t. LXXV • nr 10/2022 (892) • DOI 10.33226/0137-5490.2022.10.4

Dr inż. Krzysztof Świtała

Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
ORCID: 0000-0003-0426-5383
e-mail: k.switala@uksw.edu.pl

Obowiązki organizacyjne administratorów danych osobowych i operatorów usług kluczowych — wnioski *de lege lata* i postulaty *de lege ferenda*

Organizational responsibilities of personal data controllers and essential services operators — *de lege lata* conclusions and *de lege ferenda* postulates

Streszczenie

W artykule poddano analizie zagadnienia związane z realizacją obowiązków organizacyjnych przez administratorów danych osobowych i operatorów usług kluczowych odnoszące się do stosowania podejścia opartego na ryzyku, ciągłego doskonalenia i ochrony prywatności w fazie projektowania, budowania wewnętrznych struktur organizacyjnych odpowiedzialnych za system zarządzania bezpieczeństwem przetwarzanych informacji, a także roli dokumentacji strategicznej i operacyjnej, stosowania samoregulacji i normalizacji w celu zwiększenia skuteczności stosowania prawa. Duża dynamika rozwoju technologii informacyjno-komunikacyjnych i powiązanych z ich wykorzystywaniem procesów biznesowych wymaga zastosowania dającego synergię, spójnego i interdyscyplinarnego podejścia do zapewniania ochrony danych osobowych i cyberbezpieczeństwa. Istotne znaczenie ma także elastyczność stosowanych rozwiązań zabezpieczających, pozwalająca na optymalną adaptację do cyklicznych zmian w otoczeniu gospodarczym i prawnym. Podstawowym celem artykułu jest analiza spójności i skuteczności regulacji prawa polskiego i UE w obszarze zapewniania bezpieczeństwa informacyjnego procesów przetwarzania danych, ze szczególnym uwzględnieniem roli zabezpieczeń organizacyjnych.

Słowa kluczowe: ochrona danych osobowych, cyberbezpieczeństwo, administrator, operator usługi kluczowej, NIS

JEL: K3

Abstract

The article analyses the issues related to the implementation of organisational responsibilities by personal data controllers and essential services operators relating to the use of risk-based approach, continuous improvement and privacy by design, building internal organisational structures responsible for the security management system of processed information, as well as the role of strategic and operational documentation, the use of self-regulation and standardisation in order to increase the effectiveness of law enforcement. The high dynamics of the development of information and communication technologies and business processes related to their use requires the application of a coherent and interdisciplinary approach to ensuring personal data protection and cybersecurity, which gives synergy effect. Flexibility of applied security solutions, allowing for optimal adaptation to continuous changes in the economic and legal environment, is also important factor. The primary objective of the article is to analyse the consistency and effectiveness of Polish and EU law regulations in the area of ensuring information security of data processing processes, with particular emphasis on the role of organisational safeguards.

Keywords: personal data protection, cybersecurity, controller, operators of essential services, NIS

Wstęp

Podmioty gospodarcze przetwarzają dane osobowe dla realizacji celów związanych ze swoją działalnością biznesową. W takiej sytuacji stają się administratorami tych zasobów, zobowiązanymi do stosowania wymogów wynikających z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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 (dalej: rozporządzenie o ochronie danych osobowych — RODO)[1]. Wiele z nich jest również operato-

rami usług kluczowych, co niesie za sobą konieczność wypełniania dodatkowych obowiązków związanych z zabezpieczaniem posiadanych systemów informacyjnych. Celem niniejszego artykułu jest przeanalizowanie wymagań prawnych w tych obszarach, odnoszących się do obowiązków organizacyjnych takich podmiotów gospodarczych. Rozważania obejmą aktualny stan normatywny dotyczący ochrony danych osobowych, a także problematyki zapewniania cyberbezpieczeństwa. Szczególna uwaga zostanie poświęcona podobieństwom przyjętych w tych obszarach rozwiązań oraz wynikającym z nich możliwościom zmniejszenia obciążeń organizacyjnych spoczywających na podmiotach gospodarczych. Pomocne będzie także odniesienie się do rozwiązań wynikających z norm technicznych z obszaru bezpieczeństwa informacji, które mogą stanowić punkt odniesienia w kontekście stosowania uniwersalnych zabezpieczeń techniczno-organizacyjnych chroniących przetwarzanie zasoby. Nie można pominąć także wątku dotyczącego toczących się na forum Unii Europejskiej prac nad nowymi regulacjami w obszarze cyberbezpieczeństwa, które dążą do zmiany podejścia w zakresie zarządzania ryzykiem w systemach informacyjnych na bardziej proaktywne działanie.

