

# Znak jakości nada jednak prezes

**ZMIANA PRAWA:** Już od 25 maja 2018 r. przedsiębiorcy będą mogli starać się o nowy rodzaj certyfikatów, które świadczyć mają o tym, że dany podmiot przetwarza dane zgodnie z przepisami wchodzącego wówczas w życie unijnego rozporządzenia RODO. Ministerstwo Cyfryzacji uznało, że najlepiej, jeśli te znaki potwierdzające jakość ochrony danych osobowych będzie wydawał prezes Urzędu Ochrony Danych Osobowych (który zastąpi generalnego inspektora ochrony danych osobowych). Ta koncepcja, przedstawiona w projekcie ustawy o ochronie danych osobowych, który na początku września trafił do konsultacji społecznych, jest zgoła odmienna, niż zapowiadano to jeszcze kilka tygodni temu. Pierwotnie planowano, że nadawaniem znaków jakości zajmować będą się podmioty prywatne, akredytowane przez organ nadzorczy. Powstaje wątpliwość: czy nowy urząd poradzi sobie z natłokiem wniosków, które do niego trafią? Zwłaszcza że procedura certyfikacji będzie wiązała się z koniecznością zweryfikowania każdego podmiotu z osobna. Pytanie jest tym bardziej zasadne, że nowa instytucja będzie miała wiele innych nowych obowiązków. A certyfikaty mogą mieć duże znaczenie dla przedsiębiorców.

Oprac. JP



**dr Paweł Litwiński**  
adwokat, Instytut Allerhanda,  
partner w Barta Litwiński Kancelaria  
Radców Prawnych i Adwokatów sp. z o.o.

Biuro rachunkowe, agent ubezpieczeniowy, adwokat i radca prawny, firma zajmująca się obsługą informatyczną – chyba każdy przedsiębiorca korzysta z ich usług. Ale skąd ma wiedzieć, czy te podmioty w odpowiedni sposób chronią dane osobowe? A w jaki sposób z kolei podmioty świadczące usługi wiążące się z przetwarzaniem danych osobowych mogą budować swoją przewagę nad konkurencją? I w jaki sposób mają spełniać wymagające i nierzadko trudne do spełnienia rygory związane z przetwarzaniem danych osobowych?

Naprzeciw tym potrzebom wychodzą przepisy ogólnego rozporządzenia o ochronie danych osobowych (RODO) wprowadzające procedurę certyfikacji w zakresie ochrony danych osobowych. Pomysł jest prosty: stworzenie mechanizmu, który oceni, czy dany podmiot działa zgodnie z przepisami o ochronie danych osobowych. Ma to być coś na kształt np. certyfikatów ekologicznych.

RODO przewiduje dwie możliwości wydawania certyfikatów na poziomie krajowym:

- przez organ nadzorczy, czyli w Polsce przez prezesa Urzędu Ochrony Danych Osobowych (następcę GIODO), albo
- przez podmioty prywatne, akredytowane przez organ nadzorczy.

Ministerstwo Cyfryzacji w projekcie ustawy o ochronie danych osobowych zdecydowało się na drugą z możliwości – certyfikaty mają być przyzna-

## Dylemat: co wybrać?

Oprócz możliwości uzyskania certyfikacji z UODO przedsiębiorcy będą mogli uzyskać analogiczne zaświadczenie wydawane przez organ unijny – Europejską Radę Ochrony Danych. Uzyskanie go od organu unijnego może okazać się atrakcyjne, gdyż ma skutkować wspólną certyfikacją, europejskim znakiem jakości ochrony. Będzie to istotne zwłaszcza dla przedsiębiorstw prowadzących działalność na terenie różnych państw członkowskich Unii.

