„Mistrz IODa" poszukiwany, czyli co trzeba wiedzieć zatrudniając na stanowisko Inspektora Ochrony Danych

Yoda – filmowy mistrz zakonu Jedi - to symbol doświadczenia i mądrości. Stając przed zadaniem zatrudnienia w firmie Inspektora Ochrony Danych powinniśmy wybrać kandydata, który również wykaże się dogłębną (i potwierdzoną!) wiedzą na temat prawnych aspektów ochrony danych oraz praktyką w tej dziedzinie. Słowem: swoistego mistrza lodę, czy raczej – IODę.

Obowiązek powołania Inspektora Ochrony Danych (IOD) wynika z unijnego rozporządzenia ogólnego o ochronie danych (skrótowo nazywanego RODO lub – z języka angielskiego – GDPR). Rozporządzenie to zostało przyjęte 27 kwietnia 2016 roku, natomiast 25 maja br. zakończy się dwuletni okres przejściowy, co oznacza, że nowe przepisy będą już w pełni stosowane na obszarze wszystkich państw członkowskich Unii Europejskiej.

Najogólniej rzecz biorąc, RODO zmienia podejście podmiotów do gromadzenia i przechowywania danych, pracowników kontrahentów, klientów, pacjentów itd. Jego celem jest zagwarantowanie ochrony podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych oraz wprowadzenie zasad, które ujednolicą ich przetwarzanie w UE.

Czy Twoja firma ma obowiązek powołać Inspektora Danych Osobowych?

W „przedrodowskim" porządku prawnym administrator danych (podmiot decydujący o celach i sposobach przetwarzania danych) samodzielnie decydował o tym, czy powołać Administratora Bezpieczeństwa Informacji (zapewniającego przestrzeganie przepisów o ochronie danych w organizacji i prowadzącego rejestr zbiorów danych), czy też nie. Jeśli firma wcześniej zdecydowała się powołać ABI, wówczas – zgodnie z art. 144 projektu nowej Ustawy o ochronie danych osobowych (UODO) – automatycznie stanie się on IOD z dniem 25 maja br. Będzie pełnił tę funkcję do 1 września br., jeżeli do tego dnia administrator zawiadomi organ nadzorczy o powołaniu na to stanowisko innej osoby, lub dalej po tej dacie, jeśli administrator potwierdzi, że „dawny" ABI ma w dalszym ciągu wykonywać obowiązki Inspektora.

Przepisy RODO mogą jednakże nakładać obowiązek powołania IOD na podmioty, które do tej pory nie posiadały ABI. Reguluje to art. 37 RODO, zgodnie z treścią którego obowiązek powołania IOD ciąży na

podmiotach lub organach publicznych, przetwarzających dane, jak też gdy „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". W art. 37 RODO opisano też trzecią sytuację, gdy powołanie IOD jest obowiązkowe. Mianowicie w sytuacji, gdy „główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych albo danych osobowych dotyczących wyroków skazujących i naruszeń prawa".

Można przyjąć, że w większości przypadków powołanie IOD przez firmy będzie wynikać z drugiego z opisanych powyżej przypadków, tj. gdy przetwarzanie danych odbywa się na dużą skalę i w sposób nierozerwalny łączy się z głównym profilem działalności podmiotu. Stąd też Inspektor znajdzie się zarówno w firmie produkcyjnej, która przetwarza dane klientów i kooperantów, jak i np. w szpitalu administrującym danymi swoich pacjentów. Wielkość firmy nie będzie mieć tu znaczenia, bo IOD może być obowiązana powołać zarówno organizacja duża, zatrudniająca setki pracowników, ale też np. kilkuosobowa agencja reklamowa. Przy czym ocenie indywidualnej podlegać będzie każdorazowo, czy przetwarzanie przez firmę danych spełnia przesłankę skali i ścisłego związku z prowadzoną działalnością.