Podejście oparte na ryzyku

Pojęcie ryzyka ma kluczowe znaczenie w procesie kształtowania podejścia do zabezpieczania chronionych zasobów informacyjnych przez podmioty zobowiązane do stosowania RODO i ustawy z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (dalej: u.k.s.c.)[2]. Zapewnianie bezpieczeństwa informacji stanowi istotny obszar zarządzania organizacją funkcjonującą w realiach gospodarki opartej na wiedzy (Byczkowski & Zawiła-Niedźwiecki, 2014, s. 45–46). Takie aktywności należą zwłaszcza do kompetencji administratora danych osobowych i operatora usługi kluczowej. Treść art. 24 i 32 RODO wskazują, że administrator przy wdrażaniu środków organizacyjnych i technicznych zabezpieczających przetwarzane przez niego dane osobowe powinien uwzględniać ryzyko naruszenia praw lub wolności osób fizycznych. W motywie 75 doprecyzowano, że sytuacje takie mogą prowadzić do uszczerbku fizycznego lub szkód majątkowych bądź niemajątkowych. Stosowanie podejścia bazującego na ryzyku ma zapewnić elastyczny dobór skutecznych środków zabezpieczających prawa i wolności podmiotów danych przy zachowaniu zasady neutralności technologicznej (Nowak, 2020, s. 40). Zarządzanie niepewnością pozwala podjąć działania ograniczające możliwe skutki związanych z nią potencjalnych negatywnych zdarzeń, takich jak awarie, nieautoryzowane ujawnienie zasobów, błędy ludzkie czy umyślne szkodliwe postępowanie.

Treść art. 32 ust. 2 RODO wskazuje, że przy ocenie stopnia bezpieczeństwa danych osobowych należy stosować holistyczne podejście, uwzględniające zagrożenia powiązane z przetwarzaniem takich zasobów, które niekoniecznie mają bezpośredni związek z ochroną praw i wolności osób fizycznych. Sytuacje takie mogą odnosić się do niezrealizowania celów biznesowych administratora danych, np. poprzez brak zadowalającego dostępu do takich zasobów, co docelowo może doprowadzić do obniżenia jakości lub nawet rezygnacji z dalszego świadczenia określonej usługi. Należy pamiętać, że zgodnie z art. 1 ust. 3 RODO akt ten nie ogranicza swobodnego przepływu danych osobowych w ramach wspólnego rynku UE, lecz tworzy dlań normatywne ramy w celu skutecznej ochrony praw i wolności osób, których takie zasoby dotyczą. Oznacza to, że w procesie zarządzania ryzykiem powinniśmy uwzględniać nie tylko zagrożenia dla jednostki, ale także w rozsądnym stopniu interesy administratora pozwalające mu bez przeszkód realizować własne cele biznesowe i oferować opłacalne oraz bezpieczne usługi i produkty wysokiej jakości.

Ryzyko jest wartością mierzalną i odnosi się do prawdopodobieństwa oraz wagi skutków potencjalnych incydentów, których ocena powinna być oparta na obiektywnych kryteriach. Takie wnioski wynikają z analizy art. 24, 32 i motywu 76 RODO. Omawiane negatywne zdarzenia odnoszą się przede wszystkim do przypadków zakłócenia atrybutów poufności, integralności, dostępności i odporności systemów i usług przetwarzania. Prezentowane tu podejście jest charakterystyczne również dla standardów zarządzania ryzykiem w bezpieczeństwie informacji, wynikających z treści norm technicznych rodziny ISO 27 000. W analogiczny sposób ustawodawca do tej problematyki podchodzi również w krajowych przepisach dotyczących cyberbezpieczeństwa. Na podstawie art. 8 u.k.s.c. operator usługi kluczowej wdraża system zarządzania bezpieczeństwem w systemie informacyjnym, zapewniając systematyczne szacowanie ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem, a także wdrożenie odpowiednich i proporcjonalnych do oszacowanego stopnia zagrożenia środków technicznych i organizacyjnych zapewniających poufność, integralność, dostępność i autentyczność chronionych zasobów.

Struktura modelowego procesu zarządzania ryzykiem związanym z bezpieczeństwem informacji jest szczegółowo opisana w normach technicznych. Standard ISO 27 005[3] zawiera wytyczne odnoszące się do ustanowienia kontekstu przetwarzania takich zasobów (inaczej rozpoznania środowiska wewnętrznego i zewnętrznego organizacji), szacowania ryzyka (jego identyfikacji, analizy, oceny) i postępowania z nim (poprzez modyfikowanie, zachowanie, unikanie czy dzielenie). Warto zaznaczyć, że omawiana norma techniczna została wskazana w poradniku Prezesa Urzędu Ochrony Danych Osobowych jako istotny merytorycznie punkt odniesienia w kontekście kształtowania własnej metodyki zarządzania ryzykiem w podmiocie przetwarzającym dane osobowe (Kaczmarek i in., 2018, s. 10). Standard ten jest również użyteczny w ramach realizacji wymagań dla systemu zarządzania bezpieczeństwem informacji operatora usługi kluczowej (Kister, 2019, s. 38). W ramach procesów normalizacji powstają dokumenty będące efektem dyskursu ekspertów specjalizujących się w określonej dziedzinie. Zgodnie z definicją zawartą w art. 2 pkt. 4 ustawy z 12.09.2002 r. o normalizacji[4] norma techniczna to dokument przyjęty na zasadzie konsensu i zatwierdzony przez upoważnioną jednostkę organizacyjną, ustalający — do po-

