POLSKA I EUROPEJSKA REFORMA OCHRONY DANYCH OSOBOWYCH

redakcja naukowa
Edyta Bielak-Jomaa, Dominik Lubasz

Tomasz A.J. Banyś, Edyta Bielak-Jomaa, Maciej Byczkowski
Witold Chomiczewski, Michał Czerniawski, Berenika Kaczmarek-Templin
Michał Kaczorowski, Damian Karwala, Piotr Kawczyński
Maciej Kawecki, Xawery Konarski, Magdalena Kuba, Andrzej Lewiński
Paweł Litwiński, Dominik Lubasz, Joanna Łuczak, Magdalena Piech
Grzegorz Sibiga, Katarzyna Witkowska, Teresa Wyka

MONOGRAFIE

Wolters Kluwer

POLSKA I EUROPEJSKA REFORMA OCHRONY DANYCH OSOBOWYCH

redakcja naukowa
Edyta Bielak-Jomaa, Dominik Lubasz

Tomasz A.J. Banyś, Edyta Bielak-Jomaa, Maciej Byczkowski
Witold Chomiczewski, Michał Czerniawski, Berenika Kaczmarek-Templin
Michał Kaczorowski, Damian Karwala, Piotr Kawczyński
Maciej Kawecki, Xawery Konarski, Magdalena Kuba, Andrzej Lewiński
Paweł Litwiński, Dominik Lubasz, Joanna Łuczak, Magdalena Piech
Grzegorz Sibiga, Katarzyna Witkowska, Teresa Wyka

MONOGRAFIE

Wolters Kluwer

WARSZAWA 2016

Publikacja dofinansowana przez Centrum Ochrony Danych Osobowych
i Zarzadzania Informacją na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego;
Publikacja dofinansowana przez Okręgową Izbę Radców Prawnych w Łodzi

Stan prawny na 1 czerwca 2016 r.

Recenzent
Dr hab. prof. KUL Paweł Fajgielski

Wydawca
Monika Pawłowska

Redaktor prowadzący
Ewa Fonkowicz

Opracowanie redakcyjne
Anna Krzesz

Łamanie
Wolters Kluwer

ISBN 978-83-264-9069-9
ISSN 1897-4392

ISBN PDF-a: 978-83-8092-764-3

Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: ksiazki@wolterskluwer.pl

www.wolterskluwer.pl
księgarnia internetowa www.profinfo.pl

Spis treści

Wykaz skrótów

Akty prawne

dyrektywa 95/46/WE	dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995, s. 31, Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, s. 355)
Konstytucja RP	Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 z późn. zm.)
k.c.	ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (tekst jedn.: Dz. U. z 2016 r. poz. 380 z późn. zm.)
k.p.	ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (tekst jedn.: Dz. U. z 2014 r. poz. 1502 z późn. zm.)
k.p.a.	ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (tekst jedn.: Dz. U. z 2016 r. poz. 23)
ogólne rozporządzenie	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia

	dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, s. 1)
p.p.s.a.	ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (tekst jedn.: Dz. U. z 2012 r. poz. 270 z późn. zm.)
u.o.d.o.	ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz. U z 2015 r. poz. 2135 z późn. zm.)
u.u.w.d.g., ustawa deregulacyjna	ustawa z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. poz. 1662 z późn. zm.)

Czasopisma i publikatory

Dz. U.	Dziennik Ustaw
Dz. Urz. WE/UE	Dziennik Urzędowy Wspólnoty Europejskiej/Unii Europejskiej
Mon. Praw.	Monitor Prawniczy
OSNAPiUS	Orzecznictwo Sądu Najwyższego. Zbiór Urzędowy. Izba Administracyjna, Pracy i Ubezpieczeń Społecznych
OSNC	Orzecznictwo Sądów Polskich. Izba Cywilna
OSNP	Orzecznictwo Sądu Najwyższego – Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych
PUG	Przegląd Ustawodawstwa Gospodarczego
RPEiS	Ruch Prawniczy, Ekonomiczny i Socjologiczny

Organy i urzędy

ABI	administrator bezpieczeństwa informacji
ADO	administrator danych osobowych

CNIL	Commission nationale de'l informatique et des libertés (Krajowa Komisja Informatyki i Wolności)
DPO	*data protection officer* lub *official*
GIODO	Generalny Inspektor Ochrony Danych Osobowych
IOD	inspektor ochrony danych
NSA	Naczelny Sąd Administracyjny
SN	Sąd Najwyższy
TS	Trybunał Sprawiedliwości

Słowo wstępne

Monografia *Polska i europejska reforma ochrony danych osobowych* porusza niezwykle istotne zagadnienia dotyczące ram prawnych działania każdego administratora danych, zarówno obecnych, jak i przyszłych. Dotyka bowiem z jednej strony problematyki związanej z polską reformą ochrony danych osobowych przeprowadzoną w latach 2014–2015, a z drugiej tematykę europejskiej reformy ochrony danych osobowych, której zwieńczeniem było przyjęcie tzw. pakietu ochrony danych, obejmującego rozporządzenie w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych)[1] oraz dyrektywę w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych[2].

[1] Projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych, COM (2012) 11, C7-0025/2012 – 2012/0011(COD), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pl.pdf. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, s. 1).

[2] Projekt dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy na potrzeby zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu takich danych, COM (2012) 10 (COD), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony

Z perspektywy organu nadzorczego dla administratorów danych wyzwaniem było już samo dostosowanie się do wymogów znowelizowanej ustawy o ochronie danych osobowych. Jeszcze trudniejszym zadaniem będzie, jak się wydaje, prawidłowe wdrożenie systemów ochrony danych osobowych zgodnie z unijnym ogólnym rozporządzeniem. Niniejsza publikacja może ułatwić zarówno weryfikację poprawności zastosowania już obowiązujących przepisów o ochronie danych, jak i pomóc w przygotowaniu na czekające w roku 2018 zmiany.

