STUDIA PRAWA PUBLICZNEGO
2020 • NR 2 (30) ISSN 2300-3936
DOI: 10.14746/spp.2020.2.30.6

Aleksandra Pyka*

Ocena skutków dla ochrony danych

Wprowadzenie

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[1] jest aktem normatywnym stosowanym od 25 maja 2018 r. przez państwa członkowskie Unii Europejskiej. Powołany akt normatywny wprowadził wiele zmian w dotychczasowym porządku prawnym. Przykładem tego jest zniesienie obowiązku notyfikacyjnego, a więc konieczności zgłaszania do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (obecnie kontynuatorowi GIODO – Prezesowi Urzędu Ochrony Danych Osobowych) zbiorów danych osobowych. Nowe ramy prawne zobowiązują administratorów do przeprowadzenia oceny skutków dla ochrony danych opartej na analizie ryzyka (ang. *risk-based approach*). Formą rozliczalności z realizacji tego zadania będzie DPIA (ang. *data protection impact assessment*), czyli ocena skutków dla ochrony danych osobowych. Warto przy tym nadmienić, że nie jest to zupełnie nowa koncepcja, która pojawia się w unijnym porządku prawnym[2]. Nie bez znaczenia pozostaje fakt, że Parlament Europejski określił ocenę skutków dla ochrony danych jako „zasadniczy rdzeń każdego zrównoważonego planu ochrony danych" („Impact assessments are the essential core of any sustainable

* Aleksandra Pyka, mgr, Katolicki Uniwersytet Lubelski Jana Pawła II, e-mail: pyka@kul.lublin.pl, https://orcid.org/0000-0003-2882-9614.

[1] Dz.Urz. UE L 119 z 4 V 2016 r., dalej „rozporządzenie ogólne".

[2] Szerzej: O. Lynskey, *The Foundations of EU Data Protection Law*, Oxford 2015, s. 81.

data protection framework")[3]. **Celem głównym niniejszego artykułu jest przedstawienie zagadnienia dokonywania oceny skutków dla ochrony danych przez administratorów, w szczególności uwzględniając problematyczną interpretację przepisów wynikającą z użycia przez prawodawcę unijnego wielu zwrotów niedookreślonych.**

1. Istota oceny skutków dla ochrony danych

Jak wynika z art. 35 ust. 1 rozporządzenia ogólnego, „jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę". Przeprowadzenie oceny skutków jest nieodzownie związane z analizą ryzyka wynikającego z operacji przetwarzania danych[4]. Nad uściśleniem definicji „wysokiego ryzyka" pracowała Grupa Robocza Art. 29 ds. Ochrony Danych, która w sposób niewiążący – poprzez wydanie opinii – określiła sposób interpretacji tego pojęcia. Niemniej konieczność przeprowadzenia oceny skutków będzie zależeć od takich determinantów, jak: charakter, zakres, kontekst i cel przetwarzania danych, co tym samym doprowadzi do maksymalnego zindywidualizowania oceny ryzyka w procesach przetwarzania danych osobowych. W myśl motywu 76 preambuły rozporządzenia ogólnego to właśnie do tych czynników należy się odnieść, analizując prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której

[3] Zob. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212#BKMD-6 (dostęp: 13 V 2020).

[4] Występowanie ryzyka jest nieodzownym elementem tzw. procesu PIA (ang. *Privacy Impact Assessment*). Według metodologii francuskiego organu ds. ochrony danych osobowych (CNIL) PIA spoczywa na dwóch filarach, a mianowicie na podstawowych prawach i zasadach niepodlegających żadnym negocjacjom (fr. *non négociables*) oraz na zarządzaniu ryzykiem związanym z ochroną prywatności osób, których dane dotyczą, co determinuje techniczne i organizacyjne środki kontroli w celu ochrony danych osobowych (fr. *les principes et droits fondamentaux, la gestion des risques sur la vie privée des personnes concernées*). Szerzej zob. https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf (dostęp: 10 V 2020).

dane dotyczą. W znacznej większości będzie się to odnosić do operacji lub zestawów operacji przetwarzania z użyciem nowych technologii (rozumianych stosunkowo szeroko – produktów, urządzeń etc.).

Wstępna analiza odpowiedzi udzielonych przez organy nadzorcze ds. ochrony danych w poszczególnych państwach członkowskich na pytania zawarte w kwestionariuszu Grupy Roboczej Art. 29 wskazuje na to, że w pewnych przypadkach organy te są zgodne, np. co do rodzaju danych, których przetwarzanie może wymagać przeprowadzenia oceny skutków dla ochrony danych. Do takich rodzajów danych zaliczyć można dane uwierzytelniające (ang. *credentials*), behawioralne (ang. *behavioural*), lokalizacyjne (ang. *location data*), finansowe (ang. *financial*) oraz specjalnych kategorii (ang. *special categories*) [tj. dane, o których mowa w art. 9 ust. 1 rozporządzenia ogólnego – dop. A.P.]. Dotychczas obowiązująca polska Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[5] nie posługiwała się przywołanymi pojęciami, niemniej można w niej wyodrębnić dane szczególnie chronione (wrażliwe/sensytywne) wskazane w art. 27 ust. 1. Warto przy tym zwrócić uwagę, że w świetle rozporządzenia ogólnego do różnych danych zaklasyfikować można jednocześnie te same dane osobowe. O takiej sytuacji mowa w odniesieniu do danych biometrycznych, które zgodnie z art. 9 ust. 1 omawianego aktu należą do szczególnej kategorii danych, a jednocześnie mogą być „wykorzystywane" jako dane uwierzytelniające (np. w sektorze bankowym w aplikacjach mobilnych dla klientów z biometrycznym dostępem), czy też jako dane behawioralne (np. identyfikacja osoby na podstawie sposobu poruszania się w systemie nadzoru wizyjnego).