wszechnego i wielokrotnego stosowania — zasady, wytyczne lub charakterystyki odnoszące się do różnych rodzajów działalności lub ich wyników i zmierzający do uzyskania optymalnego stopnia uporządkowania w określonym zakresie. Stanowią one standard dobrej praktyki techniczno-biznesowej w wybranym obszarze gospodarczej aktywności (Fischer, 2017, s. 86). Ze względu na takie okoliczności stosowanie podejścia opartego na normach technicznych dotyczących bezpieczeństwa informacji i zarządzania ryzykiem w zakresie procesów funkcjonujących w organizacji w związku z ochroną danych osobowych i zapewnianiem satysfakcjonującego poziomu cyberbezpieczeństwa wydaje się jak najbardziej zasadną praktyką.

Proponowane w projekcie dyrektywy NIS 2[5] zmiany w podejściu do zarządzania ryzykiem, zaprezentowane w art. 18 ust. 3, zakładają położenie większego nacisku na działania prewencyjne i proaktywne realizowane przez niezbędne i istotne podmioty — zastępujące operatorów usług kluczowych. Takie aktywności pozwolą na zidentyfikowanie podatności zasobów i procesów na zagrożenia przed ich wykorzystaniem. W szczególności uwagi te odnoszą się do analizy bezpieczeństwa relacji z zewnętrznymi dostawcami i usługodawcami. Jest to istotne uzupełnienie koncepcji zarządzania incydentami, zakładającej uporządkowaną reakcję na zidentyfikowane sytuacje zrealizowania się ryzyka związanego z bezpieczeństwem informacji. Zbieranie i wymiana doświadczeń oraz budowanie na tej podstawie bazy wiedzy pozwoli na szybszą i bardziej precyzyjną reakcję na zagrożenia.

Odpowiednie prowadzenie procesu zarządzania ryzykiem w organizacji stanowi kluczowy aspekt zapewniania satysfakcjonującego poziomu bezpieczeństwa przez cały cykl życia chronionej informacji. Dotyczy to zarówno gwarantowania cyberbezpieczeństwa, jak i ochrony danych osobowych. Aby realnie spełniać wymagania prawne wynikające z RODO i przepisów implementujących dyrektywę NIS, konieczne jest uporządkowane zarządzanie ryzykiem, umożliwiające dobór adekwatnych do jego poziomu zabezpieczeń odpowiadających specyfice konkretnej organizacji.

Ciągłe doskonalenie i ochrona prywatności w fazie projektowania

Koncepcja uwzględniania ochrony danych już w fazie projektowania wynika z art. 25 RODO. Przytoczony przepis wskazuje, że zarówno przy określaniu sposobów przetwarzania danych, jak i w czasie jego realizacji należy wdrożyć odpowiednie i skuteczne środki techniczne i organizacyjne pozwalające na zachowanie poufności, integralności, dostępności i odporności zabezpieczanych procesów. Podstawą koncepcji ochrony danych w fazie projektowania, wywodzącej się z mającego kanadyjskie korzenie podejścia *Privacy by Design* (Cavoukian, 2011), jest działanie proaktywne — prewencyjne, w odróżnieniu od reagowania *ex post* na faktyczne incydenty i ich skutki (Wiewiórowski, 2012, s. 17). W ramach takich aktywności należy zapewnić adekwatną do zidentyfikowanych i ocenionych ryzyk ochronę praw osób, których dane dotyczą, i być przygotowanym do sprawnego przeciwdziałania ewentualnym rezultatom wystąpienia negatywnych zdarzeń związanych z bieżącym wykorzystywaniem tych zasobów (Cavoukian, 2015, s. 303). Omawiana ocena skutków dotyczy nie tylko etapu przygotowywania czynności przetwarzania danych, ale całego cyklu życia do momentu ich usunięcia, wraz z ewentualną anonimizacją.