Nie ulega wątpliwości, że bez prawidłowego odczytania i zrozumienia już obowiązujących przepisów podnoszenie standardów ochrony nie jest możliwe. Polski ustawodawca, nowelizując ustawę o ochronie danych osobowych, starał się dostosować ją do kierunku zmian wyznaczonego w styczniu 2012 roku przez projekt ogólnego rozporządzenia, zaproponowany przez Komisję Europejską. Jest to jeden z podstawowych argumentów świadczących o wadze polskiej regulacji oraz wskazujący, jak ważna jest prawidłowa interpretacja wprowadzonych zmian również pod kątem zrozumienia nadchodzących zmian.

W publikacji poruszono zarówno problematykę stosowania nowych przepisów z perspektywy administratora danych, jak i administratora bezpieczeństwa informacji. Omówione zostały problemy związane z wykonywaniem zadań przez ABI, koniecznością zagwarantowania mu odpowiedniej pozycji w strukturze administratora danych, konfliktem między niezależnością ABI a podległością pracowniczą. Odniesiono się także do bardzo istotnego zagadnienia transferu danych do państw trzecich, przeprowadzając analizę obowiązujących przepisów, nadchodzących zmian i bardzo ważnych orzeczeń Trybunału Sprawiedliwości Unii Europejskiej w sprawach C-230/14, *Weltimmo*[3] i C-362/14, *Schrems*[4], poddano również analizie najważniejsze elementy europejskiej reformy ochrony danych z uwzględnieniem najnowszego

osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 4.05.2016, s. 89).

[3] Wyrok z dnia 1 października 2015 r. w sprawie C-230/14, *Weltimmo s.r.o. przeciwko Nemzeti Adatvédelmi és Információszabadság Hatóság*, ECLI:EU:C:2015:639.

[4] Wyrok z dnia 6 października 2015 r. w sprawie C-362/14, *Maximillian Schrems przeciwko Data Protection Commissioner*, ECLI:EU:C:2015:650.

orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej oraz programu „Tarcza Prywatności UE–USA" (*EU–U.S. Privacy Shield*)[5].

Perspektywa ogólnego rozporządzenia, które będzie stosowane od 25 maja 2018 roku, a także optyka i *ratio legis* polskiej nowelizacji, nie pozwalają jednak patrzeć na ochronę danych wyłącznie przez pryzmat prawa krajowego. Skala nadchodzących zmian jest na tyle rozległa, że zarówno ustawodawca krajowy, jak i administratorzy danych powinni już teraz przeanalizować nowe mechanizmy ochrony danych. Dla ustawodawcy nadchodzące zmiany będą również bez wątpienia wyzwaniem, jako że związane są one z koniecznością dokonania kompleksowej rewizji aktów prawnych, tak by w okresie przejściowym dostosować obowiązujące przepisy prawa krajowego do nowych ram ochrony danych bezpośrednio obowiązującego rozporządzenia unijnego i zapewnić tym samym warunki do pełnego stosowania tego aktu prawnego. Według szacunkowych danych Rządowego Centrum Legislacji analizy będzie wymagać około 800 aktów prawnych, dwuletni okres *vacatio legis* od publikacji ogólnego rozporządzenia w Dzienniku Urzędowym Unii Europejskiej do jego wejścia w życie wymusi więc potrzebę podjęcia intensywnych prac w tym zakresie.

Dla administratorów danych rozpoczyna się z kolei czas na przegląd stosowanych procedur i wdrożonych rozwiązań oraz rozważenie, w jaki sposób i z wykorzystaniem jakich środków rozpoczną stosowanie nowych przepisów w swojej praktyce. Rozporządzenie jest konsekwentnie technologicznie neutralne, jednakże zmienia optykę dotychczasowych przepisów i poprzez takie nowe instytucje, jak *privacy by design*, *privacy by default* czy też *privacy risk assessment*, a także *privacy impact assessment*, daje administratorom danych swobodę wyboru środków zabezpieczających przetwarzanie danych. Celem tej swobody jest jednak podwyższenie standardów ochrony, a także odwrócenie jej ciężaru i uczynienie z niej ochrony aktywnej, w miejsce reaktywnej.

Podkreślić należy, że *ratio legis* nowych ram prawnych ochrony danych, zwłaszcza ogólnego rozporządzenia, miało być uwspółcześnienie ochrony danych osobowych, podniesienie poziomu ochronnego, a także przyznanie

[5] Źródło: http://europa.eu/rapid/press-release_IP-16-216_en.htm [dostęp: 5 marca 2016 r.].

większej kontroli osobom, których dane dotyczą, nad całością procesów przetwarzania danych. Podnoszenie standardów ochrony danych przez administratorów w naturalny sposób skorelowane jest ze zwiększaniem uprawnień podmiotów danych. Obserwujemy wyraźną tendencję do rozbudowywania obowiązków informacyjnych, nacisk na tworzenie jasnych i przejrzystych komunikatów kierowanych do osób, których dane dotyczą, a to prowadzi do zwiększania świadomości nie tylko istnienia, ale i potrzeby egzekwowania przepisów.

Wyznaczanie granic prywatności, zwłaszcza w czasie globalizacji informacji, jest zabiegiem wzbudzającym kontrowersję. Należy jednak pamiętać, że większa świadomość podmiotów danych oznacza też większe oczekiwania i wymagania co do ochrony danych i bardziej stanowczą potrzebę egzekwowania respektowania tych granic. Stosowanie przepisów, zwłaszcza wobec wprowadzonych do ogólnego rozporządzenia sankcji za ich naruszenie, z pewnością przyczyni się do wzmocnienia ochrony danych osobowych obywateli. Warto więc już teraz rozpocząć przygotowania do wdrażania nowych rozwiązań, w czym z pewnością pomoże Państwu nasza publikacja.

Edyta Bielak-Jomaa[*]

[*] Doktor, adiunkt w Katedrze Prawa Pracy Wydziału Prawa i Administracji Uniwersytetu Łódzkiego. Od 2015 r. pełni funkcję Generalnego Inspektora Ochrony Danych Osobowych.