Ocena ryzyka jest nieodzownym elementem DPIA. Niewykluczone, że administratorzy będą sugerować się m.in. także opiniami Grupy Roboczej Art. 29 ds. Ochrony Danych, jako niezależnego podmiotu o charakterze doradczym, w zakresie zasadności przeprowadzania oceny skutków dla ochrony danych osobowych, czy też Europejskiej Rady Ochrony Danych. Posiłkowanie się opiniami lub wytycznymi wyżej wskazanych podmiotów może być korzystnym rozwiązaniem dla administratorów. Wspomniane opinie lub wytyczne nie mają co prawda charakteru wiążącego, lecz odznaczają się sporym stopniem fachowości. Można wskazać, że Grupa Robocza Art. 29 nierzadko podkreślała w swoich opiniach konieczność przeprowadzenia choćby oceny ryzyka przed rozpoczęciem przetwarzania danych. Jak bowiem wynika z opinii

[5] Tekst jedn. Dz.U. 2016, poz. 922.

5/2012 Grupy Roboczej Art. 29 ds. Ochrony Danych przyjętej w dniu 1 lipca 2012 r. w sprawie przetwarzania danych w chmurze obliczeniowej, „w konsekwencji warunkiem wstępnym polegania na rozwiązaniach *cloud computingu* jest przeprowadzenie przez administratora odpowiedniej oceny ryzyka, obejmującej lokalizację serwerów, gdzie przetwarzane są dane, oraz rozważenie zagrożeń i korzyści z perspektywy ochrony danych […]"[6].

1.1. Pojęcie „wysokiego ryzyka"

Odnosząc się do literalnego brzmienia definicji ryzyka zawartej w słowniku języka polskiego, pod pojęciem tym należy rozumieć „możliwość, że coś się nie uda; też przedsięwzięcie, którego wynik jest niepewny", czy też „odważenie się na takie niebezpieczeństwo"[7]. Biorąc jednak pod uwagę, że niniejszy artykuł dotyczy tematyki ochrony danych osobowych, warto odnieść się przy tym do definicji ryzyka zawartych w normach technicznych ISO, w tym ISO 27001 (tj. normach zapewniających kompleksowe podejście do zagadnienia bezpieczeństwa informacji)[8]. W piśmiennictwie podkreśla się różnorodność znaczeniową tego pojęcia, jaka występuje w przywołanych normach[9]. Z kolei według norm PN-I-02000:2002-3.1.096 oraz PN-ISO/IEC 2382-8:2001-08.05.09 ryzyko to „możliwość, że konkretne zagrożenie wykorzysta konkretną podatność systemu przetwarzania danych". Ponadto norma ISO 31000:2009 definiuje ryzyko jako „skutek niepewności do ustalonych celów"[10]. Ta niespójność w siatce pojęciowej odnośnie do znaczenia ryzyka wynika przede wszystkim z rozbieżnych zakresów wskazanych norm.

Rozporządzenie ogólne wprowadza gradację występującego w operacjach lub zestawach operacji przetwarzania ryzyka na: „ryzyko" i „wysokie ryzyko". Przykładowo, jak stanowi motyw 76 preambuły rozporządzenia ogólnego, „[r]yzyko należy oszacować na podstawie ww. obiektywnej oceny, w ramach której stwierdza się, czy z operacjami

[6] Opinia 5/2012 z dnia 1 VII 2012 r. (01037/12/PL, WP 196).

[7] Hasło „Ryzyko", http://sjp.pwn.pl/sjp/ryzyko;2518509.html (dostęp: 10 V 2020).

[8] Są to normy techniczne określające standardy w zakresie bezpieczeństwa informacji ustanowione przez Międzynarodową Organizację Normalizacyjną (ang. *International Organization for Standardization* – ISO).

[9] D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016, s. 35.

[10] Ibidem.

przetwarzania danych wiąże się ryzyko lub wysokie ryzyko". DPIA powinno być przeprowadzone wówczas, gdy operacja przetwarzania wiązać się będzie nierozerwalnie z zaistnieniem „dużego prawdopodobieństwa" wystąpienia wysokiego ryzyka naruszenia praw lub wolności podmiotów danych. Niemniej biorąc pod uwagę, że nie każda operacja wiąże się z istnieniem prawdopodobieństwa – w stopniu wysokim – naruszenia praw i wolności podmiotów danych, warto przy tym wyodrębnić także pojęcie „niskiego ryzyka". Określenie takie nie wynika wprost z treści przepisów rozporządzenia ogólnego, ale pojawiło się już w piśmiennictwie. Jak wskazują przedstawiciele doktryny, „identyfikuje się ją [kategorię niskiego ryzyka – dop. A.P.] na podstawie sformułowań art. 27 ust. 2 lit. a) oraz art. 33 ust. 1 rozporządzenia 2016/679"[11].