W odniesieniu do cyberbezpieczeństwa operator usługi kluczowej ma obowiązek ciągłego doskonalenia podejścia do zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do jej świadczenia. Powinność taka wynika z treści art. 8 pkt 1 i 2 u.k.s.c., które wskazują, że podmiot ten jest obowiązany do systematycznego szacowania ryzyka wystąpienia incydentu, zarządzania nim i wdrażania zabezpieczeń adekwatnych do zagrożeń. Aktywność taka ma charakter cykliczny i powinna się opierać na wynikach stałego monitoringu podatności posiadanych zasobów i realizowanych procesów biznesowych. Należy dodać, że jak stanowi § 2 pkt 1 rozporządzenia Rady Ministrów z 16.10.2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej[6], dokumenty te mają być wytworzone zgodnie z wymaganiami normy ISO 27 001, gdzie w załączniku A wspomniano o konieczności stosowania uporządkowanego podejścia do planowania, wdrożenia, weryfikowania, przeglądu i oceny ciągłości bezpieczeństwa informacji. Takie aktywności pozwolą na zagwarantowanie stabilności i nieprzerwanej realizacji kluczowych procesów biznesowych związanych ze świadczeniem usługi kluczowej. Dodatkowo w punkcie 3 omawianego przepisu wskazuje się na konieczność stosowania również normy ISO 22 301, odnoszącej się do wymagań dla systemów zarządzania ciągłością działania. Doskonalenie systemu bezpieczeństwa informacji związanych ze świadczeniem usług kluczowych pozwala na zachowanie jego spójności i skuteczności poprzez monitoring związanego z nim ryzyka oraz podejmowanie reakcji korygujących adekwatnych do zidentyfikowanych niepożądanych odchyleń.

Koncepcje ciągłego doskonalenia i ochrony danych osobowych już w fazie projektowania mają istotne cechy wspólne. Obydwie odnoszą się do całokształtu cyklu życia procesów przetwarzania zasobów informacyjnych — od ich przygotowania, przez wdrożenie, bieżącą pielęgnację, po zakończenie realizacji. Podstawę doboru odpowiednich organizacyjnych i technicznych środków bezpieczeństwa stanowią wyniki procesu zarządzania ryzykiem pozwalające zastosować właściwe metody postępowania.

Wewnętrzne struktury organizacyjne odpowiedzialne za ochronę danych osobowych i cyberbezpieczeństwo

Zapewnienie bezpieczeństwa informacji wymaga utworzenia i utrzymywania struktury organizacyjnej odpowie-

dzialnej za realizację działań zabezpieczających chronione zasoby. W art. 37 RODO przewidziano obowiązek wyznaczenia Inspektora Ochrony Danych przez niektórych administratorów, takich jak podmioty publiczne czy organizacje przetwarzające na dużą skalę szczególne kategorie danych osobowych (przykładowo podmioty wykonujące działalność leczniczą prowadzące szpitale). Funkcja ta zdradza pewne podobieństwa z rolą osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, przewidzianą w art. 9 ust. 1 pkt. 1 u.k.s.c. Inspektor Ochrony Danych na podstawie art. 39 ust. 1 lit. d i e RODO stanowi punkt kontaktowy i jest obowiązany do współpracy z organem nadzorczym. Łączenie obydwu omówionych ról wydaje się możliwe na podstawie art. 38 ust. 6 RODO, ale nie powinno prowadzić do konfliktu interesów i niemożności swobodnego wykonywania podstawowych zadań zabezpieczających przez taką osobę.

Operator usługi jest zobowiązany na podstawie art. 14 ust. 1 u.k.s.c. do zbudowania wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo[7]. Powinny one spełniać warunki organizacyjne i techniczne pozwalające na realizację wyznaczonych zadań, a także funkcjonować w odpowiednio zabezpieczonych pomieszczeniach i stosować środki bezpieczeństwa adekwatne do aktualnego stanu zagrożeń. Szczegółowe wymagania dotyczące takich praktyk odnajdziemy w rozporządzeniu Ministra Cyfryzacji z 4.12.2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo[8]. Należy zaznaczyć, że akt ten koncentruje się przede wszystkim na środkach fizycznych i technicznych związanych z zapewnianiem bezpieczeństwa świadczenia usług kluczowych. Zabezpieczenia organizacyjne nie są tu przedstawione w sposób wystarczająco rozbudowany. W związku ze zidentyfikowanymi mankamentami obowiązującej regulacji ustawodawca pracuje nad zmianami legislacyjnymi w omawianym obszarze[9]. Mają one obejmować wprowadzenie tzw. SOC, będącego zespołem eksperckim pełniącym funkcję operacyjnego centrum bezpieczeństwa w organizacji realizującej usługę kluczową (wewnętrzny) lub działającego na jej rzecz (zewnętrzny), wprowadzającego zabezpieczenia na podstawie przeprowadzonego procesu szacowania ryzyka.

Zagwarantowanie satysfakcjonującego poziomu bezpieczeństwa informacji jest długotrwałym i wieloetapowym procesem, wymagającym uwzględniania aktualnej i interdyscyplinarnej wiedzy oraz stosowania odpowiednich środków ochronnych. Obejmują one nie tylko rozwiązania techniczne, ale także organizacyjne — dokumentację, procedury i struktury. Poza zastosowaniem zabezpieczeń technicznych zarówno zapewnianie cyberbezpieczeństwa, jak i należyta ochrona danych osobowych wymaga zbudowania sprawnej i kompetentnej struktury organizacyjnej, która odpowiednio reaguje na zmiany zagrożeń w środowisku przetwarzania informacji.