Wprowadzenie

Prezentowane opracowanie poświęcone jest zmianom w przepisach o ochronie danych osobowych w prawie unijnym, wprowadzonym do polskiego porządku prawnego z dniem 1 stycznia 2015 r. na mocy ustawy z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej[1]. Zmiany w prawie polskim – podyktowane, jak wynika z tytułu ustawy nowelizującej, potrzebą uproszczenia procedur obciążających przedsiębiorców, co może dotyczyć m.in. gromadzenia i przetwarzania informacji – zostały dokonane w momencie szeroko zakrojonych prac legislacyjnych na poziomie unijnym związanych z ogólnym rozporządzeniem o ochronie danych osobowych, ostatecznie zakończonych jego przyjęciem 14 kwietnia 2016 r. przez Parlament Europejski. Zrodziła się więc potrzeba skonfrontowania nowych uregulowań polskich z projektowanymi regulacjami w UE w przedmiotowym obszarze. Taki też cel przyświecał autorom niniejszej publikacji, aby dokonać oceny nowych regulacji wprowadzonych do ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[2] z perspektywy ogólnego rozporządzenia o ochronie danych osobowych[3] i ustalić, w jakim stopniu ustawodawstwo polskie jest przygotowane do stosowania rozporządzenia.

Publikacja składa się z trzech części. Wspólnym przesłaniem są zmiany w przepisach o ochronie danych osobowych. Chodzi zarówno o zmiany

[1] Dz. U. poz. 1662 z późn. zm.

[2] Tekst jedn.: Dz. U. z 2015 r. poz. 2135 z późn. zm.

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, s. 1).

w uregulowaniach unijnych, jak i polskich. W różnym jednak stopniu obszary tych zmian zostały poddane analizie w poszczególnych częściach książki.

Część I zawiera prezentację wybranych, ogólnych zagadnień wyłaniających się głównie na tle unijnej reformy ochrony danych osobowych. Reforma ta jest zasadniczo przedstawiona z punktu widzenia administratora danych osobowych.

W świetle wskazanych wyżej regulacji prawnych został on postawiony przed problemem dokonania ewentualnego (bo nieobowiązkowego) powołania administratora bezpieczeństwa informacji, co jest oceniane jako ułatwienie w wykonywaniu działalności gospodarczej, szczególnie jednak w kontekście unormowań unijnych, a nie polskich (część I, rozdział 1, *„Deregulacyjna" nowelizacja i unijna reforma zasad ochrony danych osobowych z perspektywy administratora danych osobowych* – M. Piech). Wśród administratorów danych osobowych występuje specyficzna grupa, jakimi są podmioty publiczne. Stoją one przed trudnym dylematem pozostania w zgodzie z licznymi ograniczeniami wynikającymi z przepisów o finansach publicznych i zamówieniach publicznych z potrzebą wyłonienia jak najlepszego kandydata na administratora bezpieczeństwa informacji (część I, rozdział 2, *Wdrażanie nowych elementów systemu ochrony danych osobowych przez podmioty publiczne* – T.A.J. Banyś). Analiza motywów i treści ogólnego rozporządzenia o ochronie danych osobowych prowadzi m.in. do wniosku, że stworzy ono szansę dla różnicowania obowiązków administratorów danych ze względu na wielkość podmiotu i znaczenie przetwarzania danych w jego działalności, z zachowaniem zasady swobody wyboru środków realizacji tych obowiązków (część I, rozdział 3, *Europejska reforma ochrony danych osobowych – nowe obowiązki administratorów w ogólnym rozporządzeniu o ochronie danych* – D. Lubasz). Nie ulega wątpliwości, że unijne rozporządzenie wpłynie na globalny system ochrony danych osobowych. W dobie internetu i społeczeństwa informacyjnego zachodzi jednak potrzeba zweryfikowania zasady właściwości miejscowej dla rozstrzygania spraw dotyczących ochrony danych osobowych (część I, rozdział 4, *Zakres terytorialny stosowania polskich i unijnych przepisów o ochronie danych osobowych w kontekście najnowszego orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej* – M. Czerniawski). Jak wynika z ogólnego rozporządzenia, zasadnicze znaczenie dla zapewnienia

właściwej ochrony prywatności i autonomii informacyjnej osoby ma przestrzeganie zasad legalności przetwarzania danych osobowych. Wśród nich na szczególną uwagę zasługuje przesłanka zgody podmiotu danych, której procedura uzyskiwania jest wyjątkowo skomplikowana w przypadku osób małoletnich (część I, rozdział 5, *Podstawy legalizacyjne przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych – wybrane zagadnienia* – B. Kaczmarek-Templin). Wśród nowych uregulowań zawartych w rozporządzeniu unijnym nie sposób pominąć instytucji profilowania, polegającego na ustalaniu profilu osób w oparciu o dane statystyczne w celu określenia przewidywanych zachowań. Zjawisko to, coraz szerzej występujące, może rodzić szereg niebezpieczeństw, w tym naruszenie prywatności, a nawet może prowadzić do dyskryminacji. Ochronie przed nadużywaniem profilowania służą przepisy rozporządzenia określające nie tylko przesłanki legalnego profilowania, ale także prawo do sprzeciwu wobec takich praktyk (część I, rozdział 6, *Profilowanie w ogólnym rozporządzeniu o ochronie danych* – W. Chomiczewski).

Część II publikacji zawiera opracowania oceniające zmiany w przepisach o ochronie danych osobowych z perspektywy administratora bezpieczeństwa informacji, a zatem osoby, która ma, co do zasady, wspomagać, lecz nie zastępować administratora danych osobowych. W tej części książki uwaga Autorów skupia się w większym stopniu, niż w części I, na uregulowaniach polskich, które są jednak badane w kontekście prawa unijnego.