Nawiązując do zwrotu „wysokiego ryzyka naruszenia praw lub wolności osób fizycznych", należy nadmienić, że przeprowadzenie DPIA nie będzie się odnosiło wyłącznie do przypadków prawdopodobnego zaistnienia wysokiego ryzyka naruszenia wyłącznie prawa do prywatności, którego emanacją jest w polskim porządku prawnym art. 47 Konstytucji Rzeczypospolitej Polskiej[12] stanowiący, że „każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym". Jak bowiem wynika z opinii 07/2013 Grupy Roboczej Art. 29 ds. Ochrony Danych w sprawie szablonu oceny skutków w zakresie ochrony danych na potrzeby inteligentnych sieci i inteligentnych systemów pomiarowych, opracowanego przez grupę ekspertów nr 2 w ramach grupy zadaniowej Komisji ds. inteligentnych sieci, „w przypadku gdy w szablonie [oceny skutków – dop. A.P] stosowana jest odmienna terminologia, np. odnosząca się jedynie do prawa do prywatności, trzeba ją interpretować jako odniesienie do bardziej kompleksowego pojęcia"[13]. Abstrahując w powyższym od kwestii samego szablonu, należy podkreślić, że stwierdzenie to oznacza tym samym, iż przeprowadzenie DPIA powinno określać szacunkowe – wymierne – skutki przetwarzania danych, jak chociażby straty finansowe, dyskryminację cenową, czy też – jak wskazuje się w przywołanej opinii – przestępstwa ułatwione przez nieupoważnione profilowanie.

[11] A. Mednis, *Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych*, „Monitor Prawniczy" 2016, nr 20: *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, pod red. G. Sibigi, s. 29.

[12] Konstytucja Rzeczypospolitej Polskiej z dnia 2 IV 1997 r. (Dz.U. Nr 78, poz. 483 ze zm.).

[13] Opinia 7/2013 z dnia 4 XII 2013 r. (2064/13/PL WP209).

Jak stanowi motyw 75 preambuły rozporządzenia ogólnego, „ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze zagrożeń, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności: jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną; jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i czynów zabronionych lub związanych z tym środków bezpieczeństwa; jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych; lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą". Ryzyko przetwarzania danych może wiązać się z naruszeniem innych praw podmiotów, a nie tylko prawa do prywatności. Administrator powinien zatem przeanalizować ostateczne skutki planowanych (czy też rozpoczętych) operacji lub zestawów operacji przetwarzania dla praw i wolności osób, których dane będzie przetwarzać, bądź też już przetwarza.

1.2. Obligatoryjne przeprowadzenie DPIA

Rozporządzenie ogólne wprowadza otwarty katalog operacji, które powinny zostać poddane ocenie skutków dla ochrony danych. W przypadkach takich rodzajów operacji przetwarzania DPIA nie może mieć charakteru uznaniowego. Operacją taką będzie np. „systematyczna,

kompleksowa ocena czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną" (art. 35 ust. 3 lit. a). Do takich operacji należy zaliczyć ponadto ocenę i scoring (w tym tzw. *credit scoring*[14]), a wśród nich m.in. wskazane wyżej profilowanie. W przypadku czynności profilowania należy odnieść się do definicji zawartej w art. 4 pkt 4 rozporządzenia ogólnego, zgodnie z którą „profilowanie oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się". Z kolei w motywie 71 preambuły rozporządzenia ogólnego dodaje się do powyższej definicji, że ta ocena czynników osobowych osoby, której dane dotyczą, ma miejsce, o ile wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa. Profilowanie nierzadko jest stosowane w procesach tworzenia reklam skierowanych (ang. *targeted ads*)[15], w prognozowaniu sprzedaży (ang. *sales forecast*), czy też w związku z wdrażaniem strategii *cross-selling*[16].

Ponadto administrator jest zobowiązany przeprowadzać ocenę skutków dla ochrony danych w odniesieniu do operacji przetwarzania na dużą skalę szczególnych kategorii danych, czy też danych dotyczących wyroków skazujących i czynów zabronionych oraz systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie (art. 35 ust. 2 lit. b i c rozporządzenia ogólnego). Do szczególnych kategorii danych osobowych zalicza się dane ujawniające pochodzenie rasowe

[14] Jest to metoda oceny ryzyka kredytowego odnosząca się do określonego wnioskodawcy, zgodnie z którą metodą punktową przyznaje się określonym zmiennym (m.in. zawód, wykształcenie, staż pracy, stan cywilny, wiek) punkty. Całość stanowi względnie miarodajną ocenę ryzyka zaistniałego w przypadku udzielenia kredytu przez instytucję finansową.

[15] Zob. R. Maciąg, *Reklama w Internecie*, w: *Zarządzanie reklamą*, pod red. B. Nierenberga, Kraków 2015, s. 142.

