Październik 2015
issn 2391-5781
nr 1

TRAPLE KONARSKI PODRECKI I WSPÓLNICY
KANCELARIA PRAWNA

OCHRONA DANYCH OSOBOWYCH

Aktualności, Orzecznictwo, Studia przypadków, Opracowania

- Udostępnianie danych a powierzanie na zlecenie ADO
- ABI u przetwarzającego (procesora)
- Sprawdzenie i sprawozdanie w praktyce

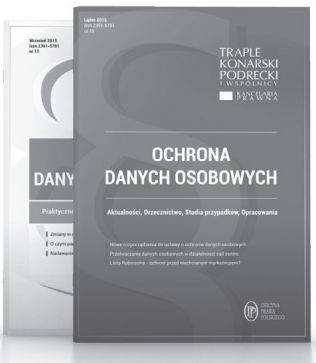
OFICYNA PRAWA POLSKIEGO

OCHRONA DANYCH OSOBOWYCH – profesjonalnie i kompleksowo

Poznaj najnowsze zmiany prawne i stanowiska ekspertów z Kancelarii Prawnej Traple, Konarski, Podrecki i Wspólnicy, oraz praktyków pełniących od lat funkcje Administratorów Bezpieczeństwa Informacji (ABI) w różnych branżach.

W naszym miesięczniku znajdziesz:

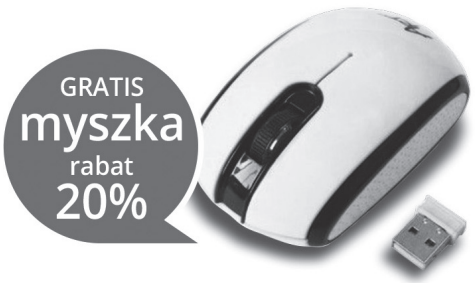
- gotowe wzory dokumentów związanych z przetwarzaniem danych osobowych,
- przykładowe zapisy umowne,
- wyjaśnienie zawiłych kwestii prawnych, w szczególności na styku ochrony danych osobowych i nowych technologii,
- porady, jak zachować się podczas kontroli GIODO,
- zmiany w prawie i ich konsekwencje dla pracy ABI, ADO i ASI,
- porady szczegółowe na temat danych osobowych dla firm prywatnych oraz administracji publicznej,
- materiały do szkoleń z zakresu danych osobowych.



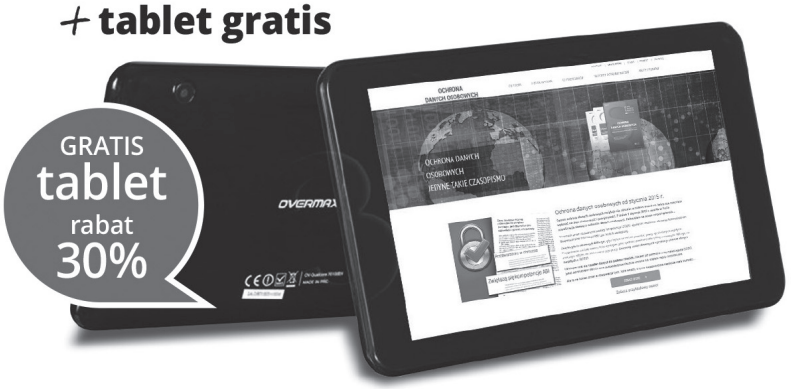
1 numer prawniczy raz na kwartał!

Zamów prenumeratę!

Półroczną z 20% zniżką
+ myszka gratis



Roczną z 30% zniżką
+ tablet gratis



Zamów prenumeratę już dziś na FabrykaWiedzy.com,
lub przez Centrum Obsługi Klienta: **tel. 22 518 29 29, email: cok@wip.pl**

Spis treści

Wioleta Szczygielska
redaktor prowadząca
odo@wip.pl
www.odo.wip.pl

Drodzy Czytelnicy!

Oddajemy w Państwa ręce specjalny dodatkowy numer miesięcznika „Ochrona danych osobowych". Do grona naszych autorów dołączył dr Grzegorz Sibiga, który też objął pismo patronatem merytorycznym.
Tematem przewodnim tego numeru jest realizacja jednego z najważniejszych obowiązków administratora bezpieczeństwa informacji, jaki wprowadziła nowelizacja ustawy o ochronie danych osobowych. Chodzi o przeprowadzenie sprawdzenia zgodności przetwarzania danych osobowych z przepisami i przygotowanie sprawozdania z tego sprawdzenia.
Nasz ekspert podpowiada, jak w praktyce przygotować się do wypełnienia tego obowiązku i jak go wypełnić.
Piszemy też o sprawdzeniu, które administrator bezpieczeństwa informacji będzie przeprowadzał na zlecenie Generalnego Inspektora Ochrony Danych Osobowych. Warto zapoznać się z tym tematem, gdyż w przypadku niezrealizowania polecenia GIODO administrator bezpieczeństwa informacji może nawet zostać wykreślony z rejestru ABI.
W tym numerze znajdą Państwo także omówienie najważniejszych wyroków Trybunału Sprawiedliwości Unii Europejskiej odnośnie ochrony danych osobowych z ostatnich dwóch lat. Najistotniejsze z nich odnoszą się do danych biometrycznych, retencji danych osobowych oraz prawa do zapomnienia.
Piszemy też o najnowszych wydarzeniach związanych z ochroną danych osobowych. Przytaczamy m.in. stanowisko GIODO na temat planowanych zmian w dostępie służb do danych telekomunikacyjnych.

Życzę owocnej lektury!

PATRONAT MERYTORYCZNY

XAWERY KONARSKI

adwokat, wspólnik w Kancelarii Prawnej *Traple Konarski Podrecki i Wspólnicy*, ekspert prawny Polskiej Izby Informatyki i Telekomunikacji, Polskiej Izby Ubezpieczeń oraz Związku Pracodawców Branży Internetowej IAB Polska

DR GRZEGORZ SIBIGA

adwokat w Kancelarii Prawnej *Traple, Konarski, Podrecki i Wspólnicy*, kierownik Zakładu Prawa Administracyjnego w Instytucie Nauk Prawnych PAN w Warszawie

GIODO o dostępie służb do danych

Forma kontroli pozyskiwania danych telekomunikacyjnych przez służby specjalne i policję zaproponowana w projekcie ustawy o zmianie ustawy o Policji i niektórych innych ustaw[1] jest niewystarczająca – uważa Generalny Inspektor Ochrony Danych Osobowych.

W opinii GIODO przepisy ustawy nowelizującej są sprzeczne z Konstytucją RP i Kartą Praw Podstawowych UE. Nie realizują też wytycznych z wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. (sygn. akt K 23/11). Nie uwzględniają też orzeczenia Trybunału Sprawiedliwości Unii Europejskiej z 8 kwietnia 2014 r. (połączone sprawy C-293/12 i C-594/12)[2], który stwierdził nieważność tzw. dyrektywy retencyjnej.

Potrzebna kontrola służb

Nad pozyskiwaniem danych telekomunikacyjnych przez służby specjalne i policję nadzór powinien sprawować niezależny organ zewnętrzny – uważa GIODO. Proponowana treść nie nakłada na te organy innych nowych obowiązków poza przekazywaniem sądom raz na sześć miesięcy sprawozdań obejmujących liczbę i rodzaj pozyskanych danych, podstawę prawną ich pozyskania oraz rodzaje przestępstw, w związku z którymi wystąpiono o dane.

W ramach kontroli sąd może zapoznać się z materiałami uzasadniającymi udostępnienie danych. Ten model kontroli przewiduje więc fakultatywną kontrolę następczą (sądy mogą z tego uprawnienia nie korzystać).

Takiego rozwiązania nie można uznać za należyte wykonanie wyroku Trybunału Konstytucyjnego, który stwierdził niezgodność przepisów ustawy o Policji oraz ustaw dotyczących innych służb z Konstytucją RP w zakresie, w jakim nie przewidują one niezależnej kontroli udostępnienia danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy Prawo telekomunikacyjne[3].

BARTOSZ JUSSAK
aplikant radcowski przy Okręgowej Izbie Radców Prawnych w Krakowie, prawnik w Kancelarii Prawnej Traple Konarski Podrecki i Wspólnicy

W 2014 roku służby, sądy i prokuratury złożyły do Urzędu Komunikacji Elektronicznej łącznie ponad 2 mln zapytań o dane telekomunikacyjne. GIODO twierdzi, że brak niezależnej kontroli państwa nad procesem pozyskiwania danych tych stwarza ryzyko nadużyć.

Model kontroli powinien opierać się na zasadzie każdorazowej, obowiązkowej oceny adekwatności, niezbędności i celowości udostępniania danych przez niezależny zewnętrzny organ. Kontrola następcza powinna być stosowana wyjątkowo.

Czas przetwarzania

Zastrzeżenia GIODO budzi też nieprecyzyjny sposób określenia okresu możliwości przetwarzania danych telekomunikacyjnych i pocztowych. Będą przetwarzane przez okres, w którym są niezbędne do realizacji ustawowych zadań. Nie rzadziej niż co trzy lata potrzeba ich dalszego przetwarzania będzie weryfikowana.

Takie określenie jest zbyt szerokie i stwarza możliwość nieuzasadnionego i bezterminowego przechowywania danych. Jest to sprzeczne z zasadą ograniczenia czasowego.

Zdaniem GIODO, projekt trzeba uzupełnić o obowiązek informacyjny wobec osób, których dane zostały pozyskane. Niejawne pozyskiwanie przez organy władzy publicznej informacji o jednostce wymaga zachowania daleko idących gwarancji proceduralnych. Dotyczy to przede wszystkim obowiązku poinformowania jej o podjętych wobec niej działaniach operacyjno-rozpoznawczych oraz pozyskaniu informacji na jej temat.

Zapewnienie informacji umożliwia jednostce skorzystanie z prawa dostępu do urzędowych dokumentów i zbiorów danych. Niepoinformowanie o informacjach zebranych o jednostkach przez władze publiczne narusza art. 51 ust. 3 i 4 Konstytucji RP.

[1] Druk nr 3765, projekt ustawy dostępny pod adresem: http://www.sejm.gov.pl/Sejm7.nsf/druk.xsp?nr=3765.

[2] Wyrok Trybunału Sprawiedliwości z 8 kwietnia 2014 r. w sprawie Digital Rights Ireland Ltd. (C-293/12) przeciwko Minister for Communications, Marine and Natural Resources i inni oraz Kärntner Landesregierung (C-594/12) i inni.

[3] Ustawa z 16 lipca 2004 r. Prawo telekomunikacyjne (tekst jedn.: Dz.U. z 2014 r. poz. 243 ze zm.).

TS w sprawie ochrony danych osobowych

W ciągu ostatnich dwóch lat Trybunał Sprawiedliwości Unii Europejskiej (TS UE) wydał orzeczenia, w których wyjaśnił wiele wątpliwości dotyczących praw jednostek w zakresie ochrony danych osobowych w cyfrowej rzeczywistości. Najistotniejsze z nich odnoszą się do danych biometrycznych, retencji danych osobowych oraz prawa do zapomnienia.

Wyrok TS UE z 17 października 2013 r. (w sprawie C-291/12)

Stan faktyczny

Michael Schwarz zwrócił się do niemieckiego miasta Bochum o wydanie mu paszportu. Nie zgodził się jednak na pobranie odcisków palców, które miały być przechowywane w tym paszporcie.
Miasto Bochum oddaliło jego wniosek. W związku z tym Schwarz wniósł do sądu skargę, w której kwestionował ważność art. 1 ust. 2 rozporządzenia nr 2252/2004[1].
Wprowadza ono obowiązek pobierania odcisków palców osób ubiegających się o paszport. Schwarz twierdził, że rozporządzenie nie zostało wydane w oparciu o właściwą podstawę prawną i jest dotknięte wadą proceduralną.
Ponadto, zarzucił mu naruszenie prawa do ochrony danych osobowych uznanego w Karcie praw podstawowych UE. W tych okolicznościach niemiecki sąd administracyjny zwrócił się do Trybunału Sprawiedliwości UE z pytaniem prejudycjalnym, dotyczącym ważności art. 1 ust. 2 tego rozporządzenia.

Zdaniem Trybunału

Oceniając przestawioną sprawę, TS UE stwierdził, że **nie istnieją okoliczności, które mogłyby wpłynąć na ważność art. 1 ust. 2 rozporządzenia 2252/2004**, zarówno z pespektywy spełnienia wymogów proceduralnych przy jego przyjmowaniu, jak i poszanowania praw podstawowych, w tym prawa obywateli do ochrony danych osobowych.

JOANNA JASTRZĄB
autorka jest aplikantką radcowską, pracownikiem departamentu Technologie Media Telekomunikacja w Kancelarii Prawnej Traple Konarski Podrecki i Wspólnicy

Zdaniem TS UE, odciski palców to dane osobowe, gdyż zawierają unikalne informacje o osobach fizycznych, pozwalające na ich zidentyfikowanie.
Ich pobieranie i przechowywanie na nośniku pamięci, który jest integralną częścią paszportu, jest ich przetwarzaniem i narusza prawa obywateli do poszanowania życia prywatnego i do ochrony danych osobowych. Prawa te jednak nie mają charakteru absolutnego i powinny zostać ocenione przez pryzmat ich funkcji w społeczeństwie.
TS UE stwierdził, że w tym zakresie ograniczenie prawa do ochrony danych osobowych w omawianym przypadku jest uzasadnione. Realizuje ono bowiem dwa precyzyjne cele:

- zapobiega fałszowaniu paszportów oraz
- uniemożliwia bezprawne korzystanie z nich przez osoby inne niż prawowity posiadacz.

W konsekwencji zmierza m.in. do uniemożliwienia nielegalnego wjazdu osób na terytorium Unii, a tym samym realizuje cel interesu ogólnego UE.
Co więcej, Trybunał potwierdził, że omawiane środki nie wykraczają poza to, co konieczne dla osiągnięcia celu.
Pobierane są jedynie dwa odciski palców, co nie wiąże się dla zainteresowanego ze szczególnym dyskomfortem. Jedyna realna alternatywa w postaci sporządzenia obrazu tęczówki oka jest obecnie procedurą znacznie bardziej kosztowną, a tym samym mniej dostosowaną do upowszechnionego korzystania.
Jednocześnie, rozporządzenie 2252/2004 zapewnia ochronę przed ryzykiem odczytania danych zawierających odciski palców przez osoby nieupoważnione.
W tym zakresie z art. 1 ust. 2 tego rozporządzenia wynika, że przedmiotowe dane są przechowywane na zintegrowanym z paszportem nośniku pamięci o wysokim stopniu zabezpie-

[1] Rozporządzenie Rady (WE) Nr 2252/2004 z 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i w dokumentach podróży wydawanych przez Państwa Członkowskie (Dz. U. L. 385/1).

czenia, który jest w wyłącznym posiadaniu osoby, na którą został wystawiony.
Rozporządzenie to nie przewiduje żadnej innej postaci lub sposobu przechowywania odcisków palców, w szczególności tworzenia przez krajowe organy scentralizowanej bazy danych. Dlatego też, ograniczenia praw jednostki, które ustanawia, są konieczne, proporcjonalne i tym samym prawnie dopuszczalne.
Powyższe argumenty zostały potwierdzone przez TS UE w wyroku z 16 kwietnia 2015 r. (w sprawach połączonych od C-446/12 do C-449/12). Dotyczył on również odmowy wydania obywatelom UE paszportów oraz, dodatkowo, dowodów osobistych zawierających odciski palców.
Rozstrzygając wątpliwości sądu odsyłającego, Trybunał uznał, że art. 1 ust. 3 rozporządzenia 2252/2004 w zakresie zabezpieczeń i danych biometrycznych w dokumentach podróży nie ma zastosowania do dowodów osobistych wydawanych przez państwa członkowskie swoim obywatelom. Tym samym, prawo europejskie nie wprowadza wymogu, by również w dowodach tożsamości przechowywano odciski palców ich posiadaczy. Nie wyklucza jednak możliwości regulacji tej kwestii na poziomie krajowym.