Instytucja administratora bezpieczeństwa informacji znalazła swoje umocowanie w dyrektywie 95/46/WE w sprawie ochrony danych osobowych i swobodnego przepływu tych danych[4], będącej podstawą dla ukształtowania jego pozycji w wielu porządkach prawnych państw należących do Unii, m.in. w Niemczech, Austrii, Danii, Finlandii, Holandii i Francji. Polska dokonała implementacji dyrektywy w tym zakresie w zasadzie dopiero na mocy przepisów obowiązujących od 1 stycznia 2015 r. Oczekiwane wejście w życie ogólnego rozporządzenia w sprawie ochrony danych osobowych stawia przed administratorem bezpieczeństwa informacji szczególne wymagania w zakresie jego profesjonalizmu (część II, rozdział 1, *Administrator bezpieczeństwa informacji – zagadnienia konstrukcyjne* – A. Lewiński). Na gruncie

[4] Dz. Urz. WE L 281 z 23.11.1995, s. 31, Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, s. 355.

prawa polskiego ów profesjonalizm okaże się niezbędny w związku z nowymi zadaniami, jakie przypisywane są administratorowi bezpieczeństwa informacji. W szczególności chodzi o poszerzenie przedmiotu jego aktywności na wszystkie przepisy o ochronie danych osobowych, jak również o obowiązek prowadzenia wewnętrznych rejestrów zbiorów danych oraz działania nie tylko z punktu widzenia potrzeb administratora danych, ale także Generalnego Inspektora Danych Osobowych (część II, rozdział 2, *Zadania administratora informacji – wybrane zagadnienia* – G. Sibiga). Mając na uwadze nowe, a nawet określane mianem nowatorskich, zadania administratora bezpieczeństwa informacji, konieczna staje się ocena procedur mocujących go do tych zadań. Należy do nich niewątpliwie procedura rejestracji, a także wykreślenia z rejestru administratora bezpieczeństwa informacji, o której stanowią przepisy ustawy o ochronie danych osobowych i przepisy wykonawcze wydane na jej podstawie (część II, rozdział 3, *Procedura rejestracji administratorów bezpieczeństwa informacji* – J. Łuczak). Ustalenie zarówno w regulacjach unijnych, jak i w prawie polskim zasady fakultatywności powoływania administratora bezpieczeństwa informacji rodzi zasadnicze pytanie o konsekwencje odpowiednich decyzji w tym przedmiocie. Pozostawienie tej decyzji administratorowi danych osobowych jest najczęściej oceniane pozytywnie, świadczy o uznaniu swobody w wyborze sposobów ochrony danych osobowych i nie może być traktowane jako osłabienie tej ochrony. Nie bez znaczenia dla podejmowanych decyzji powinien być fakt, że ustawodawca polski wśród różnych zawodów występujących na rynku pracy wskazuje administratora bezpieczeństwa informacji w grupie specjalistów ds. rozwoju zarzadzania i organizacji[5]. Świadczy to o dostrzeganej specyfice i randze tego nowego zawodu (część II, rozdział 4, *Mieć czy nie mieć ABI? Korzyści i obawy związane z powołaniem administratora bezpieczeństwa informacji* – M. Byczkowski). Zawód ten wymaga wykonywania określonych zadań, także na wezwanie Generalnego Inspektora Danych Osobowych. Chodzi w szczególności o przygotowywanie sprawdzenia i sprawozdania zgodnie z rozbudowanymi procedurami wynikającymi z ustawy i aktów doń wykonawczych (część II, rozdział 5, *Sprawdzenie i sprawozdanie przygotowywane przez administratora bezpieczeństwa informacji na wezwanie Generalnego Inspektora Ochrony Danych Osobowych* –

[5] Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 7 sierpnia 2014 r. w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy oraz zakresu jej stosowania (Dz. U. poz. 1145).

P. Kawczyński). Niezwykle istotne z punktu widzenia efektywności działania administratora bezpieczeństwa informacji zarówno w jego relacjach z administratorem danych osobowych, jak i organami nadzoru ma określenie podstaw świadczenia przez niego pracy. Ustawodawca tego nie przesądza. Może to więc być także forma zatrudnienia pracowniczego. Rodzi to jednak zasadnicze pytanie o granice jego podporządkowania pracodawcy – administratora danych osobowych, tak aby nie ograniczał go w wykonywaniu jego zadań również wobec organów nadzoru. Założona zasada niezależności administratora bezpieczeństwa informacji może być w takim wypadku zagrożona (część II, rozdział 6, *Pozycja administratora bezpieczeństwa informacji na gruncie ustawy o ochronie danych osobowych a jego podporządkowanie w ramach stosunku pracy* – M. Kuba). Wybór podstawy świadczenia pracy przez administratora bezpieczeństwa informacji nie pozostaje bez wpływu na ewentualne łączenie przez niego wykonywania innych zawodów, w szczególności prawniczych. Powstaje jednak wówczas istotny problem pogodzenia reguły wynikającej z ustawy o bezpośredniej podległości kierownikowi jednostki organizacyjnej – administratorowi danych osobowych z zasadą swobody prowadzenia działalności gospodarczej. Istota tego problemu ujawnia się szczególnie wówczas, gdy administratorem bezpieczeństwa informacji chciałby być radca lub adwokat. Wprawdzie ustawa o ochronie danych osobowych nie przewiduje wyraźnie w tym zakresie żadnych ograniczeń, jednak uważa się, że z uwagi na pewne ograniczenia wynikające z regulacji sektorowych byłoby to możliwe w stosunku do radcy prawnego w sytuacji zapewnienia mu z jednej strony niezależności wewnętrznej i zewnętrznej, z drugiej zaś konieczne byłoby stworzenie podległości administratorowi danych (część II, rozdział 7, *Nowe wymogi związane z pełnieniem funkcji ABI a pozycja prawna kancelarii prawnych i zasady wykonywania zawodu radcy prawnego i adwokata – czy można łączyć te role?* – M. Kawecki). Szczegółowe problemy związane z pozycją administratora bezpieczeństwa informacji, głównie na gruncie polskiego porządku prawnego, wymagają oceny także z perspektywy unijnego ogólnego rozporządzenia w sprawie ochrony danych osobowych. Akt ten poświęca bardzo dużo miejsca inspektorowi danych osobowych, wyraźnie eksponując w szczególności regułę fakultatywności jego powoływania, regułę profesjonalizmu i niezależności, co w dużym stopniu przewidują już polskie przepisy o ochronie danych osobowych (część II, rozdział 8, *Data protection officer, czyli inspektor*

ochrony danych w ogólnym rozporządzeniu o ochronie danych – K. Witkowska).

Zmiany w prawie unijnym i polskim w przedmiocie ochrony danych osobowych postawiły na nowo problem transgranicznego przepływu tych danych. Te właśnie zagadnienia zostały przedstawione w części III publikacji, w której Autorzy poddają często krytycznej ocenie obowiązujące i przyjęte na poziomie unijnym rozwiązania prawne z perspektywy różnych podmiotów uczestniczących w transferze.