[16] Zwiększanie liczby transakcji w sektorze bankowym (ściślej, internetowych usługach bankowych) następuje często w wyniku personalizacji klientów (wynikającej z profilowania tej grupy osób), a następnie wdrażania odpowiednich strategii, takich jak *cross-selling*. Zob. E. Guzek, E. Ślęzak, *Innowacyjna bankowość internetowa. Bank Web 2.0*, Warszawa 2012, s. 29.

lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia oraz dane dotyczące seksualności lub orientacji seksualnej podmiotu danych, przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej (art. 9 ust. 1 rozporządzenia ogólnego). Warto nadmienić, że pojęcie przetwarzania danych szczególnych kategorii „na dużą skalę" może mieć wydźwięk dychotomiczny – odnosić się zarówno do ilości przetwarzanych danych, jak i liczby osób, których dane są przetwarzane, bądź też rozumianych łącznie.

Z kolei nawiązując do kwestii systematycznego monitorowania, należy odnieść się choćby do pojęcia reklamy behawioralnej. W świetle opinii 2/2010 Grupy Roboczej Art. 29 ds. Ochrony Danych przyjętej 22 czerwca 2010 r. w sprawie internetowej reklamy behawioralnej pod pojęciem reklamy behawioralnej należy rozumieć „monitorowanie użytkowników podczas korzystania z Internetu i tworzenie z biegiem czasu profili, wykorzystywanych następnie w celu wyświetlania użytkownikom reklam odpowiadających ich zainteresowaniom"[17].

Motyw 93 preambuły rozporządzenia ogólnego stanowi, że „przyjmując prawo, które ma być dla organu lub podmiotu publicznego podstawą do wykonywania zadań i ma regulować konkretną operację przetwarzania lub konkretny zestaw operacji, państwa członkowskie mogą uznać, że przed takimi czynnościami przetwarzania należy koniecznie przeprowadzić taką ocenę [skutków dla ochrony danych – dop. A.P.]". Prawodawca unijny pozostawia tym samym w gestii ustawodawstw krajowych (klauzula *option and choices*) możliwość zobligowania organów bądź podmiotów publicznych do przeprowadzenia DPIA w odniesieniu do skonkretyzowanych operacji przetwarzania (ograniczenie podmiotowo-przedmiotowe, a więc dotyczące określonego organu/podmiotu publicznego i określonego procesu przetwarzania).

1.3. Wykazy rodzajów operacji przetwarzania

Prawodawca unijny zobowiązał jednocześnie krajowe organy nadzorcze do ustanowienia oraz podania do publicznej wiadomości wykazu rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków.

[17] Opinia 2/2010 z dnia 22 VI 2010 r. (00909/10/PL, WP 171).

Klauzula *option and choices* zawarta w art. 35 ust. 5 rozporządzenia ogólnego stanowi, że „Organ nadzorczy może także ustanowić i podać do wiadomości publicznej wykaz rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych". Sporządzenie wykazu operacji przetwarzania niepodlegających procedurze DPIA (odwołując się do przywołanego przepisu) prawodawca unijny pozostawia do rozważenia krajowym organom nadzorczym (pozostaje to w gestii organu nadzorczego, a nie krajowego ustawodawcy), a zatem ustanowienie takiego wykazu ma wyłącznie charakter fakultatywny i uznaniowy. Omówione powyżej wykazy operacji lub zestawów operacji przetwarzania są dla administratora wyznacznikiem co do konieczności (czy też zwolnienia z tego obowiązku) przeprowadzenia DPIA. Nie oznacza to jednak, że administrator nie musi samodzielnie dokonywać analizy dotyczącej zasadności przeprowadzenia oceny skutków dla ochrony danych.

1.4. Forma i zakres DPIA

Wprawdzie prawodawca unijny nie przesądza o formie DPIA ani o konieczności określenia przez ustawodawcę wzorca szablonu stanowiącego dowód przeprowadzenia oceny skutków przez administratora, jednak taka możliwość nie jest wykluczona. W rozporządzeniu nie zastrzeżono *explicite* formy pisemnej, lecz zasadne wydaje się twierdzenie, że taka forma przeprowadzenia oceny skutków dla ochrony danych powinna być zachowana *ad probationem.*

Trzeba wszakże zwrócić uwagę na zakres DPIA, który został wyodrębniony w art. 35 ust. 7 rozporządzenia ogólnego. Zgodnie z tym przepisem „Ocena zawiera co najmniej: systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora (lit. a); ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów (lit. b); ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1 (lit. c); oraz środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych

interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy (lit. d)". Zakres DPIA został przez prawodawcę unijnego określony w sposób absolutnie minimalny, a tym samym w rozporządzeniu ogólnym nie zawarto wszystkich dopuszczalnych elementów oceny skutków, o które można uzupełnić szablon.

Istotne znaczenie przy przeprowadzaniu DPIA będzie mieć przestrzeganie przez administratora, bądź też podmiot przetwarzający, kodeksów postępowania (art. 35 ust. 8 rozporządzenia ogólnego) zatwierdzonych w ramach procedury, o której mowa w art. 40 ust. 5 rozporządzenia. Ponadto prawodawca unijny wskazał na możliwość zasięgnięcia „opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania". Niemniej warto dodać, że samo wyrażenie „w stosownych przypadkach" użyte w powyższej normie prawnej (art. 35 ust. 9) jest zwrotem niedookreślonym i ocennym. Tym samym administrator przeprowadzający ocenę skutków dla ochrony danych będzie w sposób selektywny, w bliżej nieokreślonych sytuacjach zwracać się do podmiotów danych o wyrażenie opinii odnośnie do planowanego procesu, przy czym nie wskazuje się, aby opinia ta miała charakter wiążący, czy też stanowiła *conditio sine qua non* poprzedzający rozpoczęcie planowanej operacji przetwarzania.