Wyrok TS UE z 8 kwietnia 2014 r. (w sprawach połączonych C-293/12 i C-594/12)

Stan faktyczny

W sierpniu 2006 roku Digital Rights (irlandzka organizacja zajmująca się obroną praw podstawowych w cyfrowym świecie) wystąpiła do High Court (irlandzkiego wysokiego trybunału) ze skargą. Kwestionowała w niej zgodność z prawem krajowych przepisów dotyczących zatrzymywania danych związanych z łącznością elektroniczną.
Organizacja domagała się w szczególności, aby sąd stwierdził nieważność dyrektywy 2006/24[1] oraz części Criminal Justice (Terrorist Offences) Act 2005 [ustawy karnej (przestępstwa o charakterze terrorystycznym) z 2005 roku]. Nakłada ona na dostawców usług telekomunikacyjnych obowiązek zatrzymywania danych o ruchu i lokalizacji w celu:
- zapobiegania i wykrywania przestępstw,
- prowadzenia czynności dochodzeniowo-śledczych oraz
- zapewnienia bezpieczeństwa państwa.

Ważność krajowych przepisów prawa telekomunikacyjnego, które są implementacją dyrektywy 2006/24, została także zakwestionowana przez ponad 11 tysięcy skarżących przed Verfassungsgerichtshof (austriackim trybunałem konstytucyjnym).
Jako główny zarzut powoływano naruszenie ich praw podstawowych.
Analiza tej kwestii, według austriackiego trybunału, wymagała oceny ważności przepisów unijnych, które zostały implementowane do krajowego porządku prawnego,

[1] Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE.

Trybunał Sprawiedliwości UE: dyrektywa retencyjna nie zapewniała dostatecznej ochrony danych osobowych obywateli UE przed nadużyciami

a które zobowiązują operatorów telekomunikacyjnych do zatrzymywania przez określony czas danych niezbędnych do:
- ustalenia źródła oraz odbiorcy połączenia,
- określenia daty, godziny i czasu trwania połączenia oraz jej rodzaju,
- określenia narzędzia komunikacji i
- identyfikacji lokalizacji urządzenia komunikacji ruchomej, w tym między innymi:
  - nazwiska i adresu abonenta lub zarejestrowanego użytkownika,
  - numeru nadawcy i odbiorcy połączenia, a także
  - adresu IP w przypadku usług internetowych,

do których danych mogą mieć dostęp właściwe organy krajowe.
W związku z rozpoznawanymi sprawami, irlandzki wysoki trybunał oraz austriacki trybunał konstytucyjny zwróciły się z pytaniami prejudycjalnymi do TS UE. Zmierzały one do dokonania przez Trybunał kontroli ważności dyrektywy 2006/24 w świetle postanowień Karty praw podstawowych UE.
W szczególności chodziło o prawa do poszanowania życia prywatnego i ochrony danych osobowych. Trybunał miał też rozważyć, czy dyrektywa ta pozwala na osiągnięcie celów, jakie zakłada, a ewentualna ingerencja w prawa podstawowe jest proporcjonalna.

Zdaniem Trybunału

Po rozważeniu przedstawionych wniosków Trybunał Sprawiedliwości UE stwierdził nieważność dyrektywy 2006/24. Takie rozstrzygnięcie było wynikiem przekonania, że jej przepisy ingerują w prawo do poszanowania życia prywatnego i ochrony danych osobowych (art. 7 oraz 8 Karty praw podstawowych EU).
Umożliwiają bowiem zebranie danych osobowych, których całokształt może dostarczyć bardzo precyzyjnych wskazówek dotyczących życia prywatnego osób, których dane są zatrzymywane.
Chodzi o takie informacje, jak:
- codzienne nawyki,
- miejsca stałego lub czasowego pobytu,
- codziennie lub okazyjnie pokonywane trasy,
- podejmowane czynności,
- relacje społeczne i środowiska społeczne, w których osoby te się obracają.

Obowiązek retencji tych danych przez operatorów powoduje jednocześnie, że przetwarzają oni dane osobowe. Dodatkową ingerencją w ocenie Trybunału jest także moż-

liwość uzyskania dostępu do tych danych przez właściwe organy krajowe.
Niemniej jednak, samo stwierdzenie ingerencji w prawa podstawowe nie przesądza jeszcze w ocenie Trybunału o ich naruszeniu, jeśli taka ingerencja jest proporcjonalna oraz konieczna i rzeczywiście odpowiada interesowi ogólnemu lub potrzebom ochrony praw i wolności innych osób.
Argumentem przemawiającym za ważnością dyrektywy stał się jej cel – zapewnienie dostępności danych dla dochodzenia, wykrywania i ścigania poważnych przestępstw. Jak stwierdził TS UE, retencjonowane dane są cennym narzędziem przy prowadzeniu czynności dochodzeniowo-śledczych.
Jednakże, w ocenie Trybunału Sprawiedliwości UE dyrektywa nie ustanawia minimalnych zabezpieczeń służących temu, aby osoby, których dane zostały zatrzymane, miały wystarczające gwarancje ich ochrony przed ryzykiem nadużyć oraz ich bezprawnym udostępnianiem i wykorzystywaniem.
Tym samym dyrektywa nie zawiera jasnych i precyzyjnych reguł określających zakres ingerencji w prawa podstawowe, gdyż w szczególności:

- obejmuje generalnie wszystkie jednostki, środki łączności elektronicznej i dane o ruchu – nie przewidziano w niej jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku – w rezultacie stosuje się ją nawet wobec tych osób, których komunikacja na gruncie przepisów prawa krajowego objęta jest tajemnicą zawodową,
- dyrektywa nie wymaga istnienia żadnego związku między danymi, które mają być zatrzymywane, a zagrożeniem dla bezpieczeństwa publicznego,
- nie określa żadnych materialnych i proceduralnych przesłanek, w przypadku zaistnienia których właściwe organy krajowe będą mogły uzyskać dostęp do danych i następnie je wykorzystać (odsyłając w tym zakresie do opracowania procedur w prawie krajowym, bez wskazywania choćby wytycznych w tym zakresie),
- nie przewiduje żadnego obiektywnego kryterium, które pozwoliłoby ograniczyć liczbę osób uprawnionych do uzyskiwania dostępu i późniejszego wykorzystywania zatrzymanych danych,
- nie wskazuje obiektywnych kryteriów, na podstawie których należy ustalić czas, na jaki dane te zostaną zatrzymane, aby zagwarantować, że będzie on ograniczał się do tego, co ściśle niezbędne (przewidując jedynie minimalny i maksymalny okres zatrzymania danych – od 6 do 24 miesięcy).

Stwierdzenie nieważności dyrektywy 2006/24 nie pociąga za sobą automatycznie nieważności krajowych ustaw, które ją implementują.
Dlatego też, obowiązujące przepisy art. 180a–180d prawa telekomunikacyjnego[1], które nakładają obowiązek retencji danych telekomunikacyjnych, obowiązują operatorów, a ich ewentualna zmiana zależy od decyzji ustawodawcy bądź stwierdzenia ich nieważności przez Trybunał Konstytucyjny.

Trybunał Sprawiedliwości UE: Operator wyszukiwarki internetowej jest administratorem danych osobowych

Wyrok TS UE z 13 maja 2014 r. (w sprawie C-131/12)

Stan faktyczny

W wydaniu drukowanym i elektronicznym jednej z hiszpańskich gazet ukazały się w 1998 roku dwa komunikaty dotyczące nieruchomości, której właścicielem był Mario Costeja Gonzalez.
Nieruchomość miała być zlicytowana ze względu na niespłacone należności wobec hiszpańskiego zakładu ubezpieczeń społecznych.
Po niemal 11 latach Gonzalez zauważył, że po wpisaniu jego imienia i nazwiska do wyszukiwarki Google na liście wyników znajdują się linki do tych komunikatów. W listopadzie 2009 roku zwrócił się więc do wydawcy gazety i zażądał usunięcia tych danych.
Twierdził, że postępowanie prowadzone wobec niego, a związane z zajęciem nieruchomości, zakończyło się przed wielu laty i informacje na ten temat nie są już aktualne. Wydawca odmówił żądaniu, powołując się na obowiązek publikacji ogłoszeń o licytacji wynikający z zarządzenia hiszpańskiego Ministerstwa Pracy i Polityki Społecznej.
Wobec tego, Gonzalez zwrócił się do Google Spain z wnioskiem, aby spółka usunęła z wyników wyszukiwania odesłania do przedmiotowych artykułów, pojawiające się po wpisaniu jego imienia i nazwiska. Żądanie to zostało przekazane do Google Inc. z siedzibą w Kalifornii (USA) – podmiotu świadczącego usługi wyszukiwania w Internecie.
Gonzalez złożył skargę do Agencia Española de Protección de Datos (hiszpański organ ds. ochrony danych, AEPD) zarówno przeciwko wydawcy gazety, jak i Google. Organ ten 30 listopada 2010 r. wydał decyzję, w której zobowiązał Google Spain oraz Google Inc. do usunięcia danych z indeksów wyszukiwania i zablokowania dostępu do nich w przyszłości.
Oddalił jednocześnie skargę wobec wydawcy gazety – stwierdził, że publikacja danych o licytacji nieruchomości była w tym przypadku prawnie uzasadniona. Odwołania od tej decyzji złożyły do Audiencia Nacional (sądu najwyższego Hiszpanii) zarówno Google Spain, jak i Google Inc. Sąd ten z kolei skierował do TS UE pytania prejudycjalne o możliwość zastosowania dyrektywy 95/46/WE[2] do

[1] Ustawa z 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2014 r. poz. 243).
[2] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

usługi świadczonej przez wyszukiwarkę internetową oraz możliwość żądania przez osobę, której dane dotyczą, usunięcia przez operatora wyszukiwarki z wyników wyszukiwania odesłań do tych danych, jeśli naruszają jej prawo do ochrony danych.

Zdaniem Trybunału

Istota i niezwykła waga omawianego orzeczenia TS UE przejawia się przede wszystkim w fakcie, że rozstrzyga ono szereg istniejących wątpliwości w zakresie świadczenia usługi wyszukiwarki internetowej na gruncie prawa ochrony danych osobowych.

Przede wszystkim Trybunał Sprawiedliwości Unii Europejskiej uznał działalność Google i innych wyszukiwarek internetowych, polegającą na:

- zlokalizowaniu informacji opublikowanych lub zamieszczonych w Internecie przez osoby trzecie,
- indeksowaniu ich w sposób automatyczny,
- czasowym przechowywaniu takich informacji i
- ich udostępnianiu internautom w sposób uporządkowany zgodnie z określonymi preferencjami,

w sytuacji, gdy takie informacje zawierają dane osobowe, za „przetwarzanie danych osobowych" w rozumieniu art. 2 lit. b dyrektywy 95/46/WE.

Operatora wyszukiwarki internetowej Trybunał uznał zaś za „administratora danych", który jest odpowiedzialny za ich przetwarzanie.

Podmiot taki bowiem, przeszukując Internet w zautomatyzowany, stały i systematyczny sposób w poszukiwaniu opublikowanych w nim informacji, dokonuje na danych czynności. W świetle dyrektywy 95/46/WE takie czynności, jak:

- gromadzenie,
- odzyskiwanie,
- zapisywanie i
- porządkowanie danych za pomocą oprogramowania indeksującego,
- przechowywanie ich na swych serwerach oraz, w odpowiednim przypadku,
- ujawnianie i udostępnianie ich użytkownikom w postaci listy wyników wyszukiwania,

należy uznać za przetwarzanie danych osobowch.

Skoro operator wyszukiwarki internetowej określa cele i sposób prowadzenia swojej działalności, to należy go uznać za administratora danych osobowych przetwarzanych w ten sposób.

Nie jest przy tym istotne, że operator nie sprawuje kontroli nad treścią publikacji zawierających dane osobowe na stronach internetowych, do których odsyła. Przetwarza bowiem dane osobowe w inny sposób i w innym zakresie niż wydawcy stron internetowych.

Ponadto, Trybunał Sprawiedliwości UE potwierdził, że do usług operatora wyszukiwarki internetowej, który jest podmiotem spoza UE i EOG, znajdzie zastosowanie dyrektywa 95/46/WE.

Chodzi o przypadki, kiedy przetwarzanie danych osobowych prowadzi spółka zależna na terytorium jednego z państw członkowskich, jeśli została powołana w celu promocji i sprzedaży powierzchni reklamowych przez wyszukiwarkę w tym państwie, by zapewnić rentowność

Trybunał Sprawiedliwości UE: użytkownik może zwrócić się bezpośrednio do operatora wyszukiwarki z prośbą o usunięcie linków do stron z informacjami o nim

oferowanej przez tę wyszukiwarkę usługi (w tym przypadku spółką taką jest Google Spain).

Według TS UE istnieje tu nierozerwalne powiązanie pomiędzy działalnością tych spółek – promocja i sprzedaż powierzchni reklamowych ma uczynić wyszukiwarkę internetową opłacalną gospodarczo, a wyszukiwarka z kolei umożliwia jednocześnie prowadzenie działalności promocyjnej.

Trybunał Sprawiedliwości UE orzekł, że użytkownicy wyszukiwarek mogą zwrócić się bezpośrednio do operatora wyszukiwarki z wnioskiem o usunięcie odesłań do witryn zawierających informacje naruszające ich prawa wynikające z dyrektywy.

Operator jest zobowiązany do usunięcia z wyświetlanej listy wyników wyszukiwania – mającego za punkt wyjścia imię i nazwisko danej osoby – linków do publikowanych przez osoby trzecie stron internetowych zawierających dotyczące tej osoby informacje, nawet gdy nie zostały one uprzednio lub jednocześnie usunięte z tych stron internetowych i nawet jeśli ich publikacja jest zgodna z prawem.

Ponadto, operator wyszukiwarki powinien także usunąć linki do zgłoszonych stron internetowych, jeśli osoba, której dane dotyczą, chce, aby zostały one „zapomniane", a przetwarzanie tych danych jest w obecnym stanie rzeczy niezgodne z dyrektywą.

Nawet jeśli początkowo dane osobowe przetwarzane były zgodnie z prawem, z powodu upływu czasu mogą zostać uznane za:

- niewłaściwe,
- niestosowne w obecnym stanie rzeczy czy też
- nadmierne w stosunku do celów, dla których są przetwarzane.

Tym samym, Trybunał przyznał prymat prawu do prywatności i ochrony danych osobowych wobec interesu gospodarczego operatora wyszukiwarki internetowej. Prawa te nie mają jednak charakteru absolutnego, co prowadzi do wniosku o konieczności konkretnej oceny przez operatora wyszukiwarki internetowej każdego zgłoszonego przypadku żądania usunięcia informacji.