Rola dokumentacji i samoregulacji w zwiększaniu skuteczności stosowania prawa w obszarze ochrony danych osobowych i zapewniania cyberbezpieczeństwa

Dokumenty związane z procesami zapewniania cyberbezpieczeństwa i ochrony danych osobowych pełnią istotną rolę stabilizującą i porządkującą podejmowane aktywności. Utrwalone w ten sposób informacje mogą dotyczyć zarówno strategii podejmowanych działań, jak i ich aspektu operacyjno-wdrożeniowego. Treść art. 24 ust. 2 RODO wskazuje, że środki techniczno-organizacyjne służące ochronie danych osobowych powinny obejmować odpowiednie polityki. Ich wdrożenie stanowi istotny przejaw realizacji wynikających z art. 5 RODO zasad zapewniania bezpieczeństwa tych zasobów informacyjnych[10]. Dokument taki jest w istocie zbiorem pryncypiów i wynikających z nich kierunków działań, według których dana organizacja przetwarza swoje zasoby w ramach systemów informacyjnych, zapewniając w tym obszarze poziom zabezpieczeń adekwatny w odniesieniu do zagrożeń i związanych z nimi ryzyk (Kowalewski & Ołtarzewska, 2007, s. 3–4).

Polityka określa zatem podejście podmiotu do zapewniania bezpieczeństwa informacji[11] i stanowi fundament dla szczegółowych procedur oraz zapisów tworzących systematycznie aktualizowaną dokumentację operacyjną. Jednym z takich bieżących dokumentów jest rejestr czynności przetwarzania danych osobowych, którego prowadzenie przez administratora wynika z art. 30 ust. 1 RODO, jak również rejestr naruszeń wymagany na podstawie art. 33 ust. 5 RODO zobowiązującego do utrwalania informacji dotyczących wszelkich takich sytuacji, z uwzględnieniem ich okoliczności, skutków i podjętych działań zaradczych. Nie można pominąć także zagadnienia wpływu zarządzania ryzykiem na prawa i wolności osób, których dane dotyczą, a także oceny skutków dla ochrony danych, gdzie sporządzanie dokumentacji podejmowanych aktywności i potwierdzania ich skuteczności ma kluczowe znaczenie przy ocenie właściwej realizacji zasady rozliczalności wynikającej z art. 5 ust. 2 RODO (Thomas, 2014, s. 146). W takich okolicznościach utrwalanie informacji o wykonanych działaniach zabezpieczających i skutkach ich realizacji pełni funkcję dowodową.

Operator usługi kluczowej jest obowiązany na podstawie art. 10 u.k.s.c. do prowadzenia dokumentacji systemu informacyjnego służącego do jej świadczenia. Zgodnie z rozporządzeniem Rady Ministrów z 16.10.2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej obejmuje ona część normatywną i operacyjną. Pierwsza z nich dotyczy sposobu realizacji wymagań wynikających normy ISO 27 001 i składa się z polityk i strategii w obszarze zarządzania bezpieczeństwem, ryzykiem, ciągłością działania oraz aspektów technicznych wdrażania zabezpieczeń. Dokumentacja operacyjna zawiera zaś opis procedur wraz z charakterystyką sposobów dokumentowania wykonywanych

w ich ramach czynności. Do tej ostatniej grupy dokumentów możemy zaliczyć rejestr ryzyka czy zasobów (aktywów), które powinny być na bieżąco aktualizowane przez operatora usługi kluczowej w przypadkach występowania istotnych zmian w środowisku przetwarzania informacji. Takie podejście związane jest z koncepcją ciągłego doskonalenia systemu bezpieczeństwa opartą na tzw. cyklu Deminga (PDCA), zakładającą nie tylko zaplanowanie i wykonanie określonego zadania, ale także weryfikację efektów jego realizacji i wprowadzenie stosownych korekt, jeśli okaże się to zasadne na podstawie analizy danych obrazujących stan faktyczny.