Niespełnienie lub naruszenie regulacji RODO, a takim będzie brak powołania IOD mimo, iż firma kwalifikuje się do spełnienia tego obowiązku, oznacza ryzyko kar finansowych w wysokości do 2% rocznego obrotu przedsiębiorstwa (lub do 10 mln euro), nie mówiąc już o utracie reputacji oraz potencjalnych korzyści ze względu na zerwane kontakty biznesowe. Obowiązkiem firm, w których powołano IOD, będzie publikacja danych osoby pełniącej tę funkcję oraz poinformowanie o tym organu nadzorczego. Z drugiej strony warto powołać w swojej firmie IOD nawet w sytuacji, gdy obowiązek ten jej nie dotyczy. Posłuży to budowie wizerunku rzetelnego i odpowiedzialnego podmiotu, który kompleksowo podchodzi do zasad ochrony danych, w zakresie większym, niż nakazuje mu unijne rozporządzenie.

Obowiązki IOD

Katalog obowiązków Inspektora Ochrony Danych zawarty jest w art. 39 RODO. Rola IOD będzie znacząco istotniejsza, aniżeli ma to miejsce w przypadku obecnych ABI. W procesie administrowania danymi Inspektor będzie mieć kluczowe znaczenie. IOD monitorować będzie, czy administrator danych lub podmiot administrujący danymi znają przepisy RODO i ich przestrzegają. Do jego zadań należeć będzie też informowanie o wszystkich obowiązkach w zakresie ochrony danych, które nakładają na administratora, „procesora" (czyli podmiot, który przetwarza dane na zlecenie administratora) i pracowników zajmujących się przetwarzaniem danych, przepisy unijne i krajowe. Inspektor Ochrony Danych będzie także punktem

kontaktowym, zarówno dla organu nadzorczego, jak i dla wszystkich osób, których dane są przetwarzane przez dany podmiot. Innymi słowy, jeśli ktoś będzie chciał np. zmodyfikować swoje dane, wówczas powinien zwrócić się w tej sprawie do IOD.

Wartą podkreślenia cechą IOD jest jego usytuowanie w strukturze organizacyjnej podmiotu, który go powoła – powinien podlegać najwyższemu kierownictwu, a inne obowiązki, nie mogą kolidować z funkcją Inspektora Ochrony Danych, jak też ograniczać niezależności i dostępności IOD. Oznacza to, że np. członek zarządu na stanowisko IOD powołany być nie może. Inspektorem Ochrony Danych może być zarówno pracownik administratora, jak i „procesora", ale możliwe będzie też outsourcowanie tej funkcji wyspecjalizowanym firmom zewnętrznym. Co więcej, grupa firm będzie mogła powierzyć funkcję IOD tej samej osobie, o ile będzie zagwarantowany swobodny dostęp i kontakt z Inspektorem.

Jakie kompetencje powinien mieć IOD?

Kompetentny „Mistrz IOD-a" powinien przede wszystkim wykazywać się dogłębną wiedzą w zakresie przepisów RODO/GDPR oraz innych krajowych i europejskich regulacji dotyczących ochrony danych. Stąd też niezbędna jest gruntowna znajomość polskich ustaw o ochronie danych, zarówno jeszcze obowiązującej (z 1997 roku), jak też nowej, której proces legislacyjny właśnie trwa.

Atutem kandydata na IOD będzie bez wątpienia doświadczenie zawodowe w sferze ochrony danych, bo oznacza ono, że osoba taka poznała tę sferę także od praktycznej strony – nie tylko zna przepisy, ale potrafi je zastosować w praktyce. W przypadku IOD mniejsze znaczenie od umiejętności i doświadczenia ma wyższe wykształcenie kandydata, chociaż bez wątpienia również będzie to wartość dodana, podobnie zresztą jak udokumentowana znajomość międzynarodowych norm dotyczących bezpieczeństwa informacji, takich jak ISO 27001.

Fachową wiedzę przyszłego IOD w zakresie przepisów RODO i umiejętności ich stosowania może potwierdzać fakt uczestnictwa w szkoleniach z tego zakresu oraz uzyskanie certyfikatu wystawionego przez niezależną jednostkę certyfikacyjną. Dokument taki potwierdza, że osoba ubiegająca się o stanowisko IOD posiada niezbędną wiedzę w tym zakresie, co udowodniła zdając egzamin specjalistyczny.

Piotr UBYCH,

Menedżer ds. Usług Ochrony Danych

Grupa DEKRA w Polsce