39 ust. 1 lit d) RODO przewiduje współpracę z organem nadzorczym. Przepis art. 39 ust. 1 lit. e) RODO przewiduje obowiązek pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

6. Podsumowanie

Dostosowanie się organizacji do ww. unijnych przepisów w zakresie ochrony danych osobowych będzie zależało m.in. przede wszystkim od rodzaju prowadzonej działalności, a także od rodzaju, zakresu i celu, dla jakiego przetwarza konkretny podmiot dane osobowe. Powinna być przeprowadzona analiza czy w danym podmiocie powinien być powołany inspektor ochrony danych, który zajmie się opisanymi zagadnieniami. Mamy nadzieję, że powyższe opracowanie odpowiada na pytania dotyczące obowiązków powołania i roli ww. inspektorów.

W razie dalszych wątpliwości zapraszamy do kontaktu z kancelarią.

Wykorzystane w opracowaniu akty prawne i opracowania:

- Rozporządzenie 2016/679 z 27 kwietnia 2016 r. Parlamentu Europejskiego i Rady UE 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. L Nr 199 z 4 maja 2016 r. s. 1-88) („RODO")

- Wytyczne Grupy Art. 29 dotyczące inspektorów ochrony danych, http://www.giodo.gov.pl/pl/259/9718

- M. Byczkowski, Przygotowanie ABI do nowej funkcji inspektora ochrony danych, Informacja w administracji publicznej 2017, nr 1, s. 24-32.

ISBN 978-83-63582-04-3

9 788363 582043

Związek Przedsiębiorców i Pracodawców :: www.zpp.net.pl

Dworzyński Rogalski Kancelaria Radców Prawnych :: www.dworzynskirogalski.pl

ISBN 978-83-63582-04-3