Przedstawiciele współczesnych społeczeństw informacyjnych oczekują od instytucji UE podejmowania działań gwarantujących zachowanie cyberbezpieczeństwa i autonomii informacyjnej jednostki (Papakonstantinou, 2022). Instrumenty prawne powinny zachowywać swoją skuteczność również w obszarach charakteryzujących się dużą zmiennością procesów gospodarczych, społecznych i technicznych. Zbyt rozbudowane przepisy, mające nadmiernie kazuistyczny charakter, mogą prowadzić w takich sytuacjach do faktycznego przeformalizowania i w konsekwencji spadku jakości regulacji, nierealizujących odpowiednio ustalonych przez prawodawcę celów (Korczak, 2012, s. 181–182). Rozwiązaniem zasygnalizowanego problemu jest uzupełnienie generalnych i abstrakcyjnych norm prawa powszechnie obowiązującego samoregulacją i aktami prawa miękkiego (*soft law*). Przyjęcie takiego podejścia pozwala poszerzyć oddziaływanie podmiotów publicznych na obszary, gdzie wykorzystywanie klasycznych instrumentów opartych na prawie stanowionym jest ograniczone (Fischer, 2010, s. 288–289). Przykładem zastosowania *soft law* i samoregulacji w obszarze ochrony danych osobowych są z jednej strony wytyczne Europejskiej Rady Ochrony Danych (wcześniej Grupy Roboczej Art. 29 dyrektywy 95/46/WE) wydawane na podstawie art. 70 ust. 1, z drugiej zaś opracowywane przez samych administratorów tych zasobów kodeksy postępowania wskazane w art. 40 RODO czy wiążące reguły korporacyjne (*binding corporate rules*) z art. 47. W zakresie regulacji problematyki cyberbezpieczeństwa podobny charakter mają kompetencje ENISA związane z wydawaniem wytycznych zgodnie z art. 7 ust. 2 lit. b rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z 17.04.2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)[12]. Zastosowanie instrumentów *soft law* i samoregulacji jako uzupełnienie ogólnych wymagań i zasad wynikających z prawa powszechnie obowiązującego w obszarach związanych z zapewnianiem bezpieczeństwa informacyjnego pozwala uzyskać pożądany stopień elastyczności i trwałości aktów normatywnych, które mogą w ten sposób zachowywać swoją skuteczność w czasie bez konieczności wprowadzania zmian legislacyjnych *ad hoc*.

Podsumowanie

Nowoczesne podejście do zapewniania bezpieczeństwa informacyjnego w organizacji, obejmującego swoim zakresem problematykę cyberbezpieczeństwa i ochrony danych osobowych opiera się na uporządkowanym procesie zarządzania ryzykiem odnoszącym się do całokształtu cyklu życia chronionych zasobów. Na podstawie wyników tak prowadzonej analizy następuje dobór środków organizacyjnych i technicznych, które powinny doprowadzić do redukcji lub ominięcia zidentyfikowanych istotnych ryzyk. Opisane tu działania nie są podejmowane jednorazowo przy rozpoczęciu przetwarzania informacji czy jako reakcja na zaistniałe incydenty, lecz stanowią spójne i stałe podejście oparte na ciągłym monitorowaniu stanu faktycznego i ewentualnych korektach odchyleń od założonych wskaźników pozwalających osiągnąć stabilność bezpieczeństwa takich zasobów w organizacji.

Stabilizację funkcjonowania systemu zarządzania bezpieczeństwem informacji w organizacji zapewnia jego dokumentacja strategiczna i operacyjna. Odnosi się ona zarówno do czynności podejmowanych w celu zapewniania należytej ochrony danych osobowych, jak i satysfakcjonującego poziomu cyberbezpieczeństwa. Dokumentacja pozwala udowodnić wykonane działania zabezpieczające i wskazać stopień redukcji ryzyk związanych z przetwarzaniem informacji w organizacji. W ten sposób można wykazać realizację przez administratora danych zasad wynikających z RODO czy wdrożenie wymagań nałożonych na operatora usługi kluczowej przepisami u.k.s.c. Dokumentacja stanowi również bazę wiedzy obejmującą utrwalone doświadczenia związane z zarządzaniem bezpieczeństwem informacji, które mogą posłużyć doskonaleniu stosowanych procedur i narzędzi ochronnych.

Wzmocnienie samoregulacji zarówno w obszarze cyberbezpieczeństwa, jak i ochrony danych osobowych nie tylko na poziomie organizacji, ale również ich branżowych zrzeszeń pozwala na zwiększenie elastyczności wymagań wynikających z prawa powszechnie obowiązującego. Poszerza to wachlarz możliwości wyboru metod ich realizacji, które najbardziej odpowiadają specyfice działalności podmiotów określonej wielkości i rodzaju.

Wartościowym źródłem dobrych praktyk w zakresie zarządzania bezpieczeństwem informacji są normy techniczne. Zdefiniowane w nich wymagania i ułatwiające ich wdrożenie wytyczne stanowią rozwinięcie minimalnego standardu ochrony wynikającego z obowiązujących regulacji. Dodatkowo takie branżowe standardy ułatwiają konkretyzację generalnych i abstrakcyjnych norm prawnych. Pozwala to na dobór środków ochrony adekwatnych do sytuacji konkretnego podmiotu i warunków przetwarzania zasobów informacyjnych w ramach jego działalności.