Odnosząc się z kolei do formy „komunikowania się" z organem nadzorczym, tj. w przypadku zaistnienia przesłanek z art. 36 ust. 1 rozporządzenia ogólnego, a więc dotyczących uprzednich konsultacji (ang. *prior checking*) po przeprowadzonym DPIA, należy optować za zachowaniem jak dotychczas (w przypadku rejestracji zbiorów danych osobowych i ABI) zarówno formy „pisemnej", jak i elektronicznej. Te formy komunikacji powinny funkcjonować alternatywnie.

1.5. Wyłączenie przeprowadzenia DPIA

W myśl art. 35 ust. 10 rozporządzenia ogólnego nie ma konieczności przeprowadzania oceny skutków, jeżeli przesłanką legalizującą przetwarzanie jest art. 6 ust. 1 lit. c rozporządzenia ogólnego (tj. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze), czy też art. 6 ust. 1 lit. e tegoż aktu (tj. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie

publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi). Niemniej należy przy tym nadmienić, że jest to „podstawa prawna w prawie Unii Europejskiej lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych". Tym samym już na etapie prac legislacyjnych warto byłoby brać pod uwagę rozważenie przeprowadzenia oceny skutków dla ochrony danych planowanych operacji lub zestawów operacji przetwarzania, które będą miały swą podstawę w konkretnym przepisie prawa.

2. Minimalizowanie ryzyka w procesie przetwarzania

Pojęcie oceny ryzyka (ang. *risk assessment*) wynikającego z przetwarzania danych nie jest instytucją nieznaną zarówno dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych[18] (dalej „dyrektywa 95/46/WE"), jak i Ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Polska ustawa nie operowała określeniem „analizy/oceny/szacowania ryzyka", jak się jednak wskazuje w piśmiennictwie, „wynikający z art. 36 ust. 1 UODO obowiązek odpowiedniej ochrony obejmuje […] także elementy oceny i zarządzania ryzykiem"[19]. DPIA nie jest jednak instrumentem *pro forma*, lecz ma służyć weryfikacji ryzyka, jego minimalizowaniu oraz zapewnieniu bezpieczeństwa danych.

Jak wskazują przedstawiciele doktryny, „[z]adania te [dotyczące zapewnienia ochrony przetwarzanych danych – dop. A.P.] powinny być zrealizowane przez zastosowanie odpowiednich, należy przez to rozumieć: skutecznych, środków technicznych i organizacyjnych. Ustawodawca nie przesądza, jakie to mają być środki. Mogą być one różnego rodzaju, od rozwiązań architektoniczno-budowlanych przez systemy alarmowe i służby ochrony aż po środki technicznego i czysto informatycznego charakteru (karty chipowe, kody dostępu, systemy

[18] Dz.Urz. WE L 281 z 23 XI 1995 r.

[19] A. Drozd, *Zabezpieczenie danych osobowych*, Wrocław 2008, s. 33.

kodujące i przeciwdziałające hakerstwu)"[20]. Szczegółowe kwestie dotyczące spełnienia wymagań w zakresie bezpieczeństwa przetwarzania danych zostały uregulowane w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 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[21]. Rozporządzenie ogólne nie przewiduje możliwości wprowadzenia aktów wykonawczych, które regulowałyby odrębnie kwestię stosowania odpowiednich środków technicznych.

Jednocześnie warto zwrócić uwagę na dyskusyjną kwestię dotyczącą tego, czy istotnie ustawodawca nie może w żaden sposób przesądzić o „trafności" środków organizacyjnych i technicznych wdrożonych przez administratora w celu minimalizowania ryzyka. Prawodawca unijny co prawda zobowiązuje zarówno administratora, jak i podmiot przetwarzający do wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia (art. 32 ust. 1 rozporządzenia ogólnego), nie określa jednak w żaden sposób – także poprzez instrumenty *soft law* – o jakich to środkach należy mówić. Nie oznacza to tym samym, że nie pozostawia się ustawodawstwom krajowym pewnej „swobody legislacyjnej", a więc możliwości odmiennego uregulowania tej kwestii w drodze aktów normatywnych na szczeblu państw członkowskich. Dla przykładu warto odnieść się choćby do Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[22]. Ten akt wykonawczy określa m.in. minimalne wymagania dla systemów teleinformatycznych, w tym sposoby zapewnienia bezpieczeństwa przy wymianie informacji oraz standardy techniczne zapewniające wymianę informacji z udziałem podmiotów publicznych z uwzględnieniem wymiany transgranicznej (§ 1 pkt 3 lit. b i c). Co szczególnie istotne, należy wskazać, że omawiane rozporządzenie posługuje się pojęciami

[20] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2015, s. 546.

[21] Dz.U. Nr 100, poz. 1024.

[22] Dz.U. 2012, poz. 526.

„szacowania ryzyka" i „analizy ryzyka", np. – jak stanowi § 20 ust. 2 pkt 3 wyżej wskazanego rozporządzenia Rady Ministrów – „zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy".