W przypadku braku odpowiedniej reakcji tego administratora danych osoba, której dane dotyczą, może zwrócić się do organu nadzorczego lub sądowniczego o przeprowadzenie koniecznej kontroli i nakazanie mu przyjęcie konkretnych środków.

Podstawa prawna:

- wyrok TS UE z 17 października 2013 r. (w sprawie C-291/12),
- wyrok TS UE z 8 kwietnia 2014 r. (w sprawach połączonych C-293/12 i C-594/12),
- wyrok TS UE z 13 maja 2014 r. (w sprawie C-131/12).

Sprawdzenie i sprawozdanie w praktyce

Ustawa o ochronie danych osobowych nakłada na ABI obowiązek przeprowadzania sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania w tym zakresie sprawozdania. Podpowiadamy, jak w praktyce realizować ten obowiązek.

Zgodnie ze znowelizowaną ustawą o ochronie danych osobowych (dalej jako uodo) administratorzy bezpieczeństwa informacji mają obowiązek przeprowadzania sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Muszą też opracować sprawozdania w tym zakresie.

Obowiązek ten może przybrać dwie formy:

- stałe sprawdzanie, czy przetwarzanie danych osobowych w organizacji jest zgodne z prawem oraz
- dokonywanie sprawdzeń na polecenie GIODO.

W pierwszym przypadku ABI powinien stale monitorować procesy przetwarzania danych osobowych, pod kątem ich zgodności z przepisami o ochronie danych osobowych (częstotliwość przyjęta w planie sprawdzeń). W przypadku stwierdzonych nieprawidłowości powinien informować o tym administratora danych osobowych – wskazuje na to obowiązek przygotowania sprawozdania dla ADO, które ma być rezultatem takiego sprawdzenia[1].

Obowiązek sprawdzeń uszczegóławia rozporządzenie ministra administracji i cyfryzacji z 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. z 2015 r. poz. 745).

Druga możliwość została przewidziana w art. 19b ustawy o ochronie danych osobowych. Zgodnie z nim, GIODO może zwrócić się do administratora bezpieczeństwa informacji wpisanego do rejestru ABI o przeprowadzenie sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych u administratora danych, który ABI powołał. Generalny Inspektor wskazuje zakres i termin sprawdzenia.

MICHAŁ BIENIAS
aplikant radcowski przy Okręgowej Izbie Radców Prawnych w Warszawie, prawnik w Kancelarii Prawnej Traple, Konarski, Podrecki i Wspólnicy, absolwent studiów podyplomowych Zarządzanie Bezpieczeństwem Informacji w Szkole Głównej Handlowej

Nie wyklucza to skorzystania przez GIODO z własnych kompetencji kontrolnych. Jednak uwzględniając średnioroczną ilość kontroli przeprowadzanych przez GIODO (np. w 2013 roku GIODO przeprowadził ogółem 173 kontrole, natomiast w 2014 roku 175 kontroli, a do tej pory w 2015: 77 kontroli[2]), w większości przypadków taka kontrola przeprowadzona przez ABI powinna zakończyć czynności kontrolne w konkretnej sprawie[3].

Sprawozdanie z przeprowadzonego sprawdzenia ma być przedstawione GIODO. Jest on jednak nadal uprawniony do przeprowadzenia kontroli.

WAŻNE

Zgodnie z doktryną aktywność ABI w związku ze sprawdzeniem, sprowadzać się powinna do:

- ustalenia stanu faktycznego,
- porównania go ze stanem postulowanym (określonym przepisami o ochronie danych osobowych) i
- wyciągnięcia wniosków.

Oznacza to, że mamy tu do czynienia z typowym postępowaniem kontrolnym.

Uzasadniając propozycję wprowadzenia tego mechanizmu prawnego, wskazywano na potrzebę uproszczenia kontroli przestrzegania przepisów, wykonywanej na wniosek GIODO przez ABI. Miała ona zastąpić w tym zakresie kontrolę GIODO, a przez to „odciążyć" ADO[4].

Na posiedzeniu Komisji Nadzwyczajnej do spraw związanych z ograniczaniem biurokracji Generalny Inspektor Ochrony Danych Osobowych wyraźnie zauważył, że chce się pozbyć części obowiązków (tych, które mogą być wykonywa-

[1] P. Barta, P. Litwiński. Ochrona danych osobowych. Komentarz do art. 36a. Legalis.

[2] Statystyki dostępne pod adresem: http://www.giodo.gov.pl/541/id_art/4583/j/pl/. Ostatni dostęp: 6 września 2015 r.

[3] P. Barta, P. Litwiński, ibidem.

[4] Por. uzasadnienie projektu nowelizacji [w:] Projekt ustawy o ułatwieniu wykonywania działalności gospodarczej z projektami aktów wykonawczych z 4 lipca 2014 r., druk sejmowy nr 2606, s. 18 uzasadnienia załączonego do projektu, dostępny na: www.sejm.gov.pl.

ne przez ABI)[1]. GIODO dodał, że większość kontroli, które będą wykonywane u ADO, którzy powołali ABI, będzie przeprowadzonych przez samych administratorów bezpieczeństwa informacji.
Rozporządzenie przewiduje dwa podstawowe tryby przeprowadzania sprawdzeń:
- planowe (według planu sprawdzeń przygotowanego przez ABI) oraz
- doraźne (w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji pojawienia się informacji o naruszeniu ochrony danych lub uzasadnionego podejrzenia naruszenia, czyli w razie wystąpienia tzw. incydentu bezpieczeństwa).

Należy określić przedmiot sprawdzeń

Sprawdzenie rozpoczyna się od opracowania planu sprawdzeń. Określa on:
- przedmiot przeprowadzenia poszczególnych sprawdzeń (zbiory danych i systemy informatyczne, które są przedmiotem poszczególnych sprawdzeń),
- zakres przeprowadzenia poszczególnych sprawdzeń (np. przepisy, z którymi zostaną zweryfikowane zbiory danych i systemy informatyczne),
- termin przeprowadzenia poszczególnych sprawdzeń,
- sposób i zakres ich dokumentowania (§ 3 ust. 3 rozporządzenia).

UWAGA

W samym planie sprawdzeń warto określić, na jaki okres został on opracowany. Dodatkowo, w nagłówku należy oznaczyć administratora danych, którego dotyczy sprawdzenie, a także imię i nazwisko ABI.

Sprawdzenie nie musi obejmować wszystkich przetwarzanych zbiorów i systemów informatycznych służących do przetwarzania danych osobowych. ABI samodzielnie określa przedmiot sprawdzenia w planie sprawdzeń. Z pewnością dobrą praktyką jest sprawdzenie nowego zbioru danych (lub nowego systemu informatycznego).
Również organ ochrony danych osobowych zwraca szczególną uwagę na przetwarzanie tych danych osobowych przez administratorów danych, co może powodować kontrolę w tym zakresie. Sprawdzenie powinno być również wykonywane przed rozpoczęciem przetwarzania zbiorów danych zawierających dane osobowe wrażliwe, o których mowa w art. 27 ust. 1 uodo.
Wynika to ze znacznego stopnia ingerencji przetwarzania takich danych w prawa i wolności podmiotu danych[2]. Zbiory danych sensytywnych podlegają rejestracji w GIODO, więc będą także przedmiotem późniejszej weryfikacji GIODO podczas analizy zgłoszenia rejestracyjnego.

Jaki powinien być zakres sprawdzeń

Po określeniu przedmiotu sprawdzenia ABI powinien opisać zakres poszczególnych sprawdzeń, czyli np.:
- weryfikacja przetwarzania danych osobowych z zasadami, o których mowa w art. 23–27 i art. 31–35 uodo (np. zasadą adekwatności, zasadą merytorycznej poprawności danych);
- weryfikacja przetwarzania danych osobowych z zasadami dotyczącymi zabezpieczenia danych osobowych, o których mowa w art. 36, art. 37–39 ustawy oraz przepisach wydanych na podstawie art. 39a uodo;
- zasady udostępniania i powierzenia danych osobowych innym podmiotom;
- weryfikacja przetwarzania danych osobowych z zasadami przekazywania danych osobowych do państw trzecich;
- weryfikacja przetwarzania danych osobowych z obowiązkiem zgłoszenia zbioru danych do rejestracji i jego aktualizacji, jeżeli zbiór zawiera dane wrażliwe;
- weryfikacja dokumentacji przetwarzania danych (m.in. Polityka bezpieczeństwa, Instrukcja zarządzania systemem informatycznym);
- zasady postępowania w sytuacjach naruszenia ochrony danych osobowych;
- proces nadawania upoważnień do przetwarzania danych osobowych;
- realizacja praw osób, których dane są przetwarzane;
- zasady archiwizacji danych osobowych.

WAŻNE

Do ABI należy wybór, które z powyższych obowiązków z uodo sprawdzić w poszczególnych sprawdzeniach. ABI może opracować listę kontrolną z powyższymi punktami, która posłuży mu w przygotowaniu planów sprawdzeń w poszczególnych latach (i gdzie ABI będzie oznaczał, co zostało/co zostanie sprawdzone).

W planie sprawdzeń należy także określić sposób i zakres dokumentowania sprawdzeń (np. czy dane będą utrwalane na nośniku danych lub które osoby zostaną objęte przesłuchaniem, czy będą sporządzane kopie zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu).

Jak określić częstotliwość sprawdzeń

Plan sprawdzeń jest przygotowywany przez ABI na nie dłużej niż rok. Musi obejmować co najmniej jedno sprawdzenie. Oznacza to, że przepisy o planie sprawdzeń nakładają obowiązek, aby było ono przeprowadzane przynajmniej raz na rok, przy czym może obejmować część zbiorów danych i systemów informatycznych.

[1] Komisja Nadzwyczajna do spraw związanych z ograniczaniem biurokracji. Rozpatrzenie rządowego projektu ustawy o ułatwieniu wykonywania działalności gospodarczej (druk nr 2606) – kontynuacja, iTV Sejm – transmisje archiwalne godz.: 15:12. Transmisja dostępna pod adresem: http://www.sejm.gov.pl/Sejm7.nsf/transmisje_arch.xsp?unid=B0CD539B48815E1FC1257D56003F18C5 Ostatni dostęp: 6 września 2015 r.

[2] M. Byczkowski. Obowiązek sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Dodatek do MoP 2015, nr 6, str. 9.

Wszystkie zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych powinny być objęte sprawdzeniem co najmniej raz na pięć lat (§ 3 ust. 6 rozporządzenia).
Mając na uwadze ostatnie intensywne prace nad ogólnym rozporządzeniem o ochronie danych osobowych (rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych, osobowych i swobodnym przepływem takich danych dalej jako rodo), wydaje się, że wejdzie ono w życie w ciągu najbliższych 5 lat. W konsekwencji nie będzie takiego ABI, który będzie zobowiązany do dokonania sprawdzenia wszystkich zbiorów danych i systemów informatycznych w organizacji.

WAŻNE

Przepisy o planie sprawdzeń wymagają, aby było ono przeprowadzane przynajmniej raz na rok, przy czym może ono obejmować część zbiorów danych i systemów informatycznych.

Przygotowany plan sprawdzeń ABI przedstawia ADO nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem. Termin ten musi zostać dotrzymany, nawet jeśli w danej organizacji krótsze wyprzedzenie umożliwia zapoznanie się z planem oraz powiadomienie o nim osób w strukturze organizacji.
Sprawdzenie doraźne jest przeprowadzane niezwłocznie po tym, jak ABI dowie się o naruszeniu ochrony danych osobowych lub będzie miał uzasadnione podejrzenie takiego naruszenia. ABI musi powiadomić ADO o rozpoczęciu sprawdzenia doraźnego lub sprawdzenia w trybie, o którym mowa w art. 19b ust. 1 ustawy, przed podjęciem pierwszej czynności w toku sprawdzenia.
Sprawdzenie doraźne będzie miało przede wszystkim miejsce w razie wystąpienia incydentu bezpieczeństwa informacji. Incydentami takimi mogą być przypadki:
- ujawnienia danych niepowołanym osobom,
- naruszenia integralności danych wrażliwych (uszkodzenie, przekłamanie, zniszczenie),
- ataków nieautoryzowanego dostępu do aplikacji,
- kradzieży lub zniszczenie urządzeń przetwarzających lub/i przechowujących dane osobowe.

Jakie są etapy sprawdzeń

Czynności sprawdzeń ABI można podzielić na dwa etapy:
- inwentaryzacja zbiorów i zasobów danych osobowych;
- zastosowanie przepisów prawa do zidentyfikowanego stanu faktycznego (zbiorów i zasobów danych osobowych).

W pierwszym etapie ABI sporządza aktualny wykaz wszystkich rodzajów danych osobowych. Polega on na dokonaniu przeglądu rejestrów w plikach na dyskach lokalnych lub sieciowych (np. pliki Excel), archiwów dokumentów w postaci papierowej, wszelkich dokumentów w postaci papierowej (np. segregator z dokumentami zawierającymi CV kandydatów do pracy)[1].
W drugim etapie do przeprowadzonej inwentaryzacji (zbiorów danych) ABI stosuje przepisy obowiązującego prawa. Przykładowo weryfikuje, czy:
- zakres zidentyfikowanych danych pracowniczych nie jest zbyt szeroki (sprzeczny z zasadą legalności i adekwatności),
- zakres zbieranych danych marketingowych został prawidłowo uwzględniony w wykazie zbiorów danych,
- dane przetwarzane są w miejscach określonych w wykazie budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
- wszystkie osoby, które mają dostęp do danych zostały odpowiednio upoważnione (zostało podpisane stosowne upoważnienie).

Zawiadomienie o rozpoczęciu sprawdzenia

Co najmniej siedem dni przed podjęciem powyższych czynności (przed sprawdzeniem) ABI musi zawiadomić kierownika jednostki objętej sprawdzeniem o zakresie czynności (§ 5 ust. 2 rozporządzenia). W toku sprawdzenia może być konieczne objęcie nim również innych komórek organizacyjnych, których wcześniej nie przewidziano. Przy takim zapisie przepisu każda komórka organizacyjna niepowiadomiona może mieć prawo odmówić poddania się czynnościom sprawdzającym.
W związku z tym rekomendowane jest zawiadomienie wszystkich kierowników jednostek organizacyjnych, których działalność może być objęta sprawdzeniem (np. poprzez wysłanie wiadomości e-mail na określoną listę adresową). Rozporządzenie przewiduje trzy wyjątki od tego wymogu, w razie:
- sprawdzenia doraźnego, jeżeli jego niezwłoczne rozpoczęcie jest niezbędne do przywrócenia stanu zgodnego z prawem lub weryfikacji, czy doszło do naruszenia;
- sprawdzenia, o którego przeprowadzenie zwrócił się GIODO, jeżeli na zawiadomienie nie pozwala wyznaczony przez niego termin;
- jeżeli kierownik jednostki organizacyjnej posiada informacje, o których należało go poinformować.

Czynności prowadzone w toku sprawdzenia

W trakcie sprawdzenia ABI może korzystać z szerokiego wachlarza czynności. Może on:
- utrwalać dane z systemu informatycznego lub zabezpieczać dane osobowe na informatycznym nośniku lub je drukować,
- sporządzać notatki,
- przeprowadzać oględziny,
- odbierać wyjaśnienia,
- kopiować dokumenty, obrazy wyświetlone czy zapisy rejestrów systemu informatycznego lub zapisy konfiguracji technicznych środków zabezpieczeń tego systemu (§ 4 ust. 2).