Kwestią wymagającą wyjaśnienia w pierwszej kolejności jest pojęcie transferu danych, które jak dotąd nie doczekało się definicji legalnej. Najczęściej pod tym pojęciem rozumie się różne działania administratora danych skutkujące przekazywaniem danych osobie trzeciej, zlokalizowanej w państwie trzecim. Zarówno regulacje unijne – te obowiązujące i te projektowane – jak i polska ustawa zawierają stosowne regulacje w tym przedmiocie, wskazując na określone procedury w zależności od m.in. tego, czy państwo trzecie zapewnia adekwatny poziom ochrony. Możliwe są także inne procedury, np. w postaci standardowych klauzul umownych czy wiążących reguł korporacyjnych. Do administratorów danych należy wybór określonego instrumentu (część III, rozdział 1, *Transfer danych osobowych do państw trzecich – perspektywa administratora danych* – M. Kaczorowski). Jest sprawą oczywistą, że kluczowe znaczenie dla transgranicznego przepływu danych będzie miało rozporządzenie unijne, które zawiera szczegółowe unormowania w tym przedmiocie, określając nie tylko różne podstawy transferu, w tym orzeczenia sądów lub decyzje organów państw trzecich, lecz także ustalając sankcje w razie naruszenia określonych procedur. Regulacje te spotykają się jednak z różną, często krytyczną oceną (część III, rozdział 2, *Transfer danych osobowych na podstawie ogólnego rozporządzenia o ochronie danych a dotychczasowy stan prawny w UE i w Polsce* – X. Konarski). Trzeba jednak mieć na uwadze, że krytyczne oceny nie odnoszą się do obowiązujących regulacji, ale są oparte na kilku wersjach projektu rozporządzenia. Z chwilą wejścia w życie rozporządzenia nastąpi m.in. rozszerzenie prawnej skuteczności wiążących reguł korporacyjnych na reguły zatwierdzane przez inny organ niż GIODO. Uważa się jednak, że w ogólnym rozporządzeniu nie wykorzystano szansy kompleksowego unormowania transgranicznego przepływu danych do państwa nienależącego do Europejskiego Obszaru

Gospodarczego (część III, rozdział 3, *Transfer danych osobowych do państw trzecich w pracach nad ogólnym rozporządzeniem o ochronie danych – stracona szansa* – P. Litwiński). Ustalanie reguł transgranicznego przepływu danych jest ciągle bardzo dynamiczne. Świadczy o tym nowy program – „Tarcza prywatności UE–USA", przyjęty w lutym 2016 r. Organizacje przystępujące do tego programu będą zobowiązane do respektowania określonych w nim zasad oraz mechanizmów kontroli. Ostatecznie podejście do transgranicznych transferów danych osobowych może mieć charakter formalistyczny, oparty na analizie jurydycznej, bez uwzględniania różnych skutków, lub pragmatyczny – uwzględniający kontekst globalny, w tym kulturowy i prawny (część III, rozdział 4, *„Tarcza Prywatności", czyli program Bezpiecznej Przystani w nowej odsłonie – uwagi wokół projektu decyzji Komisji Europejskiej w sprawie adekwatności „Tarczy Prywatności UE–USA"* – D. Karwala).

Prezentowana publikacja została przygotowana przez przedstawicieli środowiska akademickiego, a także przez praktyków zajmujących się od wielu lat zagadnieniami ochrony danych osobowych w Polsce i na świecie. Zapewnia to wszechstronne spojrzenie na skomplikowane konstrukcje prawne służące ostatecznie ochronie prywatności coraz bardziej zagrożonej w dobie globalizacji i społeczeństwa informacyjnego. W książce tej postawiono wiele pytań, poddano analizie różne możliwości interpretacyjne w przedmiotowej dziedzinie, sformułowano także szereg wniosków *de lege ferenda*. Żywimy nadzieję, że publikacja ta pobudzi dyskusję na temat pożądanego modelu ochrony danych osobowych z perspektywy różnych podmiotów.

Teresa Wyka[*]

[*] Profesor nadzwyczajny, doktor habilitowany, kierownik Centrum Ochrony Danych Osobowych i Zarządzania Informacją na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego, kierownik Zakładu Prawa Ochrony Pracy w Katedrze Prawa Pracy na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego, kierownik Katedry Prawa Pracy na Akademii Leona Koźmińskiego w Warszawie; obszary badawcze: prawo ochrony pracy, prawo ochrony danych osobowych.

Część I

Zmiany w przepisach o ochronie danych osobowych – zagadnienia ogólne

Magdalena Piech

Rozdział 1. „Deregulacyjna" nowelizacja i unijna reforma zasad ochrony danych osobowych z perspektywy administratora danych osobowych

1. Wstęp

Prawo ochrony danych osobowych jest przedmiotem szerokiej dyskusji toczącej się wśród prawodawców, przedstawicieli doktryny, przedsiębiorców i obywateli zainteresowanych ochroną swojej prywatności. W ostatnich latach osią debaty był przedstawiony przez Komisję Europejską w 2012 roku projekt ogólnego rozporządzenia o ochronie danych osobowych[1]. Miał on na celu dostosowanie unijnych ram prawnych do nowych warunków technologicznych, wzmocnienie praw obywateli, harmonizację unijnych przepisów dotyczących ochrony danych i ułatwienie działalności przedsiębiorstw poprzez zmniejszenie kosztów działalności transgranicznej i wprowadzenie tzw. zasady *one stop shop*[2]. Projekt regulował obowiązki administratorów względem podmiotu danych i organu nadzorczego. Doprecyzowywał role podmiotów przetwarzających dane na zlecenie oraz ich obowiązki. Rozstrzygał o zakresie stosowania unijnych przepisów, obejmując podmioty z państw trzecich, które przetwarzają dane osób fizycznych mających miejsce zamieszkania w Unii. Projekt rozwijał mechanizmy współpracy organów do spraw ochrony danych oraz tryb podejmowania przez te organy decyzji w sprawach

[1] Projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych COM (2012) 11 final, C7-0025/2012 – 2012/0011(COD), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pl.pdf.

