Monitorowanie przestrzegania RODO to obowiązek inspektora ochrony danych

- jak go realizować

experto24.pl

Spis treści

Czym są polityki ochrony danych 2
Co należy uregulować w polityce ochrony danych 3
Inspektor ochrony danych musi być niezależny 3
Inspektor ochrony danych musi szkolić pracowników 4
Pamiętaj o podziale obowiązków 4
Czy można prowadzić dotychczasowe sprawdzenia 5
Monitorowanie przestrzegania RODO w praktyce 5

Monitorowanie przestrzegania przepisów ogólnego rozporządzenia o ochronie danych (RODO), przepisów krajowych i polityk obowiązujących u administratora (ADO) to jedno z kluczowych zadań, jakie musi wykonywać inspektor ochrony danych (IOD) od 25 maja 2018 r. Czym w praktyce jest to monitorowanie i jak ten obowiązek spełniać? Czy można skorzystać z dotychczasowych doświadczeń administratorów bezpieczeństwa informacji (ABI) lub osób pełniących nadzór nad zgodnością przetwarzania danych z przepisami?

Tak, w tym obszarze IOD mogą korzystać ze swoich dotychczasowych doświadczeń (jeżeli pełnili funkcję ABI). Obowiązek zapewnienia zgodności przetwarzanych danych z przepisami prawa nie jest niczym nowym dla ADO, ABI i IOD. Dotychczasowi ABI, dzięki zmianom w ustawie o ochronie danych osobowych po 1 stycznia 2015 r., mają już potrzebne doświadczenie m.in. dzięki wykonywaniu zadań określonych w art. 36a ust. 2 pkt 1 lit. a–c ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (uodo).

Obowiązek monitorowania przestrzegania przepisów oraz polityk ADO spoczywający na IOD został wskazany w art. 39 ust. 1 lit. b. RODO – „monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich 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".

Należy pamiętać, że proces monitorowania, a właściwie raporty sporządzone po przeprowadzonych kontrolach, ma zapewnić administratorowi oraz podmiotowi przetwarzającemu wiedzę na temat ewentualnych niezgodności i ryzyka związanego z przetwarzaniem danych osobowych.

Czym są polityki ochrony danych

Ponieważ RODO nie definiuje wprost tego, czym w praktyce są polityki administratora, należy sięgnąć do art. 24 ust. 1 oraz ust. 2 RODO. Zgodnie z tymi przepisami ADO musi wdrożyć odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych osobowych odbywało się zgodnie z RODO. Następnie ADO ocenia, czy te środki, w odniesieniu do zasady proporcjonalności, wymagają wdrożenia odpowiednich polityk. Zgodnie z motywem 78 RODO polityki mają pomóc ADO wykazać, że przestrzega przepisów rozporządzenia, oraz zapewnić przetwarzanie danych zgodnie z zasadami *privacy by design* i *privacy by default.* Politykami mogą być również wiążące reguły korporacyjne, kodeks branżowy oraz inne regulacje czy też procedury, które obligują ADO do ich stosowania.

Czy w związku z tym ADO może posługiwać się dalej dotychczasową polityką ochrony danych osobowych oraz instrukcją zarządzania systemem informatycznym? Tak, ale pod pewnymi warunkami.

Należy pamiętać, że zgodnie z RODO polityki bezpieczeństwa nie są obowiązkowe. Można znaleźć takie polityki i instrukcje zarządzania systemem informatycznym, które nie odpowiadają wymogom obecnie obowiązujących przepisów, są ubogie, zbyt ogólne, nie zawierają wszystkich elementów. W takiej sytuacji właściwe będzie przygotowanie dokumentu dedykowanego RODO. Jeżeli jednak administrator dysponuje dobrze i rzetelnie przygotowaną dokumentacją, powinien zweryfikować kolejne elementy.