Prawodawca posłużył się sformułowaniem „w szczególności" w odniesieniu do „utrwalania danych z systemu informatycznego służącego do przetwarzania lub zabez-

[1] M. Byczkowski, ibidem, str. 9.

pieczania danych osobowych na informatycznym nośniku danych lub dokonania wydruku tych danych". Nie ma natomiast tego sformułowania przed wyliczeniem pozostałych czynności.
Zamierzeniem ustawodawcy jest jednak, aby ABI mógł wybrać, które czynności przeprowadzi w toku sprawdzenia (w myśl § 4 ust. 1: „ABI dokumentuje czynności przeprowadzone w toku sprawdzenia, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania").
Katalog tych czynności należy więc uznać za otwarty. Rozporządzenie nie określa, czy ABI może dokumentować czynności w toku sprawdzenia jedynie w sposób określony w przygotowanym wcześniej planie sprawdzeń. Brak prawnego ograniczenia w tym zakresie oraz otwarty katalog czynności pozwala na dokonywanie czynności w toku sprawdzenia, które nie zostały wcześniej przewidziane w planie sprawdzeń.
Materiały ze sprawdzenia są sporządzane w postaci papierowej lub elektronicznej. W poprzednich wersjach projektu rozporządzenia pojawiał się wymóg pisemności poszczególnych dokumentów (wyjaśnień) czy obowiązek podpisywania notatek, ale został ostatecznie usunięty.
Przy sprawdzeniu systemu informatycznego służącego do przetwarzania lub zabezpieczenia danych ABI może korzystać z asysty osób upoważnionych do przetwarzania danych (w szczególności osoby zarządzającej systemem). Niezbędna będzie współpraca ABI z innymi zespołami, specjalistami (w szczególności z zakresu informatyki) przy przeprowadzaniu sprawdzeń.
Pracownicy (wszelkie osoby objęte sprawdzeniem), a nie tylko administrator danych, mają umożliwić przeprowadzenie czynności w toku sprawdzenia. Zgodnie z § 5 ust. 1 rozporządzenia osoba odpowiedzialna za przetwarzanie danych osobowych, której dotyczy sprawdzenie, bierze udział w sprawdzeniu lub umożliwia ABI przeprowadzenie czynności w toku sprawdzenia.

Przeprowadzenie analizy ryzyka

Niezależnie od wymogów wynikających z uodo, organizacje, które chcą zapewnić najwyższe standardy bezpieczeństwa informacji, wdrażają normę ISO 27001.

WAŻNE

W organizacjach, które wdrożyły system zarządzania bezpieczeństwem informacji zgodnie z Normą PN-ISO 27001, audyty zgodności przetwarzania danych osobowych są wykonywane w ramach funkcjonowania takiego systemu[1].

W pierwszym projekcie rozporządzenia wykonawczego do znowelizowanej ustawy o ochronie danych osobowych wprost odniesiono się do normy ISO 27001. Zapisano w nim, że: „wymagania dotyczące sprawdzeń oraz nadzoru nad dokumentacją przetwarzania danych określone w rozporządzeniu uważa się za spełnione, jeżeli administrator danych wdrożył system zarządzania bezpieczeństwem informacji z uwzględnieniem Polskiej Normy PN-ISO/IEC 27001, pod warunkiem że system ten obejmuje ochronę danych osobowych, a osobą wykonującą czynności w nim określone jest administrator bezpieczeństwa informacji" (§ 12 rozporządzenia).
Ostatecznie przepis ten został wykreślony z rozporządzenia, jednak szeroka praktyka wdrażania normy ISO 27001 w dużych organizacjach skłania do wykorzystania sposobów audytowania zgodności z normą ISO do sposobu dokonywania sprawdzeń.
Podczas wdrażania normy ISO 27001 organizacja przeprowadza także analizę ryzyka (*risk assessment*). Szczegółowe wytyczne i zalecenia dotyczące zarządzania ryzykiem w bezpieczeństwie informacji zostały przedstawione w normie ISO 27005.
Analiza ryzyka to proces wieloetapowy. Na początku należy opracować metodyki zarządzania ryzykiem. Dzięki stosowaniu jednolitych metodyk, wyniki szacowania ryzyka będą porównywalne na przestrzeni czasu.
Następnie organizacja powinna zidentyfikować ryzyka bezpieczeństwa informacji (przyczyny i sposoby materializacji ryzyka). Warto na tym etapie wskazać także podatności zwiększające ryzyka, np. brak szkoleń z ochrony danych osobowych czy też brak regularnego sprawdzania zabezpieczeń sprzętowych.
Po identyfikacji ryzyka powinna nastąpić estymacja ryzyka, czyli określenie prawdopodobnych skutków wystąpienia ryzyka (np. konieczność naprawy sprzętu i poniesienia związanych z tym kosztów). Ostatni etap to szacowanie ryzyk, czyli podzielenie ich na niskie, średnie i wysokie.
Proces analizy ryzyka kończy się planem postępowania z ryzykiem (RTP – „Risk Treatment Plan").
Drugim dokumentem, który powstaje na skutek dokonania analizy ryzyka, jest zakres stosowania (SOA – „Statement of Applicability").

PRZYKŁAD

„Statement of Applicability" zawiera wykaz zabezpieczeń z krótkim opisem ich wdrożenia. Przyporządkowuje występujące ryzyka do proponowanych zabezpieczeń, np.:

- ryzyko ujawnienia danych przez pracowników

Proponowane zabezpieczenia:

- prowadzenie szkoleń dla pracowników,
- wprowadzenie platformy e-learningowej z obowiązkiem szkoleniowym co najmniej raz na rok,
- ograniczenie dostępu do danych klientów dla praktykantów,
- blokowanie nośników USB, tzw. pendrive'ów itd.

Mając na uwadze powyższe wymagania normy ISO 27001, dobrą praktyką będzie przeprowadzenie przez ABI analizy ryzyka i przygotowanie SOA – „Statement of Applicability" (dokument przyporządkowujący występujące ryzyka do proponowanych zabezpieczeń).

Sprawozdanie po zakończonym sprawdzeniu

Z przeprowadzonego sprawdzenia ABI przekazuje administratorowi danych sprawozdanie w postaci elektronicz-

[1] M. Byczkowski, ibidem str. 8–9.

nej albo papierowej. W toku prac nad rozporządzeniem usunięto wymóg opatrzenia sprawozdania „bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu".
Przez postać elektroniczną rozumie się więc dowolną formę elektroniczną (zapisanie na urządzeniu, elektronicznym nośniku danych, w systemie informatycznym).
Sprawozdanie powinno zostać przekazane z zachowaniem odpowiednich terminów określonych w § 6 ust. 3.
Poszczególne elementy, które mają znaleźć się w sprawozdaniu, zostały szczegółowo wymienione w art. 36c uodo. Podczas obrad Komisji Nadzwyczajnej do spraw związanych z ograniczaniem biurokracji, GIODO zauważył, że przepis ten odpowiada dokładnie art. 16 uodo.
Reguluje on elementy, które powinny się znaleźć w protokole z czynności kontrolnych. Świadczy to także o roli, którą sprawuje ABI (wykonywanie zadań inspektorów GIODO). Sprawozdanie powinno zawierać następujące elementy w poszczególnych rubrykach:

- oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania,
- imię i nazwisko ABI,
- wykaz czynności podjętych przez ABI w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach (np. jakie oględziny przeprowadzono, które osoby zostały przesłuchane, jakie dane z systemu informatycznego zostały utrwalone);
- datę rozpoczęcia i zakończenia sprawdzenia,
- określenie przedmiotu i zakresu sprawdzenia,
- opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
- stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem,
- wyszczególnienie załączników stanowiących składową część sprawozdania (m.in. notatki z czynności, zapiski z wyjaśnień lub kopie sporządzonych dokumentów),
- podpis ABI, a w przypadku sprawozdania w postaci papierowej – dodatkowo parafy ABI na każdej stronie sprawozdania,
- datę i miejsce podpisania sprawozdania przez ABI.

Warto także umieścić w sprawozdaniu informacje o tym, czy sprawdzenie zostało wykonane dla administratora danych, czy dla GIODO w trybie art. 19b uodo oraz czy jest ono planowe, czy doraźne.

Sprawdzenie, gdy ABI nie został powołany

Jeżeli administrator danych nie powołał ABI, sam wykonuje jego obowiązki, z wyjątkiem obowiązku sporządzania sprawozdania. Na administratorze danych będzie także ciążył obowiązek przeprowadzenia sprawdzenia (poza sprawdzeniem na żądanie GIODO)[1].

WAŻNE

Zarząd spółki może wyznaczyć odpowiednie osoby do wykonywania zadań ABI, gdy nie zostanie on powołany (np. koordynatora ochrony danych osobowych). Zadaniem administratora danych będzie zatem właściwe określenie w dokumentacji ochrony danych osobowych, w jaki sposób wykonuje on zadania z art. 36a ust. 2 pkt 1 w razie niepowołania ABI.

Rozporządzenie stosuje się więc jedynie do ABI. Nie ma zastosowania w sytuacji niepowołania ABI i wykonywania jego obowiązków przez administratora danych na podstawie art. 36b ustawy. Wskazuje na to fakt, że w toku konsultacji nad rozporządzeniem usunięto § 15 (zgodnie z nim „do administratora danych, o którym mowa w art. 36b ustawy, stosuje się odpowiednio przepisy rozporządzenia…").
Administrator danych w dokumentacji ochrony danych osobowych (w polityce bezpieczeństwa lub innym przeznaczonym w tym celu dokumencie) określa:

- częstotliwość sprawdzeń,
- przedmiot sprawdzeń,
- istnienie planu sprawdzeń czy listy kontrolnej, a także
- czynności podejmowane w toku sprawdzenia.

W literaturze zauważono, że pomimo braku obowiązku opracowania sprawozdania (z przeprowadzonego sprawdzenia), to jednak nawet w przypadku braku osoby pełniącej taką funkcję sprawdzenie powinno kończyć się dokumentem podsumowującym. To administrator danych powinien w tym wypadku ustalić formę przedstawienia wyników sprawdzenia oraz zakres informacji, które powinny się znaleźć w takim podsumowaniu.
Zasadne wydaje się, aby w dokumencie podsumowującym został opisany zakres przeprowadzonych prac, informacje o przeprowadzonych wywiadach z osobami odpowiedzialnymi za dany proces przetwarzania danych osobowych czy uczestniczących w takich procesach oraz wnioski dotyczące zgodności przetwarzania danych osobowych z przepisami wraz z podaniem niezgodności oraz zaleceń ich wyeliminowania (informacje, które są umieszczane w sprawozdaniu)[2].
Podobnie jak wyniki audytów pod względem zgodności z normą ISO 27001 są zapisywane w formie udokumentowanej informacji i przedstawiane właściwym członkom kierownictwa, tak rezultat sprawdzenia zgodności przetwarzania danych z przepisami powinien być zapisany i przedstawiony wszystkim członkom zarządu.

Podstawa prawna:

- ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r. poz. 1182),
- rozporządzenie ministra administracji i cyfryzacji z 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. z 2015 r. poz. 745).

[1] P. Barta, P. Litwiński Ochrona danych osobowych. Komentarz do art. 36b. Legalis.
[2] Byczkowski M. ibidem str. 10.

Monitoring a przepisy o ochronie danych osobowych

Coraz częściej spotykamy się z przypadkami monitoringu wizyjnego. Na ulicy, w pracy czy nawet na sąsiedniej działce – wszędzie tam możemy natknąć się na kamery rejestrujące dźwięk i obraz z otoczenia. Czy używanie tego typu urządzeń zostało uregulowane w przepisach? Jakie obowiązki ciążą na podmiocie, który chce prowadzić wideorejestrację?

LESZEK SYTNIEWSKI
radca prawny, Traple Konarski Podrecki i Wspólnicy

W Ministerstwie Spraw Wewnętrznych trwają obecnie prace nad założeniami ustawy o monitoringu wizyjnym[1]. Jest to wynikiem wielu opinii, w tym ze strony GIODO, wskazujących na nieadekwatność obecnych przepisów do realiów nagrywania, przechowywania oraz wykorzystywania takiego typu nagrań. Już obecnie do monitoringu wizyjnego można zastosować pewne reżimy prawne.

Jak wskazała Grupa robocza ds. ochrony danych osobowych, ustanowiona na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, w Opinii 4/2007 w sprawie pojęcia danych osobowych[2]:

„Obrazy osób zarejestrowane przez system nadzoru wideo mogą stanowić dane osobowe, jeżeli można rozpoznać te osoby".

Jeśli więc na nagraniu utrwalone zostaną dane osobowe, do ich przetwarzania (przez co – zgodnie z ustawą – rozumie się jakiekolwiek operacje, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych) znajdzie zastosowanie ustawa o ochronie danych osobowych.

Czy to już dane?

Możliwość zarejestrowania danych osobowych na nagraniu jest potwierdzana w wielu rozstrzygnięciach wydanych przez GIODO. I tak np. w decyzji z 21 czerwca 2013 r. (sygn. DOLiS/DEC-674/13/39142, 39150) GIODO nie miał wątpliwości, że nagrania z monitoringu hotelowego, na których utrwalono wizerunek gości hotelowych, zawierały ich dane osobowe tych osób. Zarejestrowany materiał był na tyle wyraźny, że pozwalał na identyfikację poszczególnych jednostek, a nawet został użyty jako dowód w postępowaniu sądowym przez osobę, która ostatecznie weszła w posiadanie nagrań – co stało się bezpośrednią przyczyną podejrzenia zaistnienia nieprawidłowości w zabezpieczeniu danych z monitoringu.

Podobnie w decyzji z 9 maja 2014 r. (sygn. DIS/DEC-446/14/35683) GIODO uznał, że w sprawie doszło do przetwarzania „(…) danych osobowych utrwalonych przy użyciu elektronicznych urządzeń rejestrujących obraz i dźwięk, znajdujących się na terenie Urzędu Miasta (monitoring zewnętrzny i wewnętrzny budynków Urzędu i terenu przyległego)".

Decyzje te można porównać z rozstrzygnięciem z 27 marca 2013 r. (DOLiS/DEC-364/13/19780, 19781). GIODO stwierdził, że nagrania z monitoringu w urzędzie miasta nie zawierały danych osobowych. Organ przychylił się do wyjaśnień podanych przez stronę, która podała:

„(…) Jakość nagrania pozwala jedynie na rejestrację sylwetek o nieokreślonej tożsamości i ogranicza się do bieżącego podglądu obrazów rejestrowanej przestrzeni w celu reakcji na niepożądane zdarzenia, np. kradzież, akty wandalizmu. Monitoring nie rejestruje dźwięków. Nie jest powiązany także z ewidencją ruchu osobowego, której Urząd nie prowadzi. Nie tworzy tym samym w sposób systematyczny zapisów oglądanych obrazów. W związku z powyższym rejestrowanych obrazów nie można przypisać do konkretnej osoby, a ustalenie tożsamości konkretnej osoby wymagałoby nadmiernych nakładów kosztów czasu lub działań".

Danymi osobowymi, które mogą znaleźć się na nagraniu, są nie tylko wizerunki osób fizycznych,

[1] https://legislacja.rcl.gov.pl/projekt/200701/katalog/200707#200707.