[2] Zob. motywy 4–11 projektu rozporządzenia.

transgranicznych. W toku prac legislacyjnych propozycje Komisji Europejskiej ulegały zmianom, odpowiadającym stanowisku Parlamentu Europejskiego[3] i Rady[4]. Choć wypracowany w 2016 roku, na skutek negocjacji między tymi instytucjami, kompromis[5] odbiega od projektu Komisji, opisany wyżej zakres regulacji pozostał bez zmian.

Mimo tak szeroko zakrojonych prac legislacyjnych na poziomie unijnym, przepisy dotyczące ochrony danych podlegały zmianom także na gruncie krajowym. 1 stycznia 2015 r. weszły w życie zmiany do ustawy o ochronie danych osobowych[6], uzupełnione rozporządzeniami w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji[7] (dalej: rozporządzenie w sprawie trybu i sposobu realizacji zadań) oraz w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych[8] (dalej: rozporządzenie w sprawie rejestru

[3] Zob. rezolucję ustawodawczą Parlamentu Europejskiego z dnia 12 marca 2014 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//PL.

[4] Zob. stanowisko Rady w pierwszym czytaniu w sprawie przyjęcia rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/pl/pdf.

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.05.2016, s. 1).

[6] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2015 r. poz. 2135 z późn. zm.), zmieniona ustawą z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. poz. 1662 z późn. zm.).

[7] Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 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. poz. 745).

[8] Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. poz. 719).

zbiorów). Biorąc pod uwagę długotrwałość prac nad projektem unijnym[9] i fakt, że akt ten będzie stosowany dopiero dwa lata po jego przyjęciu[10], wydaje się zrozumiałe, że prace na gruncie krajowym nie mogły ulec „zamrożeniu". Z drugiej strony nieodległa perspektywa zasadniczej reformy przepisów o ochronie danych mogła przemawiać za ograniczeniem wprowadzanych zmian krajowych do niezbędnych lub „przygotowujących grunt" pod nadchodzącą reformę unijną.

Niniejszy rozdział ma na celu przeanalizowanie zmian wprowadzonych do ustawy o ochronie danych osobowych z perspektywy administratora danych osobowych. Ocena zostanie przeprowadzona z uwzględnieniem deregulacyjnego[11] celu, przyświecającego prawodawcy oraz spójności ze zmianami planowanymi na poziomie unijnym. W dalszej części omówiona zostanie ewolucja roli urzędnika do spraw ochrony danych[12], począwszy od projektu Komisji Europejskiej, poprzez stanowiska Parlamentu i Rady aż do wersji finalnej. Z uwagi na to, że status i zadania urzędników do spraw ochrony danych zostaną szczegółowo omówione w innej części publikacji, niniejsza praca skupi się głównie na analizie przedstawianych w toku prac koncepcji ukształtowania tej funkcji.

[9] Parlament Europejski i Rada wypracowały swoje stanowiska do projektu odpowiednio dopiero w marcu 2014 i w czerwcu 2015 roku, czyli dwa i trzy lata od przedstawienia projektu przez KE. Porozumienie w sprawie ostatecznego tekstu osiągnięto w grudniu 2015 r., http://europa.eu/rapid/press-release_IP-15-6321_en.htm.

[10] Zob. art. 99 rozporządzenia, zgodnie z którym rozporządzenie ma zastosowanie od dnia 25 maja 2018 r. Okres pomiędzy wejściem w życie a stosowaniem rozporządzeń unijnych ma dać adresatom czas na przygotowanie się do zmian w przepisach.

[11] Nowelizacja ustawy o ochronie danych osobowych została wprowadzona ustawą o ułatwieniu wykonywania działalności gospodarczej, będącą czwartym z projektów rządowych zmierzających do deregulacji gospodarki. Zob. uzasadnienie do ustawy, https://legislacja.rcl.gov.pl/docs//2/181358/181362/181363/dokument87483.pdf.

[12] Takim pojęciem, w odniesieniu do osób powołanych przez administratorów w celu nadzorowania zgodności przetwarzania z przepisami, posługuje się dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995, s. 31, Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, s. 355), którą ma zastąpić projekt rozporządzenia.

2. Nowelizacja deregulacyjna

2.1. Geneza zmian krajowych

Zmiany w przepisach krajowych zostały wprowadzone ustawą z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej[13]. Uzasadnienie do projektu ustawy[14] przyjętego przez Radę Ministrów 10 czerwca 2014 r.[15] wyraźnie wskazuje założenia „deregulacyjne"[16]. Celem ustawodawcy była poprawa warunków prowadzenia działalności poprzez „uproszczenie regulacji, redukcję niektórych obowiązków informacyjnych, doprecyzowanie zagadnień budzących wątpliwości, wsparcie inwestycji oraz podniesienie efektywności pracy". W uzasadnieniu zwracano uwagę na po-

[13] Jak wspomniano wcześniej, była to czwarta ustawa przedstawiona w ramach rządowej inicjatywy określanej mianem deregulacji gospodarki. Ustawa o ułatwieniu wykonywania działalności gospodarczej była w związku tym nazywana „deregulacją IV".

[14] Projekt ustawy poprzedzony został projektem założeń do ustawy przyjętym przez Radę Ministrów 23 kwietnia 2013 r., https://legislacja.rcl.gov.pl/docs//1/70340/70372/70373/dokument74914.pdf. Konsultacje społeczne projektu założeń rozpoczęto w październiku 2012 r.

[15] https://legislacja.rcl.gov.pl/docs//2/181358/181395/181399/dokument122560.pdf. Projekt skierowano do Sejmu 7 lipca 2014 r.