W art. 32 ust. 1 rozporządzenia ogólnego wprowadzono jedynie enumeratywny katalog środków mających na celu zapewnienie adekwatnego stopnia bezpieczeństwa danych w odniesieniu do stopnia ryzyka, a mianowicie: pseudonimizację danych i szyfrowanie danych osobowych; zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania[23]; zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznych oraz regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania (art. 32 ust. 1 lit. a–d rozporządzenia ogólnego). Ponadto, jak wynika z art. 32 ust. 2 rozporządzenia ogólnego, „oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych".

Za prawodawcą unijnym należy wskazać, iż potwierdzeniem wywiązania się przez administratora i podmiot przetwarzający z obowiązku wdrożenia odpowiednich środków organizacyjnych i technicznych zapewniających bezpieczeństwo danych mogą być m.in. zatwierdzone kodeksy postępowania (art. 40 rozporządzenia ogólnego), bądź też zatwierdzone mechanizmy certyfikacji (art. 42 rozporządzenia ogólnego). W myśl motywu 77 preambuły rozporządzenia ogólnego „wskazówki

[23] W omawianej regulacji prawodawca unijny nawiązuje częściowo do nomenklatury norm ISO. Dla przykładu warto wskazać, że zgodnie z normą PN-ISO/IEC-17799:2005 „przez bezpieczeństwo informacji należy rozumieć zachowanie poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności". Zob. *ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych*, pod red. A. Rudnickiego, Warszawa 2007, s. 6.

co do tego, jak wdrożyć odpowiednie środki oraz wykazać przestrzeganie prawa przez administratora lub podmiot przetwarzający dane – w szczególności jeżeli chodzi o identyfikowanie ryzyka związanego z przetwarzaniem, o jego ocenę pod kątem źródła, charakteru, prawdopodobieństwa i wagi zagrożenia oraz o najlepsze praktyki pozwalające zminimalizować to ryzyko – mogą być przekazane w szczególności w formie zatwierdzonych kodeksów postępowania, zatwierdzonej certyfikacji, wytycznych Europejskiej Rady Ochrony Danych lub poprzez sugestie inspektora ochrony danych".

3. Ocena skutków dla ochrony danych a uprzednie konsultacje

Prawodawca unijny w motywie 84 preambuły rozporządzenia ogólnego wskazał, że „aby poprawić przestrzeganie niniejszego rozporządzenia, gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, należy zobowiązać administratora do dokonania oceny skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka. Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z niniejszym rozporządzeniem. Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego administrator nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed przetwarzaniem należy skonsultować się z organem nadzorczym". W myśl art. 36 ust. 1 rozporządzenia ogólnego administrator będzie zobowiązany przed rozpoczęciem przetwarzania skonsultować się z organem nadzorczym ds. ochrony danych w przypadku, gdy dokonana przez niego ocena wykaże, że planowane operacje przetwarzania będą się wiązać z zaistnieniem wysokiego stopnia ryzyka i nie zastosowano odpowiednich środków mających na celu jego zminimalizowanie. Literalne brzmienie tego artykułu stanowi o konieczności przeprowadzenia konsultacji z organem nadzorczym przed rozpoczęciem przetwarzania, niemniej jak wynika z motywu 89 preambuły rozporządzenia ogólnego – stanowiącego integralną część tego aktu normatywnego – „takie rodzaje operacji przetwarzania [mogących powodować wysokie ryzyko naruszenia praw lub wolności

osób fizycznych – dop. A.P.] obejmują w szczególności operacje, które wiążą się w szczególności z użyciem nowych technologii lub które są nowe i nie zostały jeszcze poddane przez administratora ocenie skutków dla ochrony danych lub stały się niezbędne z uwagi na upływ czasu od pierwotnego przetwarzania". Prawodawca unijny nie zwalnia więc administratorów, którzy będą już przetwarzać dane przed rozpoczęciem stosowania rozporządzenia ogólnego, z obowiązku dokonania oceny skutków.

Fakt dokonania zgłoszenia zbioru do rejestracji GIODO przed rozpoczęciem stosowania rozporządzenia ogólnego w żadnym wypadku nie wpłynie na przeprowadzenie DPIA, do czego będzie zobowiązany administrator w świetle obowiązujących ram prawnych. Oznacza to, że nowy reżim prawny nie pozostawił „w próżni" procesów przetwarzania danych, które ze względu na wysokie ryzyko mogły stanowić zagrożenie dla ochrony praw lub wolności jednostek, a wynikające z operacji lub zestawów operacji przetwarzania rozpoczętych przed 25 maja 2018 r. Uprzednie konsultacje z organem nadzorczym nie mają jedynie charakteru pisemnych zaleceń, w ich toku bowiem organ może skorzystać z uprawnień wynikających z art. 58 rozporządzenia ogólnego. W swojej treści odnosić się mogą m.in. do środków i zabezpieczeń bądź oceny skutków dla ochrony danych. Organ nadzorczy może nakazać administratorowi lub podmiotowi przetwarzającemu dostosowanie operacji przetwarzania do przepisów rozporządzenia ogólnego (w przypadku gdy ocena skutków dotyczy operacji przetwarzania), czy też wydać ostrzeżenie dotyczące możliwości naruszenia tego rozporządzenia (planowane operacje przetwarzania).

