

Rozdział 2

Wyznaczanie inspektora ochrony danych

Art. 8. [Inspektor ochrony danych]

Administrator i podmiot przetwarzający są obowiązani do wyznaczenia inspektora ochrony danych, zwanego dalej „inspektorem”, w przypadkach i na zasadach określonych w art. 37 rozporządzenia 2016/679.

Art. 9. [Organy i podmioty zobowiązane do wyznaczenia inspektora]

Przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora, o których mowa w art. 37 ust. 1 lit. a rozporządzenia 2016/679, rozumie się:

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

Art. 10. [Zawiadomienie o wyznaczeniu inspektora]

1. Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o jego wyznaczeniu w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora.

2. Zawiadomienie może zostać dokonane przez pełnomocnika podmiotu, o którym mowa w ust. 1. Do zawiadomienia dołącza się pełnomocnictwo udzielone w formie elektronicznej.

3. W zawiadomieniu oprócz danych, o których mowa w ust. 1, wskazuje się:

- 1) imię i nazwisko oraz adres zamieszkania, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna;
- 2) firmę przedsiębiorcy oraz adres miejsca prowadzenia działalności gospodarczej, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna prowadząca działalność gospodarczą;

3) pełną nazwę oraz adres siedziby, w przypadku gdy administratorem lub podmiotem przetwarzającym jest podmiot inny niż wskazany w pkt 1 i 2;

4) numer identyfikacyjny REGON, jeżeli został nadany administratorowi lub podmiotowi przetwarzającemu.

4. Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o każdej zmianie danych, o których mowa w ust. 1 i 3, oraz o odwołaniu inspektora, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania.

5. W przypadku wyznaczenia jednego inspektora przez organy lub podmioty publiczne albo przez grupę przedsiębiorców, każdy z tych podmiotów dokonuje zawiadomienia, o którym mowa w ust. 1 i 4.

6. Zawiadomienia, o których mowa w ust. 1 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

Art. 11. [Udostępnienie danych inspektora]

Podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa w art. 10 ust. 1, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.

Treść uzasadnienia rządowego dotycząca rozdziału 2 ustawy

Rozdział 2. Wyznaczanie inspektora ochrony danych

W rozdziale 2 projektowanej ustawy uregulowano tryb notyfikacji inspektorów ochrony danych osobowych, zwanych dalej „inspektorami”, oraz podmioty obowiązane w polskim porządku prawnym do wyznaczenia inspektora ochrony danych osobowych.

Rozporządzenie reguluje kwestię inspektorów w przepisach art. 37–39. Przypadki obowiązkowego wyznaczenia inspektorów określa art. 37 Rozporządzenia. Zgodnie z tym przepisem administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze, gdy:

- a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
- b) 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
- c) 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.

W innych niż ww. przypadkach wyznaczenie inspektora jest dobrowolne. Projektodawca nie zdecydował się rozszerzyć przedmiotowo sytuacji obligatoryjnego wyznaczania inspektora, traktując katalog wymieniony w art. 37 ust. 1 Rozporządzenia jako zapewniający dostateczną ochronę podmiotów danych, a jednocześnie uwzględniający także koszty powołania inspektora.

Rozporządzenie nie definiuje terminu „organu lub podmiotu publicznego”. Grupa Robocza art. 29, jako unijne forum współpracy organów ochrony danych osobowych państw członkowskich UE, wskazała w swoich wytycznych, dotyczących inspektorów ochrony danych (WP243), że: „takie pojęcie powinno zostać określone na poziomie przepisów krajowych. Do podmiotów takich najczęściej zalicza się organy władzy krajowej, organy regionalne i lokalne, ale również – na mocy właściwego prawa krajowego – szereg innych podmiotów prawa publicznego”. Uwzględniając powyższe oraz treść Rozporządzenia, wskazującego na obowiązek wyznaczenia inspektorów, ciążący na „organach lub podmiotach publicznych”, projektodawca zdecydował się wprowadzić do projektu szerokie rozumienie takich podmiotów publicznych. Przepisy projektu w celu zapewnienia stosowania art. 37 ust. 1 lit. a Rozporządzenia precyzują, iż organami i podmiotami publicznymi obowiązany do wyznaczenia inspektora są organy publiczne i podmioty publiczne wskazane w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, a także instytuty badawcze oraz Narodowy Bank Polski.