[16] Pojęcie deregulacji nie jest zdefiniowane ustawowo. Początkowo było ono używane w odniesieniu do znoszenia ograniczeń w dostępie do zawodów regulowanych, prowadzonych przez rząd z inicjatywy Ministerstwa Sprawiedliwości w latach 2013–2014. Zob. https://ms.gov.pl/pl/deregulacja-dostepu-do-zawodow/i-transza/. W latach 2011–2015 używano go w kontekście prac rządowych zmierzających do ułatwienia wykonywania działalności gospodarczej. Założenia deregulacji opisano następująco: „Znoszenie barier administracyjnych i zmniejszanie liczby obowiązków informacyjnych bądź uciążliwości związanych z ich wykonywaniem jest najlepszym, często bezkosztowym sposobem na wyzwolenie sił i mechanizmów rozwojowych. Dlatego Rząd podjął się zniesienia zbędnych regulacji oraz zmniejszenia kosztów regulacyjnych ponoszonych przez adresatów regulacji. Dzięki temu możliwe będzie m.in. ograniczanie obszarów korupcjogennych i zwiększanie sfery wolności obywateli, w tym wolności gospodarczej. Takie podejście jest podstawą zmiany filozofii tworzenia prawa i co ważne tworzenia innej relacji między państwem a obywatelem". Zob. http://www.mg.gov.pl/Prawo+dla+przedsiebiorcy/Dzialania+legislacyjne oraz rozporządzenie Rady Ministrów z dnia 6 grudnia 2011 r. w sprawie ustanowienia Pełnomocnika Rządu do spraw deregulacji gospodarczych (Dz. U. Nr 276, poz. 1630), następnie uchylone na mocy rozporządzenia Rady Ministrów z dnia 5 kwietnia 2016 r. w sprawie zniesienia Pełnomocnika Rządu do spraw deregulacji gospodarczych (Dz. U. poz. 491). Takie rozumienie nawiązuje do potocznej definicji tego słowa, zgodnie z którą deregulacja to „wycofywanie się państwa z regulowania jakichś dziedzin życia społecznego lub gospodarczego, unieważnienie uznanych za zbędne przepisów prawnych, regulujących jakiś rodzaj aktywności". Zob. http://sjp.pl/deregulacja.

zytywny wpływ, jaki zmiany wywrą na małe i średnie przedsiębiorstwa. Projektodawca deklarował, że „uproszczenie regulacji i procedur odciąży przedsiębiorstwa i ich pracowników od wykonywania niektórych zbędnych formalności administracyjnych, co w konsekwencji umożliwi zwiększenie efektywności gospodarowania posiadanymi zasobami i koncentrację na podstawowej działalności przedsiębiorcy".

2.2. Deregulacja w ustawie o ochronie danych osobowych

Z analizy części uzasadnienia ustawy o ułatwieniu wykonywania działalności gospodarczej odnoszącej się do nowelizacji ustawy o ochronie danych osobowych wynika, że głównymi zmianami realizującymi cele deregulacyjne w odniesieniu do przetwarzania danych osobowych są:

a) zwolnienie administratorów, którzy zgodnie z nowymi wymogami powołają i zgłoszą do Generalnego Inspektora Ochrony Danych Osobowych administratora bezpieczeństwa informacji oraz administratorów, którzy nie prowadzą swoich zbiorów danych w systemie informatycznym, z obowiązku zgłaszania do GIODO zbiorów danych;
b) poszerzenie katalogu środków, które mogą być wykorzystane w celu zgodnego z prawem przekazania danych osobowych do państw trzecich oraz państw członkowskich EOG bez zgody GIODO. Wprowadzono m.in. ułatwienia w przeprowadzaniu transferów danych w oparciu o wiążące zasady korporacyjne oraz z wykorzystaniem standardowych klauzul umownych[17];
c) wprowadzenie instytucji uproszczonej kontroli, tzn. możliwości przeprowadzenia jej na zlecenie GIODO przez ABI. Kontrola, zwana w ustawie sprawdzeniem, zakończona jest opracowaniem sprawozdania, które przekazywane będzie GIODO.

Do ustawy o ochronie danych osobowych wprowadzono również przepisy niezbędne do wdrożenia tych zmian, tj. uregulowano zasady powoływania ABI, tryb zgłaszania ABI do GIODO i ich odwoływania oraz sposób prowa-

[17] Niniejszy rozdział nie będzie odnosił się do zmian dotyczących transferów danych do państw trzecich. Warto jednak zasygnalizować, że zmiany dotyczące transferu danych do państw trzecich należy ocenić jako zasadne i spójne z proponowanymi przez Komisję Europejską unijnymi rozwiązaniami w tym zakresie. Nie budzi też wątpliwości, że zmiany te spełniają deregulacyjne założenia prawodawcy krajowego.

dzenia przez GIODO rejestru tych podmiotów. Doprecyzowano obowiązki ABI i warunki, jakie osoba pełniąca tę funkcję powinna spełniać. Określono też podstawowe elementy sprawozdania. Aktom wykonawczym pozostawiono tryb i sposób realizacji zadań ABI oraz sposób prowadzenia jawnego rejestru zbiorów danych, przetwarzanych przez administratora danych osobowych.

3. Tło nowelizacji

3.1. Przepisy dyrektywy 95/46/WE

Część zmian wprowadzonych w ustawie o ochronie danych osobowych wymuszona została postanowieniami dyrektywy 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[18]. Akt ten określa warunki, jakie przepisy państw członkowskich muszą spełniać, żeby prawodawcy krajowi mogli wprowadzić zwolnienia z obowiązku notyfikowania przetwarzania danych[19] organom nadzorczym. Dyrektywa 95/46/WE wymaga powołania przez administratora danych osobowych (ADO) urzędnika do spraw ochrony danych[20], który ma współpracować z organem nadzorczym i które-

[18] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. Urz. WE L 281 z 23.11.1995, s. 31, Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, s. 355).

[19] Motyw 49 dyrektywy 95/46/WE stanowi, że „w celu uniknięcia zbędnych formalności Państwa Członkowskie mogą wprowadzić zwolnienia z obowiązku zawiadamiania oraz uproszczenia procedury zawiadamiania w przypadkach, gdy mało prawdopodobne jest, aby przetwarzanie danych mogło niekorzystnie wpłynąć na prawa i wolności osób, których dane dotyczą, jeżeli jest to zgodne ze środkiem podjętym przez Państwo Członkowskie określającym jego zakres; Państwa Członkowskie mogą również wprowadzić zwolnienia i uproszczenia w przypadku gdy osoba wyznaczona przez administratora zapewni, że przetwarzanie danych wpłynie niekorzystnie na prawa i wolności osób, których dane dotyczą; urzędnik odpowiedzialny za ochronę danych będący lub niebędący pracownikiem administratora danych, musi mieć możliwość wykonywania swoich funkcji w sposób całkowicie niezależny".