Istnieje możliwość certyfikowania przez uprawniony podmiot trzeci Systemu Zarządzania Bezpieczeństwem Informacji w organizacji za zgodność z wymaganiami normy ISO 27 001. Podobne rozwiązania potwierdzające spełnienie ustalonych standardów ochrony odnajdziemy w art. 42 RODO

czy art. 8 aktu o cyberbezpieczeństwie statuującym kompetencje ENISA w zakresie harmonizacji standardów oceny bezpieczeństwa informacji. Obowiązki w tym ostatnim obszarze dla podmiotów będących częścią krajowego systemu cyberbezpieczeństwa przewiduje również art. 21 proponowanej dyrektywy NIS 2. Rozwój procedur certyfikacyjnych w krajowych i europejskich regulacjach należy ocenić pozytywnie. Uczestnictwo w nich pozwala uzyskać uprzednie potwierdzenie zgodności z określonymi prawnymi wymaganiami, które — poza oczywistym zminimalizowaniem ryzyk potencjalnie skutkujących incydentami związanymi z naruszeniem tych regulacji — może uprościć i skrócić ewentualne następcze czynności kontrolne realizowane przez organ nadzorczy.

Zarządzanie ryzykiem zarówno w przypadku ochrony danych osobowych, jak i zapewniania cyberbezpieczeństwa opiera się na podobnych zasadach i procesach w organizacji. Zwiększenie skuteczności działań przy jednoczesnym zmniejszeniu kosztów jest możliwe przy zastosowaniu jednolitej strategii zarządzania ryzykiem, procedur postępowania z nim i prowadzeniu kompleksowej dokumentacji. Spójne podejście organizacji do zarządzania niepewnością związaną z jej funkcjonowaniem pozwala uzyskać swoisty efekt synergii. Należy zaznaczyć, że do każdej kategorii ryzyka powinny być przyporządkowane wyspecjalizowane działania i dodatkowe elementy w strukturze dokumentacji, aby możliwe było zrealizowanie wymagań wynikających treści aktów prawnych.

Obowiązujący stan prawny niejako separuje zbliżone zakresem przedmiotowym regulacje odnoszące się do ochrony danych osobowych od przepisów dotyczących cyberbezpieczeństwa. Przykładem może być brak norm kolizyjnych między kompetencjami inspektora ochrony danych a strukturą operatora usługi kluczowej odpowiedzialną za cyberbezpieczeństwo. Podobna sytuacja ma miejsce w odniesieniu do procedury zgłaszania i usuwania skutków naruszeń ochrony danych i incydentów, czyli pokrewnych w swojej naturze zdarzeń przejawiających się niekorzystnym wpływem na bezpieczeństwo przetwarzanych informacji (Schmitz-Berndt, & Schiffner, 2021, s. 111). W kontekście tej ostatniej uwagi należy jednak zaznaczyć, że w projekcie dyrektywy NIS 2 odnajdziemy propozycję stosownej normy kolizyjnej w art. 32. Procedura przeprowadzania oceny skutków dla ochrony danych z art. 35 RODO, obejmująca ocenę ryzyka naruszenia praw lub wolności osób i zaplanowania środków zaradczych, wskazuje na istotne podobieństwa podejmowanych w ramach niej działań do przewidzianego w art. 8 pkt 1 u.k.s.c. obowiązku operatora usługi kluczowej w zakresie prowadzenia systematycznego szacowania ryzyka i wdrażania ograniczających je zabezpieczeń. W kontekście poczynionych tu uwag zasadna wydaje się dalej idąca integracja tych zbliżonych do siebie zakresowo regulacji, co może doprowadzić do niewielkiego uproszczenia strukturalnego i obniżenia kosztów wdrażania i utrzymywania organizacyjnych zabezpieczeń przetwarzanych informacji w organizacjach.

Przypisy/Notes

[1] Dz. Urz. UE L 119, 4.05.2016, s. 1–88.

[2] T.j. Dz.U. z 2020 r., poz. 1369.

[3] Jest on rozwinięciem ogólnego podejścia do zarządzania ryzykiem w organizacji, wynikającego z normy ISO 31 000 zawierającej zbiór zasad i wytycznych odnoszących się do takich działań.

[4] T.j. Dz.U. z 2015 r., poz. 1483.

[5] Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylająca dyrektywę (UE) 2016/1148 (COM(2020) 823).

[6] Dz.U. z 2018 r., poz. 2080.

[7] Alternatywnie podmiot taki może zamiast tworzenia własnej wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo zawrzeć umowę z podmiotem świadczącym takie usługi (art. 14 ust. 1 u.k.s.c. *in fine*).

[8] Dz.U. z 2019 r., poz. 2479.

[9] Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy — Prawo zamówień publicznych (UD68). https://legislacja.rcl.gov.pl/projekt/12337950 (pobrano 28.06.2022).

[10] Takie podejście pozwala skutecznie wykazać stosowanie standardów bezpieczeństwa wynikających z RODO, co jest istotą respektowania zasady rozliczalności (wyrok WSA w Warszawie z 26.08.2020, II SA/Wa 2826/19).

[11] W orzecznictwie wskazuje się, że „polityka bezpieczeństwa to dokument, który powinien być dostosowany do konkretnych warunków przetwarzania danych osobowych u określonego administratora danych" (wyrok WSA w Warszawie z 5.10.2005, II SA/Wa 734/05).