Kwalifikacje, jakie powinien posiadać inspektor, określono bezpośrednio w Rozporządzeniu. Z jego przepisów wynika, iż inspektor powinien dysponować wiedzą fachową na temat prawa oraz odbyć praktyki w dziedzinie ochrony danych, a także posiadać umiejętność wypełniania zadań, o których mowa w art. 39 Rozporządzenia. Projektodawca nie zdecydował się na dookreślenie kwalifikacji, jakie powinien spełniać inspektor, wychodząc z założenia, że każda próba doprecyzowania tych przesłanek – np. w zakresie długości praktyk – mogłaby narazić go na zarzut nakładania ograniczeń, niewystępujących w innych państwach członkowskich UE, a tym samym barierę w swobodzie świadczenia usług. Co do umiejętności wypełniania zadań, to należy podkreślić, iż odpowiedzialność za wybór inspektora, a tym samym za umiejętność wykonywania zadań, ponosi administrator. To w jego interesie leży taki wybór inspektora, który da mu rękojmię umiejętnego wykonywania przez niego zadań. Grupa Robocza art. 29 wskazała w swoich wytycznych nr WP 243, dotyczących inspektorów ochrony danych, że wymagany rozporządzeniem 2016/679 „poziom wiedzy fachowej nie jest nigdzie jednoznacznie określony, ale musi być współmierny do charakteru, skomplikowania i ilości danych, przetwarzanych w ramach jednostki. Dla przykładu, w przypadku wyjątkowo skomplikowanych procesów przetwarzania danych osobowych lub w przypadku przetwarzania dużej ilości danych szczególnych kategorii, inspektor może potrzebować wyższego poziomu wiedzy i wsparcia. Ponadto inaczej sytuacja przedstawiać się będzie w przypadku podmiotów regularnie przekazujących dane do państw trzecich niż w przypadku, gdy przekazywanie takie ma charakter okazjonalny. W związku z tym wybór inspektora powinien być dokonany z zachowaniem należytej staranności i brać pod uwagę charakter przetwarzania danych w ramach podmiotu”. Z kolei, wypowiadając się w przedmiocie kryterium kwalifikacji zawodowych, Grupa wskazała, że: „istotne

jest, by inspektor posiadał odpowiednią wiedzę z zakresu krajowych i europejskich przepisów o ochronie danych osobowych i praktyk, jak również dogłębną znajomość rozporządzenia. Propagowanie odpowiednich i regularnych szkoleń dla inspektorów przez organy nadzorcze również może być przydatne. Przydatna jest również wiedza na temat danego sektora i podmiotu administratora. Inspektor powinien również posiadać odpowiednią wiedzę na temat operacji przetwarzania danych, systemów informatycznych oraz zabezpieczeń stosowanych u administratora i jego potrzeb w zakresie ochrony danych. W przypadku organów i podmiotów publicznych Inspektor powinien również posiadać wiedzę w zakresie procedur administracyjnych i funkcjonowania jednostki”. Powyższe stanowiska wskazują więc skuteczny kierunek wykładni przepisów Rozporządzenia i są praktycznym drogowskazem dla inspektorów (dzisiejszych Administratorów Bezpieczeństwa Informacji, zwanych dalej „ABI”). Jednocześnie należy wskazać, że w dzisiejszym porządku prawnym ustawodawca także nie wypowiada się w przedmiocie kwalifikacji zawodowych koniecznych do pełnienia funkcji ABI. Przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych wskazują bowiem, że funkcję taką może pełnić osoba, posiadająca odpowiednią wiedzę w zakresie ochrony danych osobowych. Weryfikację takiego kryterium podejmuje więc w każdym przypadku przedsiębiorca zatrudniający ABI oraz Generalny Inspektor Ochrony Danych Osobowych na etapie przeprowadzanych postępowań kontrolnych.

Co ważne, projekt Rozporządzenia przewiduje, że inspektor może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług. W tym miejscu należy zwrócić także uwagę, iż art. 37 Rozporządzenia nie przyznaje państwowym członkowskim kompetencji do określenia, w ilu maksymalnie podmiotach dana osoba może pełnić funkcję inspektora.

Projektodawca nie zdecydował się przewidzieć w projektowanych przepisach instytucji zastępcy inspektora ochrony danych oraz możliwości powołania kilku inspektorów w jednym podmiocie. W opinii projektodawcy byłoby to niezgodne z Rozporządzeniem. Zgodnie z art. 37 oraz motywem 97 Rozporządzenia administrator i podmiot przetwarzający wyznaczają inspektora, mowa jest o inspektorze w liczbie pojedynczej. Co więcej ustawodawca unijny przewidział możliwość wyznaczenia jednego inspektora dla kilku podmiotów, nie przewidział natomiast możliwości wyznaczenia kilku inspektorów czy też zastępcy inspektora w jednym podmiocie. Ponadto warto zauważyć, że inspektorem może zostać osoba, która posiada odpowiednie kwalifikacje zawodowe oraz wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych, ponadto inspektor ma obowiązek m.in. współpracować z organem nadzorczym oraz pełnić funkcję punktu kontaktowego. Natomiast wyznaczenie zastępców wiąże się z prawem do delegowania uprawnień i obowiązków także w sytuacji, gdy w danym podmiocie jest obecny inspektor. Na taką osobę mogłyby zostać przekazane niektóre zadania czy też uprawnienia przysługujące inspektorowi. W opinii projektodawcy, w przypadku gdy administrator albo podmiot przetwarzający powźmie wiadomość o długiej nieobecności inspektora ochrony danych osobowych, powinien on wyznaczyć nową osobę do pełnienia tej funkcji, o czym powinien niezwłocznie zawiadomić Prezesa Urzędu. W przypadku krótszej, okresowej nieobecności administrator bądź podmiot przetwarzający powinien upoważnić innego pracownika do podejmowania działań inspektora.