[2] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pl.pdf.

ale wszelkie inne informacje, które nawet dopiero w powiązaniu z innymi posiadanymi przez administratora danych pozwalają na ich przypisanie do określonej osoby fizycznej. Potwierdził to Wojewódzki Sąd Administracyjny w Warszawie w wyroku z 9 kwietnia 2014 r. (sygn. II SA/Wa 211/13) dotyczącym nagrań będących w posiadaniu Straży Miejskiej. W rozstrzygnięciu czytamy:
„(…) Nie można też przyjąć, że numer rejestracyjny pojazdu nie może prowadzić do identyfikacji osoby, a zatem, że nie stanowi on danych osobowych w rozumieniu cytowanego art. 6 ustawy o ochronie danych osobowych. Straż Miejska (…) posiada bowiem prawo dostępu do danych, zawartych w Centralnej Ewidencji Pojazdów i Kierowców, ma więc możliwość ustalenia tożsamości właściciela pojazdu, posiadając numer rejestracyjny pojazdu, bez nadzwyczajnego wysiłku i nakładów".
Również w literaturze przyjmuje się, że do danych osobowych można zaliczyć także taką informację, którą można odnieść do określonej osoby fizycznej dopiero przy użyciu innych posiadanych informacji, przetwarzanych również w innym zbiorze danych[1].

Uważaj na sąsiada

Ze względu na powszechny dostęp do nowych rozwiązań technologicznych coraz więcej rozstrzygnięć dotyczy również przydomowych systemów monitoringu. Powstaje więc pytanie, czy rejestrowanie nagrań wyłącznie w celu zapewnienia bezpieczeństwa na własnej posesji „podpada" pod uregulowania uodo.
Kwestia ta została poruszona w decyzji GIODO z 22 maja 2012 r. (sygn. DOLiS/DEC–455/12/31693, 31694, 31696, 31697). Orzeczenie to dotyczyło przypadku monitoringu drogi wewnętrznej, na której ustanowiono służebność przejazdu i przechodu dla mieszkańców przylegających posesji. A zatem z jednej strony nagrania dotyczyły terenu, który był własnością ADO, z drugiej jednak mogły na nich znaleźć się również inne osoby korzystające zgodnie z prawem z przysługującej im możliwości.
Ostatecznie GIODO stwierdził, że dane osobowe zawarte w ocenianym materiale były przetwarzane „wyłącznie w celu osobistym i domowym, tj. w celu zapewnienia osobistego bezpieczeństwa i zabezpieczenia nieruchomości stanowiącej ich własność (…)". W konsekwencji, zdaniem GIODO, do takich nagrań w ogóle nie znajdują zastosowania przepisy ustawy o ochronie danych osobowych – ze względu na zwolnienie przewidziane w art. 3a ust. 1 pkt 1 ustawy.

UWAGA

Generalny Inspektor Ochrony Danych Osobowych nie rozstrzygał, czy zastosowanie monitoringu wizyjnego w takim miejscu nie będzie naruszać prawa do prywatności osób, które zgodnie z prawem mogły korzystać ze służebności – w tym zakresie organ odesłał jedynie do możliwości dochodzenia praw przed sądami powszechnymi (art. 23 i art. 24 Kodeksu cywilnego).

Kwestię naruszenia prywatności przez zamontowanie monitoringu wizyjnego na sąsiedniej działce rozważał też Sąd Apelacyjny w Krakowie w sprawie zakończonej wyrokiem z 28 maja 2014 r. (sygn. akt I ACa 184/14). Z jednej strony sąd jednoznacznie potwierdził uprawnienie do stosowania środków ochrony poprzez instalację monitoringu własnej nieruchomości.
Stwierdził, że jest to działanie zarówno w ramach porządku prawnego, jak i wykonywania praw podmiotowych. Jednakże z drugiej strony sąd wyraźnie podkreślił, że prawo do stosowania zabezpieczenia w postaci monitoringu może podlegać ograniczeniom – w szczególności ze względu na prawo do prywatności, w tym ochronę danych osobowych, przysługujące innym osobom.
Omawiana sprawa dotyczyła zamontowania czterech kamer monitoringu na budynku właściciela działki. O ile kamery rejestrujące wyłącznie jego teren nie były zagrożeniem dla prywatności innych osób, o tyle kamery, które mogły rejestrować również części działki sąsiadującej – już tak. Za dostateczne uzasadnienie dla prowadzenia takiego monitoringu sąd nie uznał faktu skonfliktowania obydwu sąsiadów.
Każda taka sytuacja powinna być jednak oceniana odrębnie. Trzeba ją analizować w szczególności w świetle przesłanek odpowiedzialności za naruszenie dóbr osobistych opisanych w art. 24 § 1 Kodeksu cywilnego oraz znajdującej się w nim przesłanki wyłączającej odpowiedzialność. Chodzi o brak bezprawności danego działania faktycznie ingerującego w dobra osobiste.
W literaturze podnosi się również, że zakłócenie korzystania z cudzej nieruchomości poprzez monitoring wizyjny na sąsiedniej posesji może potencjalnie powodować powstanie roszczenia negatoryjnego z art. 222 § 2 w zw. z art. 144 Kodeksu cywilnego[2].

Monitoring – obowiązki

Przetwarzanie danych osobowych w ramach monitoringu wizyjnego wiąże się z wieloma obowiązkami wskazanymi w ustawie o ochronie danych osobowych. Ich zakres jest różny w zależności od tego, czy podmiot przetwarzający dane dokonuje tego w charakterze procesora, czy też administratora danych.
Procesor danych przetwarza dane osobowe wyłącznie na zlecenie administratora danych, w zakresie i celu przewidzianym w umowie z administratorem (zob. art. 31 ust. 1 i 2 ustawy o ochronie danych osobowych). W przypadku braku innych uregulowań w umowie procesor jest odpowiedzialny wyłączne za należyte zabezpieczenie danych osobowych (art. 36, 37–39 oraz rozporządzenie wydane na podstawie art. 39a uodo).
W praktyce jednak najczęściej przetwarzanie danych osobowych w ramach monitoringu wizyjnego nie jest zlecane podmiotom trzecim. Realizuje je sam podmiot monitorujący. Jeśli decyduje on o celach i środkach przetwarzania – należy uznać go za ADO w rozumieniu art. 7 pkt 4 ustawy o ochronie danych osobowych.

[1] J. Barta, P. Fajgielski, R. Markiewicz, Ochrona danych osobowych. Komentarz – komentarz do art. 6, LEX 2011; źródło: LexPrestige.

[2] M. Wróblewski, Podstawy prawne funkcjonowania monitoringu wizyjnego w Polsce, Monitor Prawniczy, 8/2013; źródło: Legalis.

Administratora danych z nagrań z monitoringu wizyjnego najczęściej obciąża obowiązek:
- informacyjny (art. 24 ust. 1 ustawy o ochronie danych osobowych);
- dołożenia należytej staranności w przetwarzaniu danych (art. 26 ust. 1 ustawy);
- związany z zabezpieczeniem danych (art. 36–39 ustawy oraz rozporządzenie wydane na podstawie art. 39a ustawy);
- zgłoszenia zbioru danych do rejestracji (art. 40 ustawy).

Można również wspomnieć o „obowiązku" posiadania odpowiedniej podstawy prawnej dla przetwarzania danych (art. 23 ust. 1 lub art. 27 ust. 1 ustawy). Charakter tego wymogu jest jednak odmienny od wyżej wymienionych.
O ile niedopełnienie obowiązków wskazanych w punktach 1–4, powoduje trwanie stanu, który obliguje administratora do ich wykonania, o tyle brak odpowiedniej podstawy prawnej dla przetwarzania danych osobowych powoduje brak prawnej możliwości ich przetwarzania. Jak jednak się okazuje, niedopełnienie jakichkolwiek ustawowych obowiązków może wiązać się z istotnymi konsekwencjami.

Konsekwencje

Jednym z rozstrzygnięć dotyczących obowiązków ciążących na administratorze danych jest przywołana już wcześniej decyzja GIODO z 21 czerwca 2013 r. (sygn. DOLiS/DEC-674/13/39142, 39150). W tej sprawie administratorowi danych zarzucono liczne naruszenia związane z przetwarzaniem danych osobowych z monitoringu wizyjnego w hotelu.
Jednym z nich było niewypełnienie obowiązku informacyjnego z art. 24 ust. 1 ustawy wobec gościa hotelowego. Ponieważ jednak odpowiednie informacje zostały przekazane – co prawda ponad dwa lata po rozpoczęciu przetwarzania danych, ale przed wydaniem decyzji – GIODO stwierdził, że „(…) brak jest (…) stanu naruszenia, który uzasadniałby sformułowanie wobec Spółki nakazu dopełnienia wobec skarżącej obowiązku informacyjnego, o którym mowa w art. 24 ust. 1 ustawy".
Pozornie wydawałoby się więc, że niedopełnienie przez administratora danych ustawowych obowiązków nie wywoła dla niego negatywnych skutków, gdyż GIODO, wydając decyzję w konkretnej sprawie, uwzględnia stan faktyczny z chwili wydania rozstrzygnięcia.
Przeczy temu jednak dalsza część omawianej decyzji. W odniesieniu do innych obowiązków GIODO podkreślił bowiem, że spółka przekazała odpowiednią dokumentację dopiero po miesiącu od wezwania organu, a wcześniej wnosiła również o przedłużenie terminu na dokonanie tej czynności.
Zdaniem organu świadczyło to o wytworzeniu dokumentacji wyłącznie na potrzeby toczącego się postępowania. To samo zastrzeżenie dotyczyło zgłoszenia do rejestracji zbioru danych, co nastąpiło ponad dwa lata po rejestracji nagrań zainteresowanej osoby.
Okoliczności sprawy wskazywały też na wysokie prawdopodobieństwo nieuprawnionego udostępnienia danych osobowych podmiotom trzecim. Zdjęcia z monitoringu trafiły bowiem do męża skarżącej, który przedłożył je w trakcie toczącego się w innej sprawie postępowania sądowego.
W konsekwencji GIODO przekazał organom zawiadomienie o podejrzeniu popełnieniu przez ADO przestępstwa.

WAŻNE

Nienależyte zabezpieczenie przetwarzanych danych osobowych, niedopełnienie obowiązku rejestracji oraz nieuprawnione ich udostępnienie osobie trzeciej – podobnie jak zaniechanie dopełnienia obowiązku informacyjnego czy też przetwarzanie danych osobowych bez adekwatnej podstawy prawnej – podlegają sankcjom karnym (zob. art. 49–54 ustawy).

Pomimo że niedopełnienie przez administratora danych niektórych wymienionych w ustawie obowiązków (w przeciwieństwie do braku podstawy prawnej dla przetwarzania danych z art. 23 ust. 1 lub art. 27 ust. 2 ustawy) nie skutkuje prawną niemożliwością przetwarzania tych danych, to takie naruszenia (podobnie jak przetwarzanie danych osobowych bez podstawy prawnej) mogą rodzić dla ADO poważne konsekwencje.

Podsumowanie

Obecny rozwój i dostępność nowych technologii powodują, że coraz częściej spotykamy się z przypadkami monitoringu wizyjnego. Dotyczą one rejestracji realizowanej nie tylko w przestrzeni publicznej lub w pracy, lecz również na prywatnych posesjach.
Do nagrań zawierających informacje dotyczące możliwej do zidentyfikowania osoby fizycznej należy stosować ustawę o ochronie danych osobowych. Z taką sytuacją mamy do czynienia nie tylko w przypadku zarejestrowania wyraźnych wizerunków osób fizycznych, lecz również np. numerów rejestracyjnych pojazdów, jeśli administrator danych może z łatwością przypasować je do danej jednostki przy użyciu posiadanych przez siebie informacji, również znajdujących się w innych zbiorach.
Podmioty prowadzące rejestrację we własnych celach mogą zostać uznane za administratorów danych osobowych. W takim przypadku ciąży na nich, oprócz konieczności posiadania podstawy prawnej dla przetwarzania danych, wiele ustawowych obowiązków.
Ich realizacja może być potwierdzana w toku postępowania przed GIODO prowadzonego z udziałem administratora danych. Ich niedopełnienie może być jednak również ścigane na drodze karnej i to nawet w przypadku gdy administrator co prawda zadośćuczynił im, ale zrobił to z opóźnieniem.
Potwierdza to konieczność zachowania przez administratorów danych szczególnej ostrożności w przypadku przetwarzania danych osobowych, które mogą znaleźć się w nagraniach z monitoringu wizyjnego.

Podstawa prawna:
- ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r. poz. 1182, 1662),
- ustawa z 23 kwietnia 1964 r. – Kodeks cywilny (Dz.U. z 1964 r. nr 16, poz. 93).

Sprawdzenie prowadzone przez ABI na zlecenie GIODO

Nowelizacja ustawy o ochronie danych osobowych wprowadziła możliwość zwrócenia się GIODO do administratora bezpieczeństwa informacji z prośbą o przeprowadzenie sprawdzenia zgodności przetwarzania danych z przepisami. Jeśli ABI tego nie zrobi, Generalny Inspektor może wykreślić go z rejestru.

Ustawa z 7 listopada 2014 r. (Dz.U. z 2014 r. poz. 1162) o ułatwieniu wykonywania działalności gospodarczej, która weszła w życie 1 stycznia 2015 r., wprowadziła do ustawy z 29 sierpnia 1997 r. (tekst jedn.: Dz.U. z 2014 r. poz. 1182 ze zm., dalej jako uodo) nową instytucję. Wyposaża ona Generalnego Inspektora Ochrony Danych Osobowych w kompetencje w stosunku do administratora bezpieczeństwa informacji powoływanego przez administratora danych.

To uprawnienie polega na możliwości zwrócenia się do administratora bezpieczeństwa informacji o dokonanie sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Zostało ono uregulowane w art. 19b uodo, a także szczegółowo w rozporządzeniu ministra administracji i cyfryzacji z 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji.

DOMINIKA NOWAK
aplikantka radcowska przy Okręgowej Izbie Radców Prawnych w Krakowie, pracownik Zespołu Technologie Media Telekomunikacja w kancelarii Traple Konarski Podrecki i Wspólnicy, specjalizuje się w prawie nowych technologii, w szczególności w ochronie danych osobowych

Sprawdzenie i sprawozdanie dla Generalnego Inspektora

Artykuł 19b uodo, który ustanawia uprawnienie Generalnego Inspektora Ochrony Danych Osobowych do wezwania administratora bezpieczeństwa informacji do wykonania określonych czynności, brzmi:

„1. Generalny Inspektor może zwrócić się do administratora bezpieczeństwa informacji wpisanego do rejestru, o którym mowa w art. 46c, o dokonanie sprawdzenia, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, u administratora danych, który go powołał, wskazując zakres i termin sprawdzenia.

2. Po dokonaniu sprawdzenia, o którym mowa w art. 36a ust. 2 pkt 1 lit. a, administrator bezpieczeństwa informacji, za pośrednictwem administratora danych, przedstawia Generalnemu Inspektorowi sprawozdanie, o którym mowa w art. 36a ust. 2 pkt 1 lit. a.

3. Dokonanie przez administratora bezpieczeństwa informacji sprawdzenia w przypadku, o którym mowa w ust. 1, nie wyłącza prawa Generalnego Inspektora do przeprowadzenia kontroli, o której mowa w art. 12 pkt 1".

Zgodnie z cytowanym przepisem GIODO może zwrócić się do ABI wpisanego do ogólnokrajowego, jawnego rejestru administratorów bezpieczeństwa informacji, o dokonanie sprawdzenia u administratora danych, który go powołał.

