

# RODO w instytucjach publicznych

**ROZMOWA** | Podmioty z sektora publicznego będą musiały wyznaczyć inspektora ochrony danych. Dziś podobną rolę pełni administrator bezpieczeństwa informacji, lecz jego powołanie jest dobrowolne.

**W:** Za nieco ponad miesiąc zaczniemy stosować unijne rozporządzenie o ochronie danych, czyli tzw. RODO. Jakie najważniejsze działania musiały/muszą podjąć podmioty będące administratorami danych osobowych, by działać zgodnie z tym rozporządzeniem?

DR EDYTA BIELAK-JOMAA, GENERALNY INSPEKTOR OCHRONY DANYCH OSOBOWYCH (GIODO): Przepisy ogólnego rozporządzenia o ochronie danych, choć we wszystkich państwach Unii Europejskiej zaczęły być bezpośrednio stosowane od 25 maja 2018 r., to weszły w życie w 2016 r. Administratorzy danych mieli dwa lata, by przygotować się do reformy systemu ochrony danych osobowych. Od 25 maja 2018 r. ich działania muszą być w pełni zgodne z RODO.

GIODO od samego początku wspierał ich w tym procesie, m.in. poprzez liczne działania edukacyjne i informacyjne. Wszystkim, którzy dopytywali, jak powinni się do nich przygotować, wskazywaaliśmy, że w pierwszej kolejności należy przeprowadzić wewnętrzny audyt, dokonać przeglądu procesów i działań, podejmowanych w związku z przetwarzaniem danych osobowych. Podpowiadaliśmy, by administratorzy sprawdzili przede wszystkim, jakie dane przetwarzają, na jakiej podstawie prawnej, czy dane te są adekwatne do celów, jakie mają być osiągnięte. Zachęcaliśmy ich do ustalenia, jakie ryzyka wiążą się z przetwarzaniem przez nich danych osobowych. Podkreślaliśmy, że taki audyt przeprowadzony pod kątem RODO może wykazać, że konieczna jest modyfikacja dotychczasowych procedur związanych z przetwarzaniem danych czy skorygowanie stosowanych zabezpieczeń, co pozwoli na opracowanie i wdrożenie niezbędnych zmian z odpowiednim wyprzedzeniem.

**Rozporządzenie zobowiązuje administratorów danych do opracowania i wdrożenia procedur bezpieczeństwa, nie narzuca jednak rozwiązań. To duża odpowiedzialność. Czy każdy urząd będzie prowadził własne rozwiązania?**

RODO nie zmienia w sposób istotny podstaw prawnych czy zasad przetwarzania danych osobowych. Nowe jest jednak podejście do ich ochrony, które wyraża się m.in. w tym, iż RODO daje administratorom danych dużą samodzielność i elastyczność w tym zakresie. Z jednej bowiem strony, muszą oni sami przeprowadzić szczegółową analizę prowadzonych procesów przetwarzania danych i dokonać samodzielnej oceny ryzyka, jakie owo przetwarzanie stwarza dla praw i wolności osób, których dane dotyczą. Z drugiej strony zaś mają większą dowolność w doborze rozwiązań i środków służących zabezpieczeniu danych.

RODO nie wskazuje środków technicznych i organizacyjnych, jakie należy zastosować w celu zapewnienia właściwej ochrony przetwarzanym danym. Dotyczy to zarówno danych przetwarzanych w sposób tradycyjny (w postaci papierowych spisów, kartotek, skródowników czy wykazów), jak i danych przetwarzanych przy użyciu systemów informatycznych. Rozporządzenie stanowi jedynie, że środki, jakie administrator musi zastosować, powinny być odpowiednie do zakresu, kontekstu i celu, a także ryzyka naruszenia praw i wolności osób, których dane są przetwarzane. Wskazuje, że przy ocenie ryzyka i ustanawianiu zabezpieczeń minimalizujących to ryzyko należy uwzględnić stan wiedzy technicznej, koszt wdrażania, a także skutki, jakie zidentyfikowane zagrożenia mogą powodować w sferze naruszenia praw i wolności osób, których dane dotyczą. W tym akcie prawnym nie znajdziemy więc odpowiedzi, jakie działania należy podjąć, aby takie ryzyko ocenić ani żadnej metodyki w tym zakresie.

**Czy Generalny Inspektor Ochrony Danych Osobowych może zaproponować instytucjom publicznym jakieś rozwiązania w tym zakresie?**

GIODO, aby wspomóc administratorów w realizacji tego zadania, przygotował dwuczęściowy poradnik dotyczący stosowania podejścia opartego na ryzyku, który jest dostępny na naszej stronie internetowej. Jego lektura może pomóc w zrozumieniu tego zagadnienia i przeprowadzeniu odpowiednich ocen.