4. Rola inspektora ochrony danych w przeprowadzeniu oceny skutków dla ochrony danych

Oszacowanie ryzyka wynikającego z przetwarzania danych z jednoczesnym jego minimalizowaniem poprzez dostosowanie odpowiednich środków bezpieczeństwa stanowi obowiązek administratora. Tym samym administrator nie może scedować odpowiedzialności za realizację tego zadania na wyznaczonego inspektora ochrony danych. Warto jednak dodać na marginesie, że nie jest wykluczone zlecenie przeprowadzenia DPIA inspektorowi ochrony danych, podmiotowi wewnętrznemu (osoby znajdujące się w strukturze organizacyjnej administratora), czy

też nawet podmiotowi zewnętrznemu. Dla potwierdzenia słuszności tej tezy należy nadmienić, że prawodawca unijny podkreślił w art. 35 ust. 2 rozporządzenia ogólnego, iż „dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony", co stanowi jedną z form faktycznego realizowania funkcji doradczej inspektora – równie istotnej jak nadzorowanie i monitorowanie. Należy przy tym nadmienić, że obligatoryjne przeprowadzenie oceny skutków może nastąpić niezależnie od konieczności wyznaczenia inspektora[24]. Prawodawca unijny wskazał wśród zadań inspektora ochrony danych m.in. „udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35"[25]. Jak stanowi dokument Grupy Roboczej Art. 29 ds. Ochrony Danych, w którym zawarto wytyczne dotyczące inspektorów ochrony danych (DPO) przyjęte w dniu 13 grudnia 2016 r., „artykuł 39 ust. 2 nakłada na DPO obowiązek wypełniania swoich zadań z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania. […] Wymaga [ten przepis – dop. A.P.] od DPO ustalania priorytetów w swojej pracy i koncentrowania się na aspektach pociągających za sobą większe ryzyko. Nie oznacza to, iż dozwolone jest zaniedbywanie kontroli zgodności operacji przetwarzania danych o niższym ryzyku, a jedynie wskazuje słuszność skupienia się, przede wszystkim, na kwestiach o wyższym ryzyku. To selektywne i pragmatyczne podejście powinno ułatwić DPO doradzanie administratorowi, jaką metodologię należy zastosować przy przeprowadzaniu oceny skutków dla ochrony danych, które obszary powinny zostać poddane wewnętrznemu albo zewnętrznemu audytowi, jakie szkolenia wewnętrzne przeprowadzić dla pracowników lub kierowników odpowiedzialnych za przetwarzanie danych i na które operacje przetwarzania przeznaczyć więcej czasu i zasobów"[26].

5. DPIA a zasada rozliczalności

Przeprowadzenie oceny skutków dla procesów przetwarzania co do zasady nie jest obowiązkowe, o ile nie sposób zaklasyfikować przetwarzania

[24] Por. art. 35 ust. 3 i art. 37 ust. 1 rozporządzenia ogólnego.
[25] Artykuł 39 ust. 1 lit. c rozporządzenie ogólnego.
[26] Wytyczne dotyczące inspektorów ochrony danych ('DPO'),16/EN WP 243.

danych do katalogu enumeratywnego z art. 35 ust. 3 rozporządzenia ogólnego, czy też operacja taka nie będzie znajdować się w wykazie ustanowionym przez organ nadzorczy.

Już w opinii 3/2010 Grupy Roboczej Art. 29 ds. Ochrony Danych przyjętej w dniu 13 lipca 2010 r. w sprawie zasady rozliczalności wskazywano, że „w uzupełnieniu do tej zasady [rozliczalności – dop. A.P.] można byłoby ustanowić szczególne wymagania dodatkowe mające na celu wprowadzenie w życie zabezpieczeń w zakresie ochrony danych lub zapewnienie ich skuteczności. Jednym z przykładów może być przepis wymagający przeprowadzenia oceny skutków w zakresie ochrony prywatności dla operacji przetwarzania danych o podwyższonym ryzyku"[27]. Co prawda w powyższej opinii wykazywano zasadność wprowadzenia zasady rozliczalności do dyrektywy 95/46/WE, niemniej istotne jest, że ostatecznie zobowiązano administratora do wykazania przestrzegania m.in. zasady integralności i poufności danych.

Podkreśla się przy tym, że administratorzy powinni stosować rzeczywiste i efektywne „instrumenty" ochrony danych w celu zminimalizowania ryzyka naruszenia praw i wolności podmiotów danych. Do takich środków można zaliczyć np. środki ochrony fizycznej, środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej, środki ochrony w ramach narzędzi programowych i baz danych czy środki organizacyjne. To na administratorze spoczywa w pełni obowiązek przestrzegania zasad dotyczących przetwarzania danych osobowych, a także wykazanie jego spełniania.