Co istotne, organ unijny będzie wydawał znaki na podstawie własnych mechanizmów certyfikacyjnych. W trakcie dotychczasowych prac na szczeblu unijnym pojawiły się pomysły, aby w tym procesie stosować podejście sektorowe – a więc różne kryteria certyfikacji w zależności od rodzaju działalności prowadzonej przez dane przedsiębiorstwo. Podejście to wydaje się słuszne choćby z tego powodu, że przedsiębiorstwa przetwarzają zarówno zwykłe, jak i szczególnego rodzaju dane osobowe, tj. dane wrażliwe, w szczególności dotyczące np. zdrowia czy wyznania.

W trakcie dotychczasowych prac legislacyjnych na szczeblu krajowym nie wskazano jeszcze, jakie będą kryteria certyfikacji. Należy także zwrócić uwagę, że w RODO stosuje się szersze pojęcie (mechanizm certyfikacji) niż w przepisach krajowych (kryteria certyfikacji). Istotne, aby mechanizmy certyfikacyjne krajowe oraz unijne były jednolite. Z tego też względu wydaje się właściwe, aby – o ile na szczeblu unijnym przeważą podejście sektorowe – także na szczeblu krajowym zastosować różne kryteria w zależności od rodzaju prowadzonej przez przedsiębiorstwo działalności. Do powyższej jednolitości będzie dążył prawdopodobnie sam organ unijny – Rada Ochrony Danych, certyfikacja przez ten organ odbywa się bowiem na zasadach mechanizmu spójności, który zakłada jednolite stosowanie RODO w całej Unii.

Anna Popowicz-Pazdej

wane bezpośrednio przez prezesa UODO. Jak więc ten proces będzie wyglądał w praktyce?

## Dla kogo

O certyfikaty będą mogły się ubiegać podmioty zajmujące się przetwarzaniem danych osobowych jako administrator danych, a także te, które przetwarzają je na zlecenie. Zatem certyfikaty będą mogły być również wydawane tym przedsiębiorcom, którzy profesjonalnie świadczą usługi związane z przetwarzaniem danych osobowych na rzecz innych podmiotów.

Zgodnie z projektem ustawy od 25 maja 2018 r. do prezesa UODO będą mogły się zgłaszać podmioty, które będą zainteresowane uzyskaniem nowe-

go świadectwa. W tym celu będą musiały złożyć wniosek o certyfikację, który oprócz danych ubiegającego się ma zawierać informacje potwierdzające spełnianie określonych kryteriów. Te jeszcze nie zostały przedstawione, zostaną opracowane przez prezesa UODO i udostępnione w Biuletynie Informacji Publicznej.

## Krótki czas

Zgodnie z projektem Ministerstwa Cyfryzacji wniosek o wydanie certyfikatu powinien zostać rozpatrzony w terminie nie dłuższym niż trzy miesiące od dnia złożenia. Jeżeli zostanie rozpatrzony pozytywnie, to wydawany będzie certyfikat. Za jego wydanie i przeprowadzenie postępowania z tym związanego pobierana będzie opłata. Ma ona wynosić trzykrotność przeciętnego miesięcznego wynagrodzenia za pracę w gospodarce narodowej w roku poprzednim (w 2016 r. było to 4047,21 zł). Zatem opłata przekroczy 12 tys. zł.

## Zalety

Co taki certyfikat będzie oznaczał dla podmiotu certyfikowanego? Zgodnie z art. 42 ust. 1 RODO świadczyć będzie on o zgodności operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające z przepisami RODO. Będzie to więc urzędowe potwierdzenie tego, że administrator danych lub podmiot przetwarzający dane na zlecenie działa zgodnie z przepisami RODO. [schemat]

## Kontrola i cofnięcie

Oczywiście takie potwierdzenie nie będzie wydawane raz na zawsze, ale na czas określony, wskazany w jego treści. W tym czasie posiadacze będą zobowiązani do spełniania kryteriów certyfikacji, co może być sprawdzone przez prezesa UODO. Osoba przeprowadzająca czynności sprawdzające będzie miała prawo do:

- wstępu na teren oraz do budynków, lokali lub innych pomieszczeń,
- wglądu do dokumentów i informacji mających bezpośredni związek z działalnością objętą certyfikacją,
- oględzin urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych,
- uzyskania ustnych lub pisemnych wyjaśnień w sprawach związanych z działalnością objętą certyfikacją.