W przypadku gdy ABI nie został jeszcze wpisany do rejestru, nie jest możliwe zwrócenie się do niego o wykonanie czynności w trybie art. 19b uodo. Taka sytuacja może się nawet zdarzyć, jeżeli administrator bezpieczeństwa informacji został już zgłoszony do rejestru w trybie art. 46b uodo.

Zakres sprawdzenia dla GIODO

Wezwanie do przeprowadzenia sprawdzenia musi zawierać termin i zakres czynności. Przedmiotem sprawdzenia może być sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. W zakresie żądanego sprawdzenia mogą znaleźć się między innymi następujące kwestie:

- zgodność przetwarzania danych osobowych z zasadami dotyczącymi podstaw prawnych, spełnienie obowiązków informacyjnych oraz zgodność z zasadami przetwarzania danych osobowych określonymi w art. 23–27 uodo zgodność z zasadami:
  - dotyczącymi zabezpieczenia danych osobowych określonymi w rozdziale piątym uodo,
  - przekazywania danych osobowych do państw trzecich określonymi w rozdziale siódmym uodo oraz

- wykonanie obowiązku zgłoszenia do rejestracji oraz aktualizacji zbioru danych, który zawiera tzw. dane wrażliwe, o których mowa w art. 27 ust. 1 uodo, wynikającym z art. 41 i 43 uodo.

Po zakończeniu sprawdzenia administrator bezpieczeństwa informacji przedstawia Generalnemu Inspektorowi Ochrony Danych Osobowych sprawozdanie ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Sprawozdanie jest przedstawianie przez ABI za pośrednictwem administratora danych.
Dokonanie tego sprawdzenia nie wyłącza prawa GIODO do przeprowadzenia kontroli w trybie art. 12 ust. 1 uodo, czyli na zasadach ogólnych. W praktyce przeprowadzenie kontroli przez administratora bezpieczeństwa informacji będzie zazwyczaj kończyć postępowanie.
Na taką ocenę pozwala liczba kontroli przeprowadzanych przez Generalnego Inspektora. Na przykład w 2013 roku odbyły się 173 kontrole[1].

ABI nie przeprowadzi sprawdzenia – konsekwencje

Sankcją za nieprzeprowadzenie sprawdzenia lub dokonanie go w innym zakresie lub terminie niż określony przez GIODO może być podstawą wykreślenia administratora bezpieczeństwa z urzędu z rejestru. Taki wniosek wynika z brzmienia art. 46d ust. 2 pkt 2 uodo, zgodnie z którym: „Generalny Inspektor z urzędu wydaje administratorowi danych decyzję o wykreśleniu administratora bezpieczeństwa informacji z rejestru administratorów bezpieczeństwa informacji, jeżeli (…) administrator bezpieczeństwa informacji nie wykonuje zadań określonych w art. 36a ust. 2".
Wśród zadań z art. 36a ust. 2 uodo można znaleźć m.in. obowiązek administratora bezpieczeństwa informacji zapewniania przestrzegania przepisów o ochronie danych osobowych poprzez sprawdzenie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania w tym zakresie sprawozdania dla administratora danych. Wykreślenie z rejestru następuje poprzez wydanie decyzji administracyjnej o wykreśleniu.

WAŻNE

W związku z krótkim obowiązywaniem nowelizacji trudno ocenić, czy w praktyce Generalny Inspektor Ochrony Danych Osobowych będzie w związku z niewykonaniem obowiązków z art. 19b uodo podejmował decyzję o wykreśleniu administratora bezpieczeństwa informacji z rejestru.

Skutkiem wykreślenia administratora bezpieczeństwa informacji z rejestru jest, zgodnie z art. 46d ust. 3 uodo, brak możliwości skorzystania przez ADO, do którego była skierowana decyzja, ze zwolnienia z obowiązku rejestracji zbiorów danych (43 ust. 1a uodo) niezawierających danych wrażliwych.

[1] P. Barta, P. Litwiński, Ustawa o ochronie danych osobowych. Komentarz. Warszawa 2015, wyd. 3, Komentarz do art. 19b.

Nowelizacją z 7 listopada 2015 r. ustawodawca z jednej strony rozszerzył zakres kompetencji i obowiązków administratora informacji. Z drugiej, zwolnił administratora danych z obowiązku rejestracji zbiorów niezawierających tzw. danych wrażliwych (art. 43 ust. 1a uodo), jeżeli zostanie powołany ABI na podstawie art. 36a.
Jednocześnie wyposażył Generalnego Inspektora w kompetencje pozwalające na ingerencję w działalność administratora danych. Chodzi o możliwości zlecenia ABI czynności kontrolnych.
Jednakże sprawne działanie na linii GIODO – ABI – ADO pozwoli już na etapie kontroli z trybie art. 19b uodo na ocenę zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
Pozwoli też na podjęcie działań zmierzających do usunięcia ewentualnych niezgodności, a w konsekwencji uniknięcie kontroli Generalnego Inspektora przeprowadzanej na zasadach ogólnych. W praktyce może ona w szerszym zakresie ingerować w funkcjonowanie działalności prowadzonej przez administratora danych.

Przygotowanie i przekazanie sprawozdania

Szczegółowe zasady sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania zostały uregulowane w rozporządzeniu ministra administracji i cyfryzacji z 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (dalej jako „rozporządzenie MAiC").
Sprawdzenia wykonywane dla Generalnego Inspektowa Ochrony Danych osobowych w trybie art. 19b ust. 1 uodo dokonywane są wyłącznie w wyniku zwrócenia się o to do administratora bezpieczeństwa informacji. Są one przeprowadzane poza planem sprawdzeń, o którym mowa w § 3 ust. 1 rozporządzenia MAiC. Zgodnie z § 3 ust. 8 tego rozporządzenia administrator bezpieczeństwa informacji zawiadamia administratora danych o rozpoczęciu sprawdzenia wykonywanego na wezwanie Generalnego Inspektora, przed podjęciem pierwszej czynności w toku sprawdzenia.
Zgodnie z § 6 rozporządzenia MAiC po zakończeniu sprawdzenia administrator bezpieczeństwa informacji przygotowuje sprawozdanie w postaci elektronicznej lub papierowej. Następnie administrator bezpieczeństwa informacji przekazuje administratorowi danych sprawozdanie, zachowując termin wskazany przez Generalnego Inspektora w wezwaniu w trybie art. 19b uodo.
Regulacja ta nawiązuje do art. 19b ust. 2 uodo. Zgodnie z nim sprawozdane jest przekazywane przez administratora bezpieczeństwa informacji, ale za pośrednictwem administratora danych. W praktyce oznacza to, że administrator bezpieczeństwa informacji nie może samodzielnie przekazać sprawozdania do organu zlecającego kontrolę.
Zgodnie z art. 36c uodo każde sprawozdanie ze sprawdzenia powinno zawierać następujące informacje:

1) oznaczenie ADO i adres jego siedziby lub miejsca zamieszkania;
2) imię i nazwisko ABI;
3) wykaz czynności podjętych przez administratora bezpieczeństwa informacji w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach;
4) datę rozpoczęcia i zakończenia sprawdzenia;
5) określenie przedmiotu i zakresu sprawdzenia;
6) opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
7) stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym sprawdzeniem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem;
8) wyszczególnienie załączników stanowiących składową część sprawozdania;
9) podpis ABI, a w przypadku sprawozdania w postaci papierowej – dodatkowo parafy ABI na każdej stronie sprawozdania;
10) datę i miejsce podpisania sprawozdania przez administratora bezpieczeństwa informacji.

Ogólne rozporządzenie o ochronie danych

Obecnie toczą się na szczeblu europejskim prace nad ogólnym rozporządzeniem Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (tzw. ogólne rozporządzenie o ochronie danych).
15 czerwca 2015 r. Rada wypracowała podejście ogólne względem ogólnego rozporządzenia o ochronie danych. Moja analiza będzie oparta na tekście opublikowanym w tym dniu.
W tekście projektu rozporządzenia w sekcji 4 została przewidziana instytucja inspektora ochrony danych (*data protection officer*), który jest odpowiednikiem istniejącego obecnie w polskim ustawodawstwie administratora bezpieczeństwa informacji.
Projekt rozporządzenia przewiduje uprawnienia organu nadzorczego względem inspektora ochrony danych osobowych. Nie są one jednak tak szczegółowe, jak w przypadku regulacji z art. 19b uodo. Zgodnie z art. 37 ust. 1 pkt g) projektu tzw. ogólnego rozporządzenia inspektor ochrony danych ma m.in. za zadanie:

- monitorowanie odpowiedzi na wnioski organu nadzorczego oraz – w ramach kompetencji inspektora ochrony danych
- współpracować z organem nadzorczym na jego żądanie lub z inicjatywy inspektora ochrony danych.

Innymi słowy inspektor ochrony danych będzie zobowiązany do współpracy z organem nadzorczym zarówno z jego inicjatywy jak i inspektora.
Projekt rozporządzenia nie przewiduje sankcji wobec inspektora ochrony danych za odmowę współpracy z organem nadzorczym. Natomiast niedokonanie czynności na wezwanie GIODO może spowodować wykreślenie ABI z rejestru na podstawie art. 46d ustawy o ochronie danych osobowych.

Regulacje w innych państwach członkowskich

Na gruncie ustawodawstwa państw członkowskich należących do Europejskiego Obszaru Gospodarczego oraz Unii Europejskiej nie jest powszechna praktyka przyznawania kompetencji uprawniających organy nadzoru do spraw ochrony danych osobowych, do zlecenia ABI lub jego odpowiednikom czynności kontrolnych u ADO.
Jako przykład podobnej regulacji należy wskazać przepisy zawarte w słowackiej ustawie nr 122/2013 o ochronie danych osobowych. Zgodnie z art. 27 ust. 2 tej ustawy inspektor ochrony danych jest zobowiązany do zapewnienia koniecznej współpracy z Urzędem w celu realizacji zadań wchodzących w jej zakres.
Na żądanie Urzędu inspektor ochrony danych jest zobowiązany złożyć natychmiastowo pisemne wyjaśnienia i zawiadomienia dotyczące zagrożeń naruszenia praw i wolności osób, których dane dotyczą, przed rozpoczęciem przetwarzania lub w jego trakcie.
Ta regulacja przypomina obowiązek wskazany w 19b uodo. W obydwu przypadkach ABI/inspektor ochrony danych wykonuje czynności na wezwanie organu nadzoru.
Ustawodawstwo litewskie nakłada na inspektora ochrony danych obowiązek powiadomienia organu nadzoru o naruszeniach przepisów przez ADO.
Zgodnie z art. 32 ust. 2 pkt 10 litewskiej ustawy o ochronie danych, inspektor ochrony danych jest zobowiązany powiadomić Państwowy Inspektorat Ochrony Danych na piśmie o tym, że ADO przetwarza dane, naruszając przepisy ustawy i inne przepisy regulujące ochronę danych oraz odmawia zaprzestania tych naruszeń.
Podobna instytucja została ustanowiona na gruncie ustawodawstwa szwedzkiego. Zgodnie z art. 38 szwedzkiej ustawy o ochronie danych osobowych, jeżeli przedstawiciel danych osobowych („*personal data representative*") ma powód, aby podejrzewać, że ADO narusza regulacje właściwe dla ochrony danych i jeżeli zaprzestanie naruszeń nie zostało wdrożone tak szybko, jak to w praktyce możliwe po wskazaniu naruszenia, jest zobowiązany powiadomić organ nadzorczy.
Na gruncie przepisów szwedzkich i litewskich odpowiednik ABI, mimo że jest powoływany przez ADO i ma zagwarantowaną niezależność w strukturze administratora danych, to w związku z nałożonymi na niego obowiązkami pełni funkcję quasi urzędnika państwowego. W tych przypadkach inspektor ochrony danych jest zobowiązany do poinformowania organu nadzoru o naruszeniach nie tylko na wezwanie, lecz również z własnej inicjatywy.

Podstawa prawna:

- ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r. poz. 1182),
- rozporządzenie ministra administracji i cyfryzacji z 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. z 2015 r. poz. 745).

ABI u przetwarzającego (procesora)

Administratora bezpieczeństwa informacji (ABI) może powołać także podmiot, któremu administrator danych powierzył przetwarzanie danych osobowych (przetwarzający). Wówczas zaistnieją jednak różnice w wykonywaniu przez ABI obowiązków w stosunku do tego powołanego przez administratora danych.

Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (uodo)[1] wprowadza dychotomiczny podział podmiotów – adresatów – obowiązków ochrony danych osobowych na:

- administratora danych oraz
- podmiot, któremu tenże administrator powierzył przetwarzanie danych osobowych (przetwarzający, procesor).

Dla działalności ABI to o tyle ważny podział, że przepisy o ochronie danych osobowych bezpośrednio określają jedynie stosunki administrator danych – ABI. Dopiero w wyniku rekonstrukcji można je odnieść do przetwarzającego.

DR GRZEGORZ SIBIGA
adwokat w Kancelarii Prawnej Traple, Konarski, Podrecki i Wspólnicy, kierownik Zakładu Prawa Administracyjnego w Instytucie Nauk Prawnych PAN w Warszawie

Powołanie ABI u procesora

Jasne jest, że samo powołanie i funkcjonowanie ABI u przetwarzającego jest dopuszczalne. Stosują się bowiem do niego przepisy z rozdziału 5 uodo dotyczące ABI, ze względu na odesłanie zawarte w art. 31 ust. 1 zd. pierwsze uodo.

Określony w tym przepisie obowiązek przetwarzającego podjęcia środków zabezpieczających zbiór danych, o których mowa w art. 36–39 uodo, będzie się również odnosił do obligatoryjnego zadania zapewniania przestrzegania przepisów o ochronie danych osobowych. Może być ono wykonywane przez powołanego ABI (art. 36a ust. 2 pkt 1 uodo) albo przez ADO działającego bez ABI (art. 36b uodo).

W zakresie przestrzegania tych przepisów (art. 36–39 uodo) przepis art. 31 ust. 3 zd. drugie uodo wyraźnie stanowi, że przetwarzający odpowiada jak administrator danych.

Należy jednak pamiętać, że ABI jest powoływany dla realizacji zadań związanych z ochroną wszystkich danych osobowych przetwarzanych w jednostce organizacyjnej (np. przedsiębiorstwie).

W praktyce oznacza to, że biorąc pod uwagę całość zasobów danych osobowych, nawet jeżeli podmiot jest przetwarzającym w stosunku do powierzonych danych osobowych, to najczęściej będzie jednocześnie administratorem danych względem innych danych osobowych, w przypadku których spełniony jest warunek decydowania o celach i środkach przetwarzania (np. danych pracowników).

To istotny podział, ponieważ w zależności od statusu podmiotu wobec określonych danych osobowych (administrator danych lub przetwarzający), wystąpią odmienności w zakresie zadań powołanego ABI, ale również w sytuacji prawnej samego przetwarzającego.

Powołanie i zgłoszenie ABI

Dobrowolność powołania ABI przez ADO (art. 36a ust. 1 uodo) z pewnością odnosi się także do przetwarzającego, a to właśnie ze względu na wspomniane już odesłanie zawarte w art. art. 31 ust. 1 zd. pierwsze uodo.

Jednak trzeba zwrócić uwagę, że już obowiązek zgłoszenia do GIODO powołania ABI został nałożony jedynie na administratora danych (art. 46b ust. 1 uodo). W tym miejscu należy jednak ponownie zauważyć, że działalność ABI odnosi się do wszystkich danych osobowych przetwarzanych w jednostce.