Administrator musi wskazać, że dotychczas stosowana dokumentacja była tworzona zgodnie z art. 36 ust. 2 uodo oraz rozporządzeniem ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Natomiast RODO daje znacznie większą swobodę w kształtowaniu wewnętrznego systemu bezpieczeństwa przez ADO. Dlatego też dokumentacja wytworzona przez ADO przed 25 maja 2018 r. wymaga aktualizacji pod kątem analizy ryzyka naruszenia praw i wolności osób fizycznych, jak również uwzględnienia w niej celu, kontekstu, zakresu i charakteru przetwarzania.

Co należy uregulować w polityce ochrony danych

Polityka ochrony danych zgodna z RODO nie powinna koncentrować się tylko na kwestiach bezpieczeństwa w odniesieniu do naruszenia (mechanizmy zabezpieczeń). Aby była dokumentem kompletnym i spójnym, musi regulować też wiele dodatkowych obszarów związanych z przetwarzaniem danych osobowych. Można tu wskazać zasady:

- doboru i kontroli dostawców ADO,
- związane z informowaniem IOD o wdrażaniu nowych procesów i nowych czynności przetwarzania,
- szkolenia pracowników,
- wykonywania praw osób fizycznych określonych w Rozdziale III RODO,
- usuwania danych i okresy przedawnienia.

Polityka powinna zawierać odwołania do funkcji samego IOD i jego uprawnień (np. wykonywanie obowiązków wynikających z art. 39 RODO). Oczywiście poziom szczegółowości dokumentu i częstotliwości odesłań do innych aktów normatywnych obowiązujących u administratora zależą od specyfiki danego podmiotu.

Inspektor ochrony danych musi być niezależny

Należy przypomnieć, że to na ADO spoczywa obowiązek wdrożenia odpowiednich polityk, zasad i środków bezpieczeństwa. IOD ma natomiast obowiązek monitorować, czy i jak są one w praktyce stosowane u ADO. Dlatego tak ważna i wymagająca podkreślenia jest konieczność zapewnienia IOD niezależności. Ciężko bowiem będzie weryfikować IOD, czy dane są przetwarzane zgodnie z prawem, jeżeli nie będzie mieć stosownego umocowania w wewnętrznych aktach normatywnych ADO, które zapewnią mu możliwość wykonywania kontroli innych jednostek.

Dotyczy to IOD, który jest pracownikiem administratora, oraz IOD zewnętrznego. Aby uniknąć konfliktów wewnątrz jednostek organizacyjnych ADO, należy zdefiniować czynności, jakie IOD może i powinien wykonywać w ramach monitorowania. Grupa Robocza Art. 29 wskazuje np. doradzanie, informowanie, wydawanie rekomendacji administratorowi, ale również zbieranie informacji na temat toczących się procesów, ich analiza i badanie zgodności z wewnętrznymi procedurami oraz z prawem.

Inspektor ochrony danych musi szkolić pracowników

Nie bez znaczenia w pracy IOD są działania związane ze szkoleniem i podnoszeniem świadomości i wiedzy pracowników ADO. Niestety wciąż najsłabszym ogniwem systemu bezpieczeństwa jest człowiek, stąd konieczność, aby IOD miał wiedzę i kontrolę nad szkoleniami pracowników. Bardzo przydatne będą zatem wszelkie inicjatywy IOD organizowane u administratora związane z ochroną danych.

Przykładem mogą być newslettery kierowane do pracowników, dedykowana strona w intranecie czy nawet dni ochrony danych. Tego typu działania, które pozwalają na budowanie świadomości i wiedzy pracowników, to jednocześnie dobra okazja dla IOD, aby podkreślać swoją obecność i rolę w firmie.

Należy zaznaczyć, że wszelkie działania promujące ochronę danych u ADO, budowanie świadomości pracowników powinny odbywać się przy aktywnym współudziale administratora. Pozwoli to umocnić rolę IOD w oczach innych pracowników. Widoczność IOD w organizacji jest niezwykle istotna, ponieważ pracownicy muszą wiedzieć, w jaki sposób łatwo się z nim skontaktować w razie pytań, wątpliwości bądź problemów związanych z przetwarzaniem danych osobowych w codziennej pracy.