[12] Dz. Urz. UE L 151, 7.06.2019, s. 15–69.

Bibliografia/References

Byczkowski, M. &, Zawiła-Niedźwiecki, J. (2014). Analiza ryzyka w zarządzaniu bezpieczeństwem danych osobowych. Aktualne problemy prawnej ochrony danych osobowych. *Dodatek do Monitora Prawniczego*, (9), 45–46.

Cavoukian, A. (2011). *Privacy by Design. The 7 foundational principles*. IPC. https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf (pobrano 25.07.2021).

Cavoukian, A. (2015). Evolving FIPPs: Proactive approaches to privacy, not privacy paternalism. W: S. Gutwirth, R. Leenes, & P. de Hert (red.), *Reforming European data protection law*. Springer. https://doi.org/10.1007/978-94-017-9385-8_12

Fischer, B. (2010). *Transgraniczność prawa administracyjnego na przykładzie regulacji przekazywania danych osobowych z Polski do państw trzecich*. Wolters Kluwer.

Fischer, B. (2017). *Prawne aspekty norm technicznych. Normalizacja jako wsparcie legislacji administracyjnej*. Wolters Kluwer.

Kaczmarek, A., Młotkiewicz, M., Łapińska, A., Miłocha, A., & Mazur, M. (2018). *Jak rozumieć podejście oparte na ryzyku?* UODO. https://uodo.gov.pl/pl/file/706 (pobrano 25.07.2021), s. 10.

Kister, Ł. (2019). Szacowanie ryzyka dla usług kluczowych opartych o systemy OT. *Nowa Energia*, (3/68).
Korczak, J. (2012). Jakość prawa administracyjnego na przykładzie materialnego, procesowego i ustrojowego prawa administracyjnego samorządu terytorialnego. W: D. Kijowski, A. Miruć, & P. Suwaj (red.), *Kryzys prawa administracyjnego? Tom I. Jakość prawa administracyjnego*. Wolters Kluwer.
Kowalewski, M., & Ołtarzewska, A. (2007). Polityka bezpieczeństwa informacji instytucji na przykładzie Instytutu Łączności — Państwowego Instytutu Badawczego. *Telekomunikacja i Techniki Informacyjne*, nr (3–4), 3–4.
Nowak, D. (2020). Podejście oparte na ryzyku w RODO w praktyce — wnioski po dwóch latach stosowania RODO. W: G Sibiga (red.), Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy ochrony danych osobowych. Dodatek do *Monitora Prawniczego*, (23).
Papakonstantinou, V. (2022). Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity? *Computer Law and Security Review*, *44*. https://doi.org/10.1016/j.clsr.2022.105653
Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy — Prawo zamówień publicznych (UD68). https://legislacja.rcl.gov.pl/projekt/12337950 (pobrano 10.09.2021).
Schmitz-Berndt, S., & Schiffner., S. (2021). Don't tell them now (or at all) — responsible disclosure of security incidents under NIS Directive and GDPR. *International Review of Law, Computers & Technology*, *35*(2). https://doi.org/10.1080/13600869.2021.1885103
Thomas, R. (2014). Accountability — a modern approach to regulating the 21st century data environment. W: H. Hijmans, & H. Kranenborg (red.), *Data protection anno 2014: How to restore trust?* Intersentia. https://doi.org/10.1093/idpl/ipv014
Wiewiórowski, W. (2012). Privacy by Design jako paradygmat ochrony prywatności. W: G. Szpor, & W. Wiewiórowski (red.), *Internet. Prawno-informatyczne problemy sieci, portali i e-usług*. C.H.Beck.
Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylająca dyrektywę (UE) 2016/1148 (COM(2020) 823).
Wyrok WSA w Warszawie z 26.08.2020, II SA/Wa 2826/19.
Wyrok WSA w Warszawie z 5.10.2005 r., II SA/Wa 734/05.

Dr inż. Krzysztof Świtała

Doktor nauk prawnych, adiunkt w Katedrze Prawa Informatycznego Wydziału Prawa i Administracji Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie. Jego zainteresowania naukowe dotyczą prawa nowych technologii, a zwłaszcza zagadnień związanych ochroną danych osobowych i cyberbezpieczeństwem.

Dr inż. Krzysztof Świtała

Doctor of Law, Assistant Professor at the Department of Information Technology Law, Faculty of Law and Administration, Cardinal Stefan Wyszyński University in Warsaw. His research interests concern the law of new technologies, in particular issues related to personal data protection and cyber security.

Klub książki PWE

Z myślą o swoich Czytelnikach Polskie Wydawnictwo Ekonomiczne stworzyło **Klub książki PWE**.
W ramach członkostwa w Klubie proponujemy następujące udogodnienia i korzyści:
✔ szybkie zakupy;
✔ zakupy z rabatem;
✔ informacje o nowościach, promocjach, konkursach.

Po więcej informacji zapraszamy na stronę PWE: *www.pwe.com.pl*