Jeśli podmiot będący przetwarzającym równocześnie względem innych danych osobowych ma status administratora danych, to oczywiście obowiązek zgłoszeniowy występuje.

WAŻNE

Do zaistnienia obowiązku zgłoszeniowego wystarczy przetwarzanie jakichkolwiek danych osobowych, w stosunku do których podmiot powołujący ABI jest administratorem danych.

Biorąc pod uwagę różnorodność danych osobowych przetwarzanych w jednostce organiza-

[1] Dz.U. z 2014 r. poz. 1182 ze zm.

GIODO nie może wezwać ABI do przeprowadzenia sprawdzenia u przetwarzającego

cyjnej, w dalszej części opracowania pod pojęciem „ABI u przetwarzającego" będę więc rozumiał sytuację, w której podmiot powołujący ABI w stosunku do określonych danych osobowych spełnia warunki przewidziane dla powierzenia danych osobowych w art. 31 ustawy o ochronie danych osobowych.

Zadania ABI

Ustawa o ochronie danych osobowych nakłada na administratora bezpieczeństwa informacji dwa zadania:

- zapewniania przestrzegania przepisów o ochronie danych osobowych oraz
- prowadzenia rejestru zbiorów danych przetwarzanych przez administratora danych, z wyjątkiem zbiorów zwolnionych z obowiązku rejestracyjnego (art. 36a ust. 2 uodo).

Drugie z tych zadań w ogóle nie jest przewidziane dla administratora bezpieczeństwa informacji u przetwarzającego. Przypomnę, że to zadanie ABI jest związane ze zwolnieniem administratora danych z obowiązków rejestracyjnych zbiorów danych wobec Generalnego Inspektora Ochrony Danych Osobowych na podstawie art. 43 ust. 1a ustawy o ochronie danych osobowych.

W zamian za to ABI prowadzi swój „wewnętrzny rejestr". Odpowiada on zakresem (co do zbiorów danych oraz informacji o zbiorach danych) ogólnokrajowemu rejestrowi prowadzonemu przez organ ds. ochrony danych osobowych (GIODO).

Ponieważ przetwarzający nie jest objęty obowiązkami rejestracyjnymi, to powołany przez niego ABI nie musi, w zakresie powierzonych zbiorów danych, prowadzić swojego rejestru, co zresztą jednoznacznie przesądza treść art. 36a ust. 2 pkt 2 uodo.

Zadanie zapewniania przestrzegania przepisów o ochronie danych osobowych spoczywa na administratorze bezpieczeństwa informacji, niezależnie od tego, czy powołał go administrator danych osobowych czy też przetwarzający. Zadanie to ABI wykonuje przede wszystkim poprzez przeprowadzanie sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania.

Zauważyć jednak trzeba, że inny będzie zakres merytoryczny sprawdzeń ABI u przetwarzającego, w porównaniu do sprawdzeń u administratora danych. Sprawdzać można bowiem wykonanie tylko tych obowiązków określonych w przepisach o ochronie danych osobowych, które spoczywają na weryfikowanym podmiocie.

W związku z tym w działalności przetwarzającego, sprawdzeniu będą podlegały wyłącznie obowiązki na niego nałożone, a już nie – obowiązki przewidziane dla administratora danych, który powierzył mu przetwarzanie danych osobowych.

Oznacza to, że administrator bezpieczeństwa informacji u przetwarzającego będzie weryfikował jedynie przestrzeganie ustawowych przepisów dotyczących zabezpieczenia technicznego i organizacyjnego (art. 36–39 uodo) i spełnienie wymagań ustalonych w tym względzie w przepisach wykonawczych wydanych na podstawie art. 39a uodo[1].

ABI będzie też weryfikował dopełnienie ustawowych warunków powierzenia przetwarzania danych osobowych, w tym przetwarzania danych osobowych zgodnie z warunkami określonymi w umowie z administratorem danych (art. 31 ust. 1–2 uodo). Adresatem innych obowiązków wyznaczonych przepisami uodo jest bowiem administrator danych.

Kompetencje GIODO wobec ABI

Uprawnienia GIODO do wezwania ABI do przeprowadzenia sprawdzenia i sporządzenia sprawozdania zostały określone w art. 19b uodo.

Jednak w ustawie określono dodatkowe warunki korzystania z powyższej kompetencji.

Po pierwsze, adresatem wezwania GIODO może być jedynie ABI wpisany do ogólnokrajowego rejestru zbioru danych osobowych, a zatem ABI, który po powołaniu i zgłoszeniu tej czynności do GIODO został zarejestrowany przez organ ds. ochrony danych osobowych.

Po drugie, wezwanie może dotyczyć jedynie sprawdzenia u administratora danych, który powołał ABI. Natomiast sprawdzenie u przetwarzającego nie zostało przewidziane w tym przepisie.

Powstaje zatem pytanie, czy GIODO może również zażądać od ABI dokonania sprawdzenia u przetwarzającego, który go powołał. Przepis art. 31 ust. 5 uodo wskazuje, jakie władcze kompetencje przysługują Generalnemu Inspektorowi w stosunku do przetwarzającego. W zakresie kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych nakazuje on jedynie odpowiednie stosowanie art. 14–19 uodo.

W tym odesłaniu nie uwzględnia się więc przepisu art. 19b uodo, który co prawda dotyczy stosunku Generalnego Inspektora z ABI, ale ma konsekwencje dla sytuacji podmiotu podlegającego sprawdzeniu ABI.

Kompetencji władczych organów administracji publicznej nie wolno domniemywać. W tym kontekście treść przepisów art. 19b ust. 1 i art. 31 ust. 5 uodo świadczy o tym, że GIODO nie może wzywać ABI do przeprowadzenia sprawdzenia u przetwarzającego.

Chociaż trzeba przyznać, że bardziej wydaje się to wynikiem niedopatrzenia legislacyjnego, niż celowego ograniczenia uprawnień organu ds. ochrony danych osobowych, czyli Generalnego Inspektora Ochrony Danych Osobowych.

[1] Wykonanie delegacji zawartej w art. 39a uodo stanowi rozporządzenie 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 (Dz.U. nr 100, poz. 1024).

Udostępnianie danych a powierzanie na zlecenie ADO

W związku z rosnącym znaczeniem w obrocie gospodarczym usług outsourcingowych, odróżnienie udostępniania danych osobowych przez ADO od ich powierzania do przetwarzania, ma bardzo istotne znacznie praktyczne dla podmiotów przetwarzających dane. Odmienne są zarówno podstawy prawne legalizujące przekazanie danych w obu tych przypadkach, jak i zasady postępowania z danymi przez podmioty, które je otrzymują.

Faktyczne przekazanie danych podmiotowi trzeciemu przez ADO lub umożliwienie zapoznania się temu podmiotowi z danymi w inny sposób, może być udostępnieniem danych, bądź ich powierzeniem do przetwarzania. Podstawą pozwalającą na odróżnienie tych sytuacji jest w szczególności rola podmiotu otrzymującego dane w procesie ich przetwarzania.

Kategorie podmiotów

Prawo ochrony danych osobowych wyróżnia w tym kontekście dwie kategorie podmiotów przetwarzających. Jest to administrator danych (ADO) oraz podmiot przetwarzający dane na jego zlecenie (w nauce prawa określany jako procesor).

Przepisy ustawy o ochronie danych osobowych (uodo) nie wprowadzają legalnej definicji pojęcia udostępniania danych. Zgodnie z art. 7 pkt 2 udostępnianie jest za jedną z form przetwarzania danych (obok takich operacji, jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie czy usuwanie danych).

W doktrynie prawa wskazuje się jednak, że do udostępnienia danych będzie dochodziło wyłącznie w przypadku, gdy odbiorcą danych jest inny administrator danych w rozumieniu art. 7 pkt 4 uodo[1]. Natomiast w przypadku gdy faktyczne przekazanie danych następuje pomiędzy ADO a podmiotem przetwarzającym dane na jego zlecenie, takie działanie powinno zostać uznane za przekazanie danych w związku z ich powierzeniem do przetwarzania (w rozumieniu art. 31).

W tym ostatnim przypadku odbiorcą danych nie będzie więc odrębny ADO, ale podmiot przetwarzający dane na zlecenie administratora powierzającego dane (procesor).

PAWEŁ TOBICZYK
aplikant adwokacki, doktorant w Katedrze Prawa Własności Intelektualnej Uniwersytetu Jagiellońskiego, pracownik Departamentu Technologie Media Telekomunikacja w Kancelarii Prawnej Traple Konarski Podrecki i Wspólnicy

W każdym przypadku, gdy ADO zamierza przekazać dane osobowe innej osobie lub podmiotowi, musi więc rozstrzygnąć, czy odbiorcą będzie odrębny administrator danych czy też procesor. Będzie to bowiem miało wpływ, na podstawę prawną, która legalizuje działanie administratora w obu tych przypadkach, w szczególności w kontekście rozstrzygnięcia, czy konieczne jest zawarcie umowy, o której mowa w art. 31 uodo.

Kto jest administratorem

Pojęcie administratora danych zostało zdefiniowane w art. 7 pkt 4 uodo. Zgodnie z nim ADO to organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3 uodo, decydująca o celach i środkach przetwarzania danych.

W definicji wskazano więc dwa konstytutywne elementy tego pojęcia, tj. decydowanie o celach przetwarzania danych oraz decydowanie o środkach przetwarzania danych[2]. Z literalnego brzmienia art. 7 pkt 4 uodo wynika więc, że każdy podmiot, który objęty został zakresem podmiotowym ustawy, może zostać uznany za ADO.

Warunkiem jest by podmiot ten jednocześnie decydował o celach i środkach przetwarzania danych. Przez decydowanie o „celach i środkach przetwarzania" danych należy przy tym rozumieć decydowanie o tym, „dlaczego i jak dane mają być przetwarzane". Obecnie proces przetwarzania danych przez podmioty zarówno z sektora prywatnego, jak i publicznego jest coraz bardziej złożony, w szczególności w kontekście organizacyjnym i technicznym. Zdarza się, że ADO nie będzie mógł decydować o wszystkich szczegółach technicznych oraz organizacyjnych przetwarzania danych, mimo że określa on cele ich wykorzystania.

[1] P. Litwiński, Obrót prawny bazami danych osobowych, PPH 2003, Nr 9, s. 49

[2] P. Barta, P. Litwiński, Ustawa o ochronie danych osobowych. Komentarz., komentarz do art. 7, Warszawa 2015, Legalis.

Przykładem sytuacji, gdy ADO nie decyduje o wszystkich szczegółach technicznych i organizacyjnych, może być przetwarzanie danych w ramach tzw. rozwiązań chmurowych. W modelu tym dostawca usługi ma bardzo daleką posuniętą autonomię, np. samodzielnie określa środki zabezpieczenia danych. To dostawca usługi chmurowej, a nie administrator danych decyduje więc zasadniczo o tym, „jak przetwarzać dane".

W takim przypadku, w oparciu o literalne brzmienie przepisów, nie byłoby możliwe jednoznaczne przesądzenie, który z podmiotów jest administratorem w stosunku do przetwarzanych danych.

Stanowisko Grupy Roboczej

Przy rozwiązaniu powyższych wątpliwości pomocne mogą być wytyczne Grupy Roboczej art. 29 zawarte w Opinii nr 1/2010[1]. Dotyczy ona rozumienia pojęć „administrator danych" oraz „przetwarzający" (*processor*) na gruncie dyrektywy nr 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych[2].

W opinii wskazano: „Określanie „sposobów" obejmuje zatem zarówno kwestie techniczne i organizacyjne, gdy podejmowanie decyzji można przekazać przetwarzającym (np. „z jakiego sprzętu komputerowego i oprogramowania korzystać?"), jak i zasadnicze elementy, które w tradycyjny i nieodłączny sposób określa administrator danych, takie jak „które dane się przetwarza?", „jak długo się je przetwarza?", „kto ma do nich dostęp?" itd.".

Widać tu wyraźny podział „środków przetwarzania danych" na środki organizacyjne i techniczne oraz tzw. zasadnicze elementy, w ramach których określa się, które dane i jak długo mają być przetwarzane, kto powinien mieć do nich dostęp, itp.

Grupa Robocza art. 29 stwierdziła też, że z punktu widzenia kwalifikacji danego podmiotu danych jako ADO, wystarczające jest ustalenie, że decyduje on o „zasadniczych elementach", nie jest natomiast bezwzględnie konieczne, aby określał również środki techniczne i organizacyjne[3].

Decyzje w tym ostatnim przedmiocie może podejmować więc również procesor. Oznacza to, że uprawniony jest wniosek, że dostawca chmury nie będzie co do zasady administratorem w stosunku do danych, które przetwarza w celu wykonania usługi.

ADO kontroluje przetwarzanie

Dla oceny, czy konkretny podmiot jest administratorem danych nie ma znaczenia, czy jest on faktycznym posiadaczem danych. Kryterium odróżniającym ADO od innych podmiotów przetwarzających dane (w szczególności procesora) jest sprawowanie faktycznej kontroli nad przetwarzaniem danych, rozumiane jako decydowanie o celach i środkach przetwarzania, a nie ich faktyczne przetwarzanie, które może zostać powierzone innemu podmiotowi[4].

Jeżeli podmiot będzie decydował o celach i środkach przetwarzania danych oraz będzie miał realną kontrolę nad ich przetwarzaniem, to będzie w odniesieniu do tych danych administratorem w rozumieniu uodo. Będzie tak nawet w przypadku, gdy nie będzie miał fizycznej styczności z danymi, od etapu ich zebrania, aż do ewentualnego usunięcia.

Możliwość powierzenia danych osobowych procesorowi wynika z art. 31 uodo. Zgodnie z nim ADO może powierzyć innemu podmiotowi wykonywanie czynności związanych z przetwarzaniem danych osobowych. Polskie prawo ochrony danych osobowych nie zawiera definicji procesora danych. Definicja „przetwarzającego" znajduje się w art. 2 pkt e) Dyrektywy 95/46/WE.

Zgodnie z nim przetwarzającym jest:

- osoba fizyczna lub prawna,
- władza publiczna,
- agencja lub
- inny organ przetwarzający dane osobowe w imieniu administratora danych.

Grupa Robocza art. 29 w Opinii nr 1/2010 wskazuje, że podmiot może być przetwarzającym, jeżeli spełnia dwa podstawowe warunki. Po pierwsze, jest odrębną osobą prawną w stosunku do ADO. Po drugie, przetwarza dane osobowe w jego imieniu.

Kluczowy w tym zakresie wydaje się zwrot „w imieniu administratora". Należy go rozumieć jako działanie w interesie innego podmiotu, czy też realizowanie jego celów. Grupa Robocza art. 29 Dyrektywy 95/46/WE wskazuje też, że podmiot przetwarzający działa pod zwierzchnictwem administratora danych.

Podstawy prawne

Udostępnienie jest jedną z form przetwarzania danych osobowych (o czym przesądza brzmienie art. 7 pkt 2 uodo). W związku z tym może zasadniczo przebiegać w oparciu o dowolną spośród podstaw prawnych przetwarzania danych wymienionych w art. 23 ust. 1 (dane zwykłe) i 27 ust. 2 uodo (dane wrażliwe).

Przepisy ustawy nie przewidują więc szczególnego trybu udostępniania danych. Wyjątkiem jest podstawa udostępniania na rzecz podmiotu z sektora publicznego.