Pamiętaj o podziale obowiązków

Jednym z elementów monitorowania jest podział obowiązków. Punkt ten wydaje się oczywisty, niemniej jednak ze względu na jego wagę wymaga podkreślenia. Z prawidłowo zdefiniowanym podziałem obowiązków w firmie ściśle łączą się następujące elementy:

a) prawidłowe przypisanie uprawnień pracowników w systemach,

b) nadawanie upoważnień do przetwarzania danych i możliwości sprawowania efektywnej kontroli w związku z przetwarzaniem danych,

c) lepsza kontrola i zapewnienie bezpieczeństwa przetwarzania danych,

d) przejrzystość w wykazaniu prawidłowego sprawowania funkcji IOD,

e) określenie, kto jest właścicielem danych na poszczególnych etapach procesów,

f) łatwość w uzyskiwaniu przez IOD informacji np. na temat celów i podstaw prawnych przetwarzania danych.

Prawidłowy podział obowiązków u administratora pozwala również wykazać rozliczalność wymaganą art. 5 ust. 2 RODO.

Czy można prowadzić dotychczasowe sprawdzenia

Jak w praktyce należy wykonywać monitorowanie zgodności administratora z ogólnym rozporządzeniem o ochronie danych, przepisami oraz wewnętrznymi politykami? Inspektorzy, którzy pełnili dotychczas funkcję ABI, będą mogli sięgnąć do swoich doświadczeń zdobytych w związku z wykonywaniem sprawdzeń oraz sprawozdań dla administratora danych. Oczywiście RODO nie wskazuje terminów oraz trybu, w jakim monitorowanie ma się odbywać, dlatego też sięgnięcie do dotychczasowych doświadczeń ABI będzie dobrym punktem wyjścia.

Inspektor ochrony danych powinien zatem mieć ustalony plan monitorowania jednostek znajdujących się w strukturze danej organizacji. Oczywiście będą podmioty, które w całości będą podlegały monitorowaniu ze względu na rozbudowane procesy przetwarzania danych, ale można wskazać i takie, w których styczność z danymi dotyczy tylko niektórych obszarów.

Niezależnie od tego, z jakim scenariuszem IOD przyjdzie się zmierzyć, musi uwzględnić zakres, cel, kontekst i rodzaj danych, jakie są w danym procesie przetwarzane. Następnie na podstawie swojej wiedzy zaczerpniętej np. z rejestru czynności przetwarzania IOD powinien określić te obszary w firmie, które wymagają kontroli. Wiedząc, jakie dane są przetwarzane, jakie jest ryzyko związane z wystąpieniem incydentu naruszenia bezpieczeństwa, trzeba ustalić częstotliwość kontroli.

Inspektor ochrony danych powinien przygotować harmonogram przeprowadzania monitorowania u administratora. Ogólne rozporządzenie o ochronie danych nie wymaga uzyskania akceptacji administratora (co mogłoby stanowić podważenie zasady niezależności IOD) opracowanego kalendarza audytów, kontroli, niemniej jednak informację o planowanych działaniach inspektora warto przekazać administratorowi. Na podstawie harmonogramu kontroli oraz procesu przetwarzania danych inspektor ochrony danych powinien określić, co dokładnie będzie chciał zweryfikować w danej jednostce.

Monitorowanie przestrzegania RODO w praktyce

Podczas monitorowania przestrzegania RODO z pewnością należy uwzględnić wszystkie regulacje, jakie w sprawdzanym obszarze regulują zasady przewarzania danych osobowych. Inspektor ochrony danych musi ocenić, czy regulaminy, procedury, zarządzenia bądź inne akty normatywne administratora zawierają niezbędne zapisy i co ważne, czy pracownicy mają praktyczną wiedzę o tym, jak procedurę stosować i czy ją stosują.