Takich opracowań, wskazówek i wyjaśnień jest na naszej stronie internetowej więcej. Dla przykładu wymienię te najnowsze, jak choćby dotyczące sposobu realizacji określonego w art. 30 RODO obowiązku prowadzenia rejestru czynności oraz kategorii czynności czy propozycję wykazu rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych.

Ponadto GIODO jako członek Grupy Roboczej Artykułu 29 – niezależnego europejskiego organu doradczego Komisji Europejskiej w zakresie ochrony danych osobowych i prywatności – wspólnie z innymi



DR EDYTA BIELAK-JOMAA  
Generalny Inspektor Ochrony Danych Osobowych

europejskimi rzecznikami ochrony danych przygotowuje wytyczne, które mają ułatwić administratorom danych zrozumienie i stosowanie konkretnych rozwiązań i instrumentów ogólnego rozporządzenia. Powstało już blisko 20 tego typu dokumentów, a nad kolejnymi prace wciąż się toczą. Wszystkie te dokumenty są dostępne na stronie internetowej urzędu. To wprawdzie wyjaśnienia pewnych zagadnień, a nie gotowe recepty do zastosowania przez każdego administratora danych, ale biorąc jednak pod uwagę istotę i filozofię RODO, tworzenie jednakowych, szablonowych wzorców byłoby sprzeczne z duchem obecnej reformy.

Ale jeśli rozmawiamy o wskazówkach związanych ze stosowaniem RODO, to chciałabym zwrócić uwagę na inny pomocny w tym zakresie instrument – kodeksy postępowania, którym GIODO poświęcił na początku tego roku specjalny warsztat informacyjno-szkoleniowy. Dokumenty te mogą być tworzone przez zrzeczenia oraz inne podmioty reprezentujące różne kategorie administratorów czy podmiotów przetwarzających. Ich celem jest doprecyzowanie postanowień rozporządzenia z uwzględnieniem specyfiki danego sektora czy możliwych do zastosowania środków technicznych i organizacyjnych mających na celu zabezpieczenie danych. Mogą być więc one pewnego rodzaju instrukcjami działania.

Idea tworzenia kodeksów postępowania (obecnie nazywanych kodeksami dobrych praktyk) nie jest nowa. W Polsce GIODO od dawna zachęcał do ich tworzenia i myślę, że to był dobry kierunek. Ogólne rozporządzenie o ochronie danych nadaje im jeszcze większą rangę, wskazując m.in., że muszą być zatwierdzone przez organy nadzorcze. M.in. dzięki temu kodeksy, ze znanego dotąd narzędzia wizerunkowo-promocyjnego, staną się instrumentem o charakterze prawnym. Warto dodać, że ich przestrzeganie będzie miało wpływ na wysokość administracyjnej kary pieniężnej nakładanej przez GIODO w przypadku naruszenia prawa.

Działania i inicjatywy GIODO mających na celu pomóc w dostosowaniu się do jak najlepszego wypełniania nowych obowiązków jest znacznie więcej. Z pewnością będziemy je kontynuować.

**Czy wszystkie instytucje publiczne będą w jednakowym zakresie stosowały nowe przepisy? Może istnieją jakieś wyłączenia, a jeśli tak, jakie i kogo dotyczą?**

Co do zasady RODO dotyczy każdego, kto przetwarza dane osobowe w związku z działalnością zarobkową, zawodową, realizacją zadań publicznych bądź celów statutowych. Jego przepisy muszą więc stosować m.in. wszystkie instytucje publiczne. Pewne różnice mogą wynikać ze specyfiki działania określonych podmiotów oraz rodzaju przetwarzanych danych czy skali tych działań.

Jednocześnie RODO dopuszcza wprowadzanie ograniczeń jego stosowania, ale tylko wówczas, jeśli spełnione są warunki wskazane w jego art. 23. Ponadto, co należy podkreślić, artykuł ten mówi o ograniczeniach, a nie o wyłączeniach. Zgodnie bowiem z tym artykułem, państwo członkowskie może

aktem prawnym ograniczyć zakres określonych w RODO praw i obowiązków, ale ograniczenie to nie może naruszać podstawowych praw i wolności oraz musi być w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym ważnym, wskazanym w tym przepisie celom. Takim chociażby, jak bezpieczeństwo narodowe czy publiczne, zapobieganie przestępczości albo ściganie przestępstw. Jeśli już w prawie krajowym wprowadza się ograniczenie, to w odpowiednim przepisie trzeba określić cele przetwarzania, kategorie danych, zakres wprowadzonych ograniczeń, zabezpieczenia zapobiegające nadużyciom lub niezgodnemu z prawem dostępowi bądź przekazywaniu, zasady przechowywania itd.