W doktrynie prawnej przyjmuje się bowiem, że podstawą takiego udostępnienia może być wyłącznie przepis prawa, tj. art. 23 ust. 1 pkt 2 uodo lub art. 27 ust. 2 pkt 2 uodo[5].

Praktyczne problemy w kontekście oceny zgodności z prawem udostępniania danych dotyczą w szczególności sytuacji, gdy podstawą legalizującą udostępnianie danych „zwykłych" jest tzw. prawnie usprawiedliwiony cel administratora danych (art. 23 ust. 1 pkt 5).

W doktrynie istnieją rozbieżności poglądów dotyczące tego, który z administratorów danych (udostępniający czy odbierający dane) powinien legitymować się podstawą prawną dla ich udostępnienia. Istnieją w tym zakresie różne poglądy.

[1] Dz. Urz. WE L 281/31, z 23 listopada1995 r.; dalej jako „dyrektywa 95/46/WE".

[2] Opinia nr 1/2010 Grupy Roboczej z 16 lutego 2010 r. w sprawie pojęć „administrator danych" i „przetwarzający", WP 169.

[3] Tamże, s.13.

[4] G. Sibiga, Postępowanie w sprawach ochrony danych osobowych, Warszawa 2003, s. 54.

[5] P. Barta, P. Litwiński, Ustawa…, jw., komentarz do art. 23 uodo; J. Barta, P. Fajgielski, R. Markiewicz, Ochrona danych osobowych. Komentarz, Kraków 2004, s. 598.

Interesy stron

Pierwszy pogląd w kwestii legitymowania się podstawą prawną udostępniania danych stanowi, że zarówno administrator udostępniający, jak i administrator odbierający dane musi wykazać podstawę prawną ich przetwarzania w tym zakresie[1].
Autorzy uzasadniają to stanowisko wskazując, że skoro czynnością przetwarzania danych jest ich udostępnienie (przekazanie), a także ich zbieranie przez odbiorcę danych, zarówno jedna, jak i druga czynność powinny odbywać się w oparciu o odpowiednią podstawę prawną.
Zatem administrator udostępniający dane osobowe musi legitymować się podstawą prawną dla udostępnienia danych, a administrator zbierający w ten sposób dane musi dysponować podstawą prawną pozwalającą mu na przetwarzanie otrzymanych danych.
Drugie stanowisko opiera się na przekonaniu, że w przypadku udostępniania danych stwierdzenie istnienia usprawiedliwionych celów powinno dotyczyć administratora udostępniającego lub podmiotu, który je st zainteresowany otrzymaniem danych, tj. któremu są one przekazywane[2].
Użycie przez ustawodawcę spójnika „lub" powoduje więc, że wystarczające jest istnienie usprawiedliwionego interesu tylko po jednej stronie, tj. udostępniającego administratora danych albo odbiorcy danych. Biorąc pod uwagę literalne brzmienie przepisu, pogląd ten wydaje się trafny.

Cel udostępnienia

W kontekście udostępniania danych istotne znaczenie odgrywa również określona w art. 26 ust. 2 uodo zasada celowości przetwarzania danych. Oznacza ona, że dane powinny być zbierane dla oznaczonych, zgodnych z prawem celów, nie powinny być też poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.
Co do zasady odbiorca danych osobowych związany jest celem, w związku z którym dane osobowe zostały udostępnione. Wykroczenie poza ten cel oznacza naruszenie zasady związania celem przetwarzania danych osobowych[3].
Zasady tej nie należy rozumieć jako zakazu przetwarzania danych osobowych w innym celu niż ten, dla którego zostały zebrane, ale jako zakaz przetwarzania danych w celu niezgodnym z pierwotnie określonym.
Dalsze przetwarzanie nie powinno być więc sprzeczne z pierwotnym celem zbierania informacji[4].
Odmienna interpretacja prowadziłaby do wniosku, że odbiorca danych nie ma żadnej swobody decyzyjnej w zakresie wyznaczenia celów przetwarzania otrzymanych danych, co jest podstawowym elementem odróżniającym ADO od procesora.

Umowa powierzenia

Podstawą prawną legalizującą powierzanie danych do przetwarzania przez ADO (i przetwarzania danych przez procesora, któremu powierzono dane) jest umowa, o której mowa w art. 31 uodo.
Obie strony powinny dążyć do zawarcia umowy powierzenia danych zgodnej z wymogami obowiązującego prawa, aby nie narazić się na zarzut przetwarzania danych bez odpowiedniej podstawy prawnej (co może być źródłem odpowiedzialności na gruncie uodo).
Umowa taka powinna być zawarta w formie pisemnej oraz precyzyjnie określać zakres i cel ich przetwarzania. Zgodnie z art. 31 ust. 2 uodo podmiot, któremu powierzono przetwarzanie danych , może przetwarzać je wyłącznie w zakresie (rozumianym jako katalog operacji wykonywanych na danych) oraz w celu (oznaczającym przeznaczenie danych) przewidzianym w umowie[5].
Umowa powierzenia może dotyczyć wszelkich operacji na danych osobowych (np. przechowywania na zewnętrznym serwerze w związku ze świadczeniem na rzecz administratora usług tzw. hostingu). W konsekwencji, zgodnie ze stanowiskiem SN także administrator ADO danych, który korzysta z usług innego podmiotu wyłącznie w celu usunięcia danych, powinien zawrzeć z nim umowępowierzenia[6].
Podmiot przetwarzający dane osobowe na zlecenie uprawniony jest więc do przetwarzania danych wyłącznie w celu i w zakresie określonym w umowie. W przypadku powierzenia danych procesor jest więc wprawdzie ograniczony w zakresie decydowania o celach przetwarzania danych, jednak ograniczenia te nie dotyczą środków przetwarzania danych. Jeżeli więc w umowie powierzenia nie zawarto postanowień w tym przedmiocie, decyzje o środkach przetwarzania danych mogą być podejmowane przez podmioty przetwarzające dane na zlecenie (stosowane przez procesora środki przetwarzania danych muszą być jednak adekwatne do wyznaczonych przez ADO celów przetwarzania). Taka interpretacja pozostaje w zgodzie z przedstawionymi wytycznymi Grupy Roboczej art. 29.

Podpowierzenie przetwarzania

Istotnym w praktyce obrotu gospodarczego zagadnieniem jest również możliwość korzystania przez podmiot przetwarzający dane na zlecenie z usług podwykonawców (tzw. podpowierzanie danych osobowych). Przepisy uodo nie regulują tej kwestii w sposób wyraźny.
Takie działanie można jednak uznać za dopuszczalne w świetle przepisów prawa, w przypadku gdy:

- w treści umowy powierzenia wskazane zostaną konkretne (wskazane co do tożsamości) podmioty, które mogą działać jako podwykonawcy procesora, albo
- w trakcie realizowania umowy powierzenia, procesor uzyska pisemną zgodę ADO na skorzystanie z usług podwykonawcy albo
- przetwarzanie danych przez podprocesora pozostaje w granicach celu i zakresu przetwarzania określonych w umowie powierzenia[7].

[1] P. Barta, P. Litwiński, Ustawa…, jw.
[2] J. Barta, P. Fajgielski, R. Markiewicz, Ochrona danych osobowych. Komentarz, komentarz do art. 23, LEX.
[3] P. Barta, P. Litwiński, Ustawa …, jw., komentarz do art. 26 uodo
[4] J. Barta, P. Fajgielski, R. Markiewicz, Ochrona…, jw., s. 552.
[5] Wyrok WSA w Warszawie z 15 lutego 2006 r., II SA/WA 2055/05, Legalis.
[6] Postanowienie SN z 11 grudnia 2000 r., II KKN 438/00, OSNKW 2001, nr 3–4, poz. 33.
[7] P. Barta, P. Litwiński, Ustawa …, jw. komentarz do art. 31 uodo

Odpowiedzialność

W przypadku udostępnienia danych oraz powierzenia danych do przetwarzania odmienne są również podstawy oraz zakres odpowiedzialności podmiotów biorących udział w przetwarzaniu. Odpowiedzialność z tytułu nieprzestrzegania przepisów ponosi ADO. Administrator może ponosić zarówno odpowiedzialność karną, jak i administracyjną. Sankcje karne określają przepisy art. 49 i 51 uodo. Zgodnie z art. 49 ust. 1 uodo przestępstwem jest przetwarzanie danych, do którego ADO nie jest uprawniony (w odniesieniu do danych wrażliwych skutkować może karą pozbawienia wolności do 3 lat – art. 49 ust. 2).
Stanie się tak, gdy ADO udostępni dane bez odpowiedniej podstawy prawnej (odbiorca nie będzie w stanie wykazać podstawy prawnej legalizującej przetwarzania otrzymanych danych). Odpowiedzialność w takim przypadku może ponieść także podmiot udostępniający.
Zgodnie z art. 51 uodo „kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2".
W przypadku naruszenia przepisów o ochronie danych osobowych Generalny Inspektor z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje administratorowi przywrócenie stanu zgodnego z prawem, np. usunięcia uchybień, nieudostępniania danych, usunięcia danych (art. 18 uodo).

Odpowiedzialność procesora

Także podmiot, któremu powierzono przetwarzanie może ponosić odpowiedzialność za ich niezgodne z prawem przetwarzanie. Odpowiedzialność procesora możliwa jest na podstawie trzech reżimów prawnych:

- odpowiedzialność cywilna w stosunku do ADO, wynikającą z postanowień umowy łączącej te dwa podmioty. Może to być bądź odpowiedzialność kontraktowa na podstawie art. 471 kc (za niewykonanie lub nienależyte wykonanie zobowiązania), bądź odpowiedzialność deliktowa z art. 415 kc (związana wyrządzeniem szkody ADO).
- odpowiedzialność administracyjna z tytułu niespełnienia wymogów w zakresie zabezpieczenia danych (na podstawie art. 18 w zw. z art. 36–39a uodo). Zgodnie z art. 31 ust. 5 uodo podmiot przetwarzający dane osobowe na zlecenie został również objęty zakresem kompetencji kontrolnych GIODO.

W związku z tym adresatem decyzji GODO może być również ten podmiot[1]. Na podstawie art. 31 ust. 3 zd. 2 uodo podmiot przetwarzający dane na zlecenie jest odpowiedzialny za przestrzeganie przepisów o zabezpieczeniu danych (art. 36–39a) „jak administrator danych". Przepis ten rodzi jednak pewne wątpliwości interpretacyjne w kontekście brzmienia art. 31 ust. 4 uodo. Wprowadza on zasadę ponoszenia przez ADO odpowiedzialności za działania własne oraz podmiotu przetwarzającego dane na zlecenie. Zgodnie z tą regulacją: „W przypadkach, o których mowa w ust. 1–3, odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową".
Zestawiając treść obu przepisów nie jest więc jasne, który z podmiotów – ADO czy procesor – ponosi odpowiedzialność za przestrzeganie przepisów o zabezpieczeniu danych w sytuacji powierzenia. W doktrynie prezentowane są w tym zakresie dwa stanowiska. Zgodnie z pierwszym, ADO odpowiada za wykonanie wszystkich obowiązków nałożonych ustawą, natomiast w zakresie zabezpieczenia danych, jego odpowiedzialność ograniczona jest wyłącznie do przetwarzania danych we własnej jednostce organizacyjnej[2].
Drugi pogląd stwierdza, że powierzenie danych do przetwarzania innemu podmiotowi nie zwalnia ADO z odpowiedzialności za przestrzeganie ustawy. Wynika to z tego, że sformułowanie „ponosi odpowiedzialność jak administrator danych" należy uznać wyłącznie za wprowadzające odpowiedzialność podmiotu przetwarzającego dane na zlecenie, a nie wyłączające odpowiedzialność ADO. Odpowiedzialność procesora jest w tym przypadku „taka jak administratora danych". Oznacza to, że oparta jest na tych samych przepisach prawa materialnego (obowiązki zabezpieczenia określone w art. 36–39a) oraz regulacjach proceduralnych (w zakresie formy i treści uprawnień kontrolnych GIODO).

- odpowiedzialność karna w przypadku, gdy przekazanie danych[3] do przetwarzania nie zostało zrealizowane z dochowaniem wymogów ustawy (nie zawarto umowy powierzenia danych).

Podstawą tej odpowiedzialności może być w szczególności art. 49 uodo. Przetwarzanie danych przez osobę nieuprawnioną występuje w przypadku, gdy realizuje je podmiot spoza kręgu osób upoważnionych do przetwarzania. Do kręgu tego zaliczyć można samego ADO, osoby mające upoważnienie nadane przez ADO na podstawie art. 37 uodo oraz procesora. Osoba, która nie zalicza się do kręgu osób uprawnionych do przetwarzania, a przetwarza dane popełnia więc przestępstwo.
Taka sytuacja może mieć miejsce, gdy nie zostanie zawarta umowa powierzenia pomiędzy ADO a „rzekomym procesorem", upoważaniająca tego ostatniego do przetwarzania danych. Przy czym brak dochowania wymogu formy pisemnej umowy powierzenia nie oznacza jej nieważności[4]. W związku z tym np. ustna umowa powierzenia danych jest w świetle prawa cywilnego ważna i w przypadku możliwości wykazania jej zawarcia procesor nie będzie ponosił odpowiedzialności karnej. Rozwiązanie takie może powodować natomiast niekorzystne skutki na gruncie odpowiedzialności administracyjnej, ponieważ niespełnienie wymogu formy powoduje naruszenie przepisów uodo i może powodować sankcje w postaci decyzji administracyjnej wydanej na podstawie art. 18 uodo.

[1] X. Konarski, G. Sibiga, Zmiany w ustawie o ochronie danych osobowych w świetle dyrektywy 95/46/WE, MoP 2004, nr 12, s. 551–552; J. Barta, P. Fajgielski, R. Markiewicz, Ochrona…, jw. s. 449–450.

[2] X. Konarski, G. Sibiga, Zmiany…, jw., s. 552.

[3] P. Barta, P. Litwiński, Ustawa …, jw. komentarz do art. 31 uodo.

[4] A. Szewc, *Z problematyki ochrony danych osobowych*, cz. III, R. Pr. 1999, nr 5, s. 21; J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona*…, jw., s. 619.

Zachęcamy do korzystania z naszej strony internetowej
www.odo.wip.pl
Znajduje się tam archiwum wszystkich dotychczasowych numerów.
Można też pobrać wszystkie wzory dokumentów publikowane w miesięczniku.

„Oficyna Prawa Polskiego”
Wydawnictwo WiP
ul. Łotewska 9A, 03-918 Warszawa

NIP: 526-19-92-256

KRS: 0000098264 – Sąd Rejonowy dla m.st. Warszawy,
Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy
Wysokość kapitału zakładowego: 200.000 zł
„Ochrona danych osobowych”

Patronat merytoryczny:
Traple, Konarski, Podrecki i Wspólnicy Sp. jawna

Redaktor:
Wioleta Szczygielska

Kierownik grupy wydawniczej:
Agnieszka Konopacka-Kuramochi

Wydawca:
Weronika Wota

Koordynacja produkcji:
Mariusz Jezierski, Magdalena Huta

Korekta:
Zespół

Projekt graficzny okładki:
Michał Marczewski

Skład i łamanie:
Ireneusz Gawliński

Drukarnia: MDdruk

Nakład: 1500 egz.

Informacje o prenumeracie:
tel.: 22 518 29 29
faks: 22 617 60 10
e-mail: cok@opp.com.pl