Jeżeli podmiot przestanie spełniać kryteria, to udzielona certyfikacja będzie cofana przez prezesa UODO.

## Wiele niewiadomych

Z mechanizmem certyfikacji wiążą się pewne niewiadome, na które dzisiaj nie sposób znaleźć odpowiedzi. Najważniejsza dotyczy samej procedury certyfikacji. Ponieważ Ministerstwo Cyfryzacji zde-

## DLACZEGO WARTO POTWIERDZIĆ JAKOŚĆ OCHRONY DANYCH OSOBOWYCH

**Za stosowaniem certyfikacji w praktyce przez podmioty przetwarzające dane osobowe przemawiają liczne argumenty. Jakie mogą być zalety certyfikatów?**

- ✓ **Będą świadczyć o zgodności operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające z przepisami RODO.** To fundamentalna zmiana w stosunku do obecnie obowiązującego stanu prawnego, w którym brak jest jakiegokolwiek mechanizmu umożliwiającego zweryfikowanie, czy dany podmiot rzeczywiście ma takie kwalifikacje, jak twierdzi, i stosuje rozwiązania zgodne z prawem.
- ✓ **Mogą stać się wskazówką ułatwiającą wybór podmiotu przetwarzającego dane.** A wybór odpowiedniego podmiotu, który będzie przetwarzał dane osobowe w imieniu administratora danych – staje się na gruncie RODO obowiązkiem. Zgodnie bowiem z art. 28 ust. 1 RODO administrator danych ma prawny obowiązek korzystania z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Zatem szukając biura rachunkowego, agenta ubezpieczeniowego, adwokata lub radcy prawnego czy firmy zajmującej się obsługą informatyczną, przedsiębiorcy po 25 maja 2018 r. powinni zwrócić uwagę, czy dany podmiot ma certyfikat; jeśli posiada, powinien to być argument przemawiający za wyborem właśnie tego wykonawcy.
- ✓ **Mogą być wykorzystywane w budowaniu przewagi nad konkurentami.** Będą czymś, czym przedsiębiorcy mogą się chwalić. Umieszczanie informacji o posiadaniu certyfikatu na stronie internetowej przedsiębiorcy z dużym prawdopodobieństwem stanie się czymś naturalnym.
- ✓ **Mogą mieć znaczenie podczas kontroli.** Posiadanie certyfikatu będzie korzystne także dlatego, że stosowanie zatwierdzonego mechanizmu certyfikacji może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciężących na nim obowiązków prawnych (art. 24 ust. 3 RODO). W szczególności certyfikacja może służyć m.in. do wykazywania stosowania rozwiązań z zakresu privacy by design i privacy by default (art. 25 RODO) oraz jako element potwierdzający wywiązywanie się z obowiązków zabezpieczenia danych osobowych (art. 32 RODO). Innymi słowy, certyfikacja będzie korzystna także dla tych podmiotów, które nie świadczą usług związanych z przetwarzaniem danych osobowych, ale które same takie dane przetwarzają na własne potrzeby.
- ✓ **Posiadanie może mieć wpływ na wymiar kary.** W art. 83 unijnego rozporządzenia znajduje się dyrektywa wymiaru kar – są to czynniki, które wpływają na wysokość kar, a prezes UODO powinien uwzględnić je w procesie nakładania kary. Wśród nich wymieniono stosowanie mechanizmów certyfikacji. Oznacza to, że legitymowanie się certyfikatem przed podmiot, na który ma być nałożona kara finansowa, będzie wpływało na obniżenie tej kary.