Jeżeli w procedurze są opisane zasady tzw. czystego biurka, które pracownicy są w stanie doskonale opisać, potwierdzając tym samym ich zrozumienie, a mimo to nie stosują się do nich, jest to jasny sygnał dla IOD, że jest to obszar wymagający pilnej zmiany. Innym przykładem może być wręczanie osobom fizycznym klauzuli informacyjnej. Inspektor ochrony danych powinien zweryfikować, czy w zakresie wykonywania obowiązku informacyjnego określonego art. 13 i 14 RODO administrator jest zgodny z przepisami. Procedura może nakładać na pracownika obowiązek wręczania lub wysłania dokumentu. Jeżeli jednak ta czynność nie jest wykonywana, wówczas administrator jest narażony na sankcje wynikające z RODO.

Poza oceną zgodności dokumentów IOD powinien sprawdzić, jak w praktyce wygląda codzienna praca jednostki i jak w praktyce dane są przetwarzane. Na to będą się składały:

- informacje o systemach, z którymi ściśle są powiązane umowy z dostawcami,
- kwestia transferu danych poza Europejski Obszar Gospodarczy, jak również
- zasady usuwania danych czy
- realizacja praw podmiotów danych.

Przeprowadzona weryfikacja danego obszaru zawsze powinna zakończyć się raportem opracowanym przez IOD, który zostanie udostępniony administratorowi danych. Planując kontrolę w jednostkach, IOD musi pamiętać, że za samym zaleceniem zmiany powinny iść wdrożenia poprawek określone harmonogramem. Końcowym etapem powinna być ponowna weryfikacja wdrożenia rekomendacji IOD.

W celu wzmocnienia zasady rozliczalności administrator może wprowadzić dodatkowe kontrole dla procesów, które są kluczowe. Bardzo często będą to też procesy związane z największym ryzykiem przetwarzania danych dla danej organizacji. I tutaj również można przyjąć różne podejście, tj. wykazać procesy kluczowe dla firmy albo dla poszczególnych obszarów. Sugestia, jak taki proces kontrolny ustalić, może, a nawet powinna być przekazana przez IOD administratorowi.

Inspektor ochrony danych jest osobą, która ma największą wiedzę na temat procesów i odpowiednie narzędzia do tego, aby diagnozować i analizować sytuację związaną z przetwarzaniem danych osobowych. Takim narzędziem będzie rejestr czynności przetwarzania, ale również uczestnictwo IOD w procesie oceny skutków dla ochrony danych.

Wydając odpowiednią rekomendację w zakresie ustalenia kluczowych procesów, IOD musi zawsze uwzględniać elementy ryzyka przetwarzania danych związane z konkretnymi danymi i celem ich przetwarzania. Należy wskazać, że same kontrole procesów powinny ustalać jednostki, a nie zaś. Wynika to z tego, że inspektor nie powinien sam siebie w tym zakresie weryfikować. Powinien

natomiast zbadać, czy mechanizmy kontrolne są faktycznie prawidłowo dobrane do poziomu ryzyka związanego z przetwarzaniem danych osobowych.

W procesie kontroli wykonywanej przez IOD można umieścić także kontrole wykonywane u dostawców i poddostawców. Taka weryfikacja powinna objąć samą umowę oraz wizytę na miejscu w celu sprawdzenia, czy faktycznie postanowienia umowne są realizowane. Wskazać tutaj należy, że przy dużych organizacjach, które korzystają z wielu dostawców, plan przeprowadzanych u nich kontroli powinien stanowić odrębny dokument zazębiający się z harmonogramem kontroli ADO.

Autor:

Anna Jaworska-Kłosowicz,

prawnik, ekspert ds. ochrony danych osobowych, audytor wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji 27001, studentka II roku studiów doktoranckich

Stopka redakcyjna

Redaktor:	Wioleta Szczygielska
ISBN:	978-83-269-7622-3
E-book nr:	2HH0774
Firma:	Wiedza i Praktyka sp. z o.o.
Adres:	03-918 Warszawa, ul. Łotewska 9a
Kontakt:	Telefon 22 518 29 29, faks 22 617 60 10, e-mail: *cok@wip.pl*
NIP:	526-19-92-256
Numer KRS:	0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego: 200.000 zł, Nr rejestrowy BDO: 000008579