6. Kompetencje organu nadzorczego

Rozporządzenie ogólne wyodrębnia także zakres zadań i uprawnień organów nadzorczych (Rozdział VI. Niezależne organy nadzorcze), które powinny być realizowane bez uszczerbku dla pozostałych, wymienionych w tymże akcie normatywnym. Spośród uprawnień wyodrębnia się naprawcze (ang. *corrective powers*), uprawnienia w zakresie prowadzonych postępowań (ang. *investigative powers*), a także uprawnienia w zakresie wydawania zezwoleń i uprawnienia doradcze (ang. *authorisation*

[27] Opinia 3/2010 z dnia 13 VII 2010 r., 00062/10/PL, WP173.

and advisory powers). Z poszczególnych „prerogatyw" organ nadzorczy może także skorzystać w odniesieniu do administratora przeprowadzającego DPIA.

Ocena skutków dla ochrony danych w myśl art. 35 ust. 1 rozporządzenia ogólnego co do zasady odnosić się ma do planowanych (tj. nierozpoczętych) operacji lub zestawów operacji przetwarzania. Dla przykładu warto wskazać, że krajowy organ nadzorczy jest uprawniony m.in. do prowadzenia postępowania w formie audytu ochrony danych, w wyniku którego może powziąć informację o tym, że administrator obowiązany do przeprowadzenia DPIA, bądź to na podstawie art. 35 ust. 1 lub 3, bądź w związku z planowaną operacją przetwarzania znajdującą się w wykazie z art. 35 ust. 4, nie dokonał oceny skutków dla ochrony danych. Tym samym w ramach prowadzonego postępowania organ nadzorczy jest uprawniony do wydania administratorowi ostrzeżenia dotyczącego możliwości naruszenia przepisów rozporządzenia poprzez planowane operacje przetwarzania. Zdaniem autora nie wyklucza się możliwości korzystania przez krajowe organy nadzorcze z uprawnień wymienionych w art. 58 rozporządzenia ogólnego wyłącznie na etapie uprzednich konsultacji (poprzedzonych oceną skutków wykazującą wysokie ryzyko zamierzonych operacji lub zestawów operacji przetwarzania), lecz także już na etapie przeprowadzania DPIA (m.in. nakazanie administratorowi dostarczenia wszelkich informacji potrzebnych organowi nadzorczemu do realizacji jego zadań).

Podsumowanie

DPIA można postrzegać zarówno jako skuteczny instrument weryfikowania ryzyka w operacjach lub zestawach operacji przetwarzania, jak i mechanizm ochronny dla administratora – stanowiący po części dowód przestrzegania ram prawnych ochrony danych osobowych. Nie jest to *novum*, lecz dopiero w rozporządzeniu ogólnym podkreśla się znaczącą rolę oceny skutków dla ochrony danych. Można się pokusić o stwierdzenie, że ocena skutków dla ochrony danych jest nowym obowiązkiem administratora, który ma skutecznie zastąpić dotychczas istniejący obowiązek notyfikacyjny (uciążliwy i nieskuteczny w dobie tak szybkiego rozwoju nowych technologii). O efektywności tego rozwiązania można będzie zapewne mówić dopiero z perspektywy czasu.

Niemniej Parlament Europejski podkreśla doniosłe znaczenie DPIA, dodając przy tym, że dokładnie przeprowadzona ocena skutków może się przyczynić do zasadniczego ograniczenia naruszeń w procesach przetwarzania danych.

DATA PROTECTION IMPACT ASSESSMENT

Summary

This article deals with the issue of impact assessment for the protection of personal data. This is a new obligation for the controller. The article presents the essence of impact assessment (DPIA), exclusion from the obligation to carry it out, the prerequisite for mandatory DPIA, the role of the data protection officer and the powers of the supervisory authority. The analysis of legal provisions related to the impact assessment presented here does not refer to specific situations, due to the wide scope for interpreting specific phrases contained in the General Regulation. Nevertheless, the article discusses the issue of conducting data protection impact assessments as one of the most problematic obligations incumbent on the controller, who in practice raises many doubts. The DPIA has been imprecisely regulated by the EU legislator, thus leaving controllers plenty of leeway to interpret the terms used in the General Regulation. In addition, carrying out a DPIA in practice (as a new obligation on entities setting the purposes and means of data processing) can be problematic due to the lack of harmonized methods for conducting a data protection impact assessment. However, controllers cannot assign DPIA implementation to other entities involved in data processing, such as an entity processing personal data on behalf of another. Entities setting the purposes and methods of data processing should not only take into account the provisions of the General Regulation but also a list of data processing operations that are obligatorily subject to DPIA. Controllers fulfilling the obligation to carry out a data protection impact assessment will be obliged by the supervisory authority to demonstrate how to carry out a data protection impact assessment.

Keywords: data protection impact assessment – DPIA – data controller – risk – personal data

LITERATURA

ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych, pod red. A. Rudnickiego, Warszawa 2007.

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Warszawa 2015.

Drozd A., *Zabezpieczenie danych osobowych*, Wrocław 2008.

Guzek E., Ślęzak E., *Innowacyjna bankowość internetowa. Bank Web 2.0*, Warszawa 2012.
Lisiak-Felicka D., Szmit M., *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016.
Lynskey O., *The Foundations of EU Data Protection Law*, Oxford 2015.
Maciąg R., *Reklama w Internecie*, w: *Zarządzanie reklamą*, pod red. B. Nierenberga, Kraków 2015, s. 131–142.
Mednis A., *Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych*, „Monitor Prawniczy" 2016, nr 20: *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, pod red. G. Sibigi.