Polski ustawodawca planuje wprowadzić takie wyłączenia w przepisach sektorowych, lecz GIODO zgłasza co do tych rozwiązań fundamentalne uwagi. Wiele z projektowanych rozwiązań obniża bowiem poziom ochrony danych osobowych obywateli, który – zgodnie z rozporządzeniem – miał ulec wzmocnieniu. Dlatego na wszystkich etapach prac legislacyjnych zabiegamy o zmianę projektowanych regulacji.

**Czym obowiązki związane z przetwarzaniem danych osobowych przez podmioty sfery publicznej różnią się od obowiązków dotyczących podmiotów ze sfery biznesowej? Czy podmioty publiczne będą np. musiały uzyskiwać zgodę na gromadzenie/przetwarzanie danych? A jeśli tak, w jakich przypadkach?**

Jedną z ważniejszych różnic między podmiotami ze sfery publicznej a podmiotami ze sfery prywatnej jest to, że podmioty z sektora publicznego będą musiały wyznaczyć inspektora ochrony danych (IOD). Dziś podobną rolę pełni administrator bezpieczeństwa informacji (ABI), lecz jego powołanie jest dobrowolne. Po 25 maja 2018 r. w sferze publicznej pojawi się obowiązek jego wyznaczenia.

Ma to być ekspert, którego wiedza, doświadczenie i umiejętności będą fundamentem, na którym zbudować można system skutecznej ochrony danych osobowych danego podmiotu.

Rola IOD jest kluczowa dla ochrony danych osobowych, gdyż jako ekspert w tej dziedzinie ma on doradzać administratorowi danych i monitorować, czy przetwarzanie danych w zatrudniającej go instytucji odbywa się zgodnie z RODO. Stąd tak istotne jest zapewnienie mu niezależności, czemu służyć ma m.in. właściwe umiejscowienie go w strukturze organizacyjnej, tj. bezpośrednie podporządkowanie najwyższemu kierownictwu. Ponadto IOD będzie punktem kontaktowym dla osób, których dane są przetwarzane, a także dla organu nadzorczego. Jego rolą będzie też m.in. szkolenie pracowników instytucji, na rzecz której działa.

Co zaś do zgody jako podstawy prawnej umożliwiającej przetwarzanie danych osobowych przez podmioty z sektora publicznego, to może być ona stosowana jedynie wyjątkowo. Zgodnie bowiem z art. 7 Konstytucji RP, organy władzy publicznej muszą działać na podstawie i w granicach prawa. Dlatego, co do zasady, to przepisy prawa powinny określać, jakie dane osobowe i w jakich celach konkretne podmioty z sektora publicznego mają prawo pozyskiwać i wykorzystywać. Zatem to przepisy prawa powinny być przesłanką umożliwiającą przetwarzanie danych osobowych.

**Od wielu miesięcy trwają prace nad nową ustawą o ochronie danych osobowych, ale do tej pory nie została uchwalona. Czy ta ustawa jest konieczna do stosowania RODO? Jakie istotne zmiany ma ona wprowadzić?**

Mam nadzieję, że polski ustawodawca doloży wszelkich starań, by przed 25 maja 2018 r. przyjąć odpowiednie przepisy krajowe, tak byśmy byli w pełni gotowi do stosowania RODO.

Niemniej chciałabym podkreślić, na co już wielokrotnie zwracałam uwagę, że przepisy krajowe mają ograniczony zakres, regulują bowiem – jak np. nowa ustawa o ochronie danych osobowych – jedynie kwestie proceduralne dotyczące postępowania przez organem nadzorczym czy prowadzenia przez niego kontroli bądź certyfikacji. To RODO określa zarówno podstawowe prawa osób, których dane są przetwarzane, jak i obowiązki ciążące na administratorach danych. Jednocześnie jest to akt prawny, który, co już wspomniałam, będzie stosowany bezpośrednio.

Zatem bez względu na to, czy uda się uchwalić nowe przepisy krajowe, w tym nową ustawę o ochronie danych osobowych przed 25 maja 2018 r., czy nie, to i tak wszystkie podmioty objęte RODO zobowiązane będą do stosowania jego przepisów bezpośrednio. ©

—rozmawiała Teresa Niedziela