© P



# UODO

## OPINIA EKSPERTA



DR EDYTA BIELAK-JOMAA

generalny inspektor ochrony  
danych osobowych

**P**orównanie pierwszego projektu ustawy o ochronie danych osobowych przedstawionego wiosną tego roku z obecną jego wersją dowodzi, że resort cyfryzacji z jednej skrajności popada w drugą. Pierwotnie UODO miał jedynie akredytować podmioty certyfikujące. Najnowsza propozycja zakłada zaś, że będzie jedynym uprawnionym do udzielania certyfikacji. Tymczasem od początku dyskusji na ten temat, opierając się na 20-letnim doświadczeniu urzędu, a także doświadczeniach moich odpowiedników z innych państw członkowskich UE, proponowałam przyjęcie modelu hybrydowego, uznając go za najskuteczniejszy.

Krąg podmiotów przyznających certyfikaty powinien być jak najszerszy. W różnych państwach europejskich to właśnie organy ochrony danych osobowych prowadzą programy certyfikacyjne, co w żaden sposób nie ogranicza funkcjonowania rynku podmiotów certyfikujących, lecz raczej ten rynek wzmacnia i stymuluje. Zwłaszcza że teraz już nie będziemy mogli mówić jedynie o krajowym rynku certyfikatów w zakresie ochrony danych osobowych, lecz raczej o rynku europejskim. I to tam będzie się rozgrywała konkurencja między dostępnymi mechanizmami certyfikacyjnymi. Proponowane przez ministerstwo rozwiązanie może skutkować tym, że w Polsce rynek certyfikacji w ogóle się nie rozwinie. Także dlatego, że z pewnością polskim administratorom certyfikaty będą oferowane przez podmioty certyfikujące z innych państw członkowskich UE.

Opiniując tę wersję projektu ustawy o ochronie danych osobowych, w którym zaproponowano, aby krajowy organ nadzorczy udzielał akredytacji podmiotom certyfikującym, wskazywałam, że rozwiązanie takie jest możliwe i korzystne z punktu widzenia prestiżu i pozycji urzędu. Podnosiłam jednak możliwość wykonywania tego zadania przez istniejącą krajową jednostkę akredytującą (Polskie Centrum Akredytacji). To ważne, by w procesie akredytacji podmiotów certyfikujących spełnić rygorystyczne procedury dotyczące zapewnienia transparentności i niezależności. Poszczególne etapy procesu, takie jak weryfikacja warunków, audyt akredytacyjny, ocena wyników i ich zatwierdzenie, powinny być realizowane przez różne osoby.

Istotna w tym procesie jest również potrzeba określenia kryteriów akredytacji. Opierając się na dotychczasowych projektach ministerstwa, GIODO od dłuższego czasu przygotowywał te kryteria. Wprowadzone przez resort zmiany powodują, że wszystkie prace prowadzone dotychczas przez GIODO trzeba będzie wyrzucić do kosza.

Zaproponowany termin trzech miesięcy na przeprowadzenie certyfikacji wydaje się zbyt krótki, bo w toku tej procedury szczególnie należy podjąć wiele skomplikowanych czynności. W przypadku podmiotów o złożonej strukturze dokonanie akredytacji w trzymiesięcznym terminie może być niewykonalne.



Oprac. JAS

cydowało się na certyfikowanie przez prezesa UODO, a nie przez podmioty prywatne, to niewątpliwie korzystnym skutkiem tej decyzji będzie zapewnienie jednolitości certyfikacji i wyeliminowanie niepewności związanej z oddaniem certyfikacji w prywatne ręce. Ale z innej strony GIODO był dotychczas znany raczej z przedłużających się postępowań administracyjnych i pozostaje otwarte pytanie, ile będą trwały postępowania certyfikacyjne. W interesie przedsiębiorców jest, aby trwały jak najkrócej.

Kolejna niewiadoma to kryteria certyfikacji – po pierwsze, nie sposób dzisiaj przewidzieć ich treści, szczegółowości czy w ogóle możliwości spełnienia; po drugie, nie wiemy, kiedy zostaną opracowane i opublikowane, a to warunkuje możliwość składania wniosków o przyznanie certyfikatów. Nie zmienia to jednak ogólnej bardzo pozytywnej oceny całości rozwiązania – certyfikacja z pewnością wpłynie pozytywnie na przestrzeganie przepisów o ochronie danych osobowych.