[20] Dyrektywa 95/46/WE w motywie 49 stanowi: „(...) urzędnik odpowiedzialny za ochronę danych będący lub niebędący pracownikiem administratora danych, musi mieć możliwość wykonywania swoich funkcji w sposób całkowicie niezależny"; w motywie 54: „(...) Państwa Członkowskie muszą zapewnić kontrolę przetwarzania danych przez organ nadzorczy lub **urzędnika odpowiedzialnego za ochronę danych, współpracującego z tym organem** [podkr. M.P.] przed ich

mu należy zagwarantować niezależność w realizacji zadań. Do jego obowiązków należeć powinno w szczególności zapewnienie stosowania u ADO przepisów prawa krajowego, przyjętych na mocy dyrektywy 95/46/WE, oraz prowadzenie rejestru operacji przetwarzania danych wykonywanych przez administratora danych (por. art. 18 ust. 1, 2, 4 i 5; art. 21 dyrektywy 95/46/WE). Ponieważ w polskiej ustawie o ochronie danych osobowych nie było dotychczas takich przepisów, chcąc zrealizować cel deregulacyjny, jakim było zwolnienie niektórych administratorów danych z obowiązku zgłaszania zbiorów danych, konieczne było zaimplementowanie tych postanowień dyrektywy 95/46/WE do przepisów krajowych. Warto zaznaczyć, że jej postanowienia w tej kwestii są dość ogólne i pozostawiają państwom członkowskim swobodę wyboru środków gwarantujących niezależność ABI oraz zasad prowadzenia rejestru.

3.2. Obowiązek powołania ABI przed nowelizacją ustawy

Omawiając kontekst nowelizacji, warto wspomnieć o orzeczeniu NSA z dnia 21 lutego 2014 r., dotyczącym powołania ABI przez administratorów danych niebędących osobami fizycznymi[21]. Ustawa o ochronie danych osobowych w wersji obowiązującej przed nowelizacją lakonicznie odnosiła się do tej funkcji. Mówił o niej jedynie art. 36 ust. 3 u.o.d.o. w brzmieniu sprzed deregulacji z 2014 r.[22], który stanowił, że: „Administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w ust. 1, chyba że sam wykonuje te czynności". Literalne brzmienie przepisu wskazywało, że zasadą jest powołanie ABI, chyba że ADO wykonuje obowiązki samodzielnie. Takie rozumienie zostało jednak zakwestionowane przez Google Poland sp. z o.o., która nie wyznaczyła do realizacji obowiązków ADO konkretnej osoby fizycznej. Podczas

przetworzeniem"; w art. 18 ust. 2: „(...) administrator danych, zgodnie z dotyczącymi go przepisami krajowymi, powoła urzędnika do spraw ochrony danych osobowych, odpowiedzialnego w szczególności: za zapewnienie w niezależny sposób wewnętrznego stosowania przepisów prawa krajowego przyjętych na mocy niniejszej dyrektywy; za prowadzenie rejestru operacji przetwarzania danych wykonywanych przez administratora danych i zawierających informacje określone w art. 21 ust. 2, zapewniając przy tym, że nie zostaną naruszone prawa i wolności osób, których dane dotyczą".

[21] Zob. wyrok NSA z dnia 21 lutego 2014 r., I OSK 2445/12, LEX nr 1438663.

[22] Ustawa z dnia 7 listopada 2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. poz. 1662 z późn. zm.).

postępowania przedstawiciele spółki argumentowali, że powołanie administratora bezpieczeństwa informacji jest jednym z dwóch przewidzianych ustawą sposobów zapewnienia zgodności z przepisami. Decyzja o powierzeniu wykonywania przewidzianych w ustawie o ochronie danych osobowych czynności ABI lub wykonywaniu ich samodzielnie należała, zdaniem spółki, do ADO. We wskazanym wyżej orzeczeniu NSA rozstrzygnął, że zgodnie z obowiązującym przed nowelizacją stanem prawnym wybór co do powołania ABI był zarezerwowany dla osób fizycznych. Zdaniem sądu art. 36 ust. 3 u.o.d.o. „nakłada na administratora danych obowiązek wyznaczenia («wyznacza») administratora bezpieczeństwa informacji w każdym przypadku, jeśli zadań administratora bezpieczeństwa informacji administrator danych nie wykonuje sam lub nie może wykonywać ich samodzielnie". W orzeczeniu stwierdzono też, że „nie powinno budzić wątpliwości, że w każdej sytuacji, w której struktura organizacyjna administratora danych jest wieloosobowa, powinien on w ramach tej struktury wyznaczyć osobę fizyczną odpowiedzialną za wykonywanie czynności nadzorczych, powierzając jej obowiązki administratora bezpieczeństwa informacji, i to niezależnie od tego, czy administrator danych jest organem, jednostką organizacyjną, podmiotem czy osobą prawną". Wyrok wykluczył ewentualne wątpliwości co do obowiązku powołania ABI przez administratorów danych, niebędących osobami fizycznymi. Status ABI pozostał jednak niedoprecyzowany i jedynie szczątkowo uregulowany w ustawie.

4. Zmiany wprowadzone nowelizacją

4.1. Dobrowolność powołania ABI

Nawiązując do przywołanego wyżej orzeczenia, należy uznać, że nowelizacja ustawy o ochronie danych osobowych odwróciła potwierdzone przez NSA wytyczne co do powoływania ABI. Usunęła ona bowiem przepis (ustęp 3 w art. 36 u.o.d.o.), wprowadzający wyjątek od wynikającej z kodeksu cywilnego reguły, że osoby prawne i jednostki organizacyjne niemające osobowości prawnej działają przez swoje organy, jeżeli innych reguł nie przyjmuje ustawa szczególna[23]. W efekcie także osoby prawne i jednostki organizacyjne

[23] W cytowanym wyżej wyroku NSA sąd uznał obowiązujący przed nowelizacją art. 36 ust. 3 u.o.d.o. za przepis szczególny, wprowadzający wyjątek od tej zasady kodeksowej.