DOI:10.17951/we.2020.6.2.145-157 | Wschód Europy • Восток Европы • East of Europe vol 6, 2 / 2020

Aleksandra Olender
Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego w Warszawie
ORCID ID: https://orcid.org/0000-0001-7145-5801

Analiza ryzyka i ocena skutków dla ochrony danych osobowych przetwarzanych w podmiotach sektora publicznego

1. Wprowadzenie

Rozkwit ery informacyjnej, rozwój zaawansowanych technologii oraz zwiększona globalizacja przepływu danych nieustannie stwarza nowe wyzwania oraz zagrożenia związane z zapewnieniem bezpieczeństwa przetwarzanych informacji. Informacja bowiem stała się najcenniejszym towarem we współczesnym świecie. Właściwe zarządzanie zasobami informacyjnymi oraz odpowiednia ochrona posiadanych danych coraz częściej stanowi priorytet dla prawidłowego funkcjonowania współczesnych organizacji. Powszechne używanie systemów informatycznych nie tylko usprawnia działanie podmiotów, ale odkrywa nowe podatności, wykorzystywane przez zagrożenia. Zatem wraz z rozwojem technologicznym wymagane jest ciągłe udoskonalanie metod ochrony posiadanych zasobów informacyjnych.

Typowym rodzajem danych przetwarzanych przez niemalże wszystkie współczesne organizacje są dane osobowe osób fizycznych. Prawo Unii Europejskiej obejmuje je szczególną ochroną, co ma swoje podwaliny już w Powszechnej deklaracji praw człowieka z 1948 r. akcentującej, iż nikt nie może być narażony na integrowanie w jego życie prywatne, domowe, rodzinne lub korespondencję ani też stać się obiektem ataków godzących w jego dobre imię i honor. Ochrona danych osobowych jest jednym z podstawowych aspektów prawa do prywatności[1]. Prace nad kompleksowym ujęciem tego zagadnienia w akcie prawnym UE trwały od 1990 r., ale dopiero przyjęcie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych

[1] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Wydawnictwo CH Beck, Warszawa 2016, s. 36.

i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne rozporządzenie – RODO) wprowadziło ujednolicenie przepisów dotyczących ochrony danych osobowych we wszystkich krajach Unii Europejskiej. Ten akt prawny ma na celu ułatwienie prowadzenia transgranicznej działalności gospodarczej i obejmuje wszystkie podmioty przetwarzające dane osobowe na obszarze Unii[2].

Przepisy RODO kładą szczególny nacisk na postrzeganie obowiązków prawnych zgodnie z prospołecznym podejściem do zarządzania podmiotami administracyjnymi oraz gospodarczymi. Taki punkt widzenia sprawia, że zarządzanie ryzykiem jest kluczowym elementem dla praktyki stosowania oraz egzekwowania unijnych przepisów[3].

Ogólne rozporządzenie podejmuje kwestie zarządzania ochroną danych osobowych z perspektywy ryzyka, co zostało ujęte w motywach preambuły tego aktu prawnego. Prawodawca unijny, mając na względzie dynamikę i różnorodność zmieniającej się rzeczywistości, precyzyjnie określił jedynie oczekiwania wobec podmiotów przetwarzających dane, natomiast kwestie adekwatności postępowania podmiotów, by te oczekiwania wypełnić, pozostawił niedookreślone. Takie rozwiązanie wymaga od podmiotów gospodarczych, urzędów, kadry zarządzającej oraz samych pracowników zwrócenia większej uwagi na zagadnienia społecznej odpowiedzialności, prawo unijne bowiem za priorytet uznaje ochronę prywatności i dóbr osobistych każdego człowieka oraz zobowiązuje organizacje do szanowania tych nadrzędnych wartości, wprowadzając jednocześnie wysokie kary za ich nieprzestrzeganie.

Artykuł porusza kwestie analizy ryzyka i oceny skutków dla ochrony danych osobowych przetwarzanych w sektorze publicznym, podjętej w celu spełnienia wymagań RODO. Ogólnym problemem badawczym artykułu jest przybliżenie obowiązku stosowania podejścia opartego na zarządzaniu ryzykiem przy przetwarzaniu danych osobowych w podmiotach publicznych. Mając na względzie, iż instytucje publiczne przetwarzając dane osobowe wszystkich obywateli, nierzadko również szczególne kategorie danych osobowych (np. informacje o pochodzeniu rasowym lub etnicznym, poglądach politycznych), których przetwarzanie może się wiązać z wysokim ryzykiem naruszenia praw i wolności osób fizycznych, powinny zwrócić szczególną uwagę na prowadzenie poprawnej analizy ryzyka dla przetwarzanych danych. Przyjęcie właściwej metodyki w procesie szacowania ryzyka umożliwia wdrożenie zabezpieczeń adekwatnych do potencjalnych zagrożeń[4]. W pracy postawiono hipotezę, że przeprowadzenie rzetelnej oceny skutków dla ochrony danych w dalszym ciągu stanowi dla podmiotów sektora publicznego wyzwanie. Główne pytanie badawcze ma charakter eksplanacyjny i zostało zawarte w następujący sposób: jakie znaczenie dla osób, których dane są przetwarzane w podmiotach sektora publicznego, ma przeprowadzenie rzetelnej i adekwatnej

[2] P. Litwiński, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Wydawnictwo CH Beck, Warszawa 2017, s. 17.

[3] J. Zawiła-Niedźwiecki, *Analiza ryzyka służąca spełnianiu wymagań RODO*, https://sip.legalis.pl/document-view.seam?documentId=mjxw62zogi3damjzhaydooa, inf. 15 VI 2019.

[4] M. Byczkowski, *Zabezpieczanie danych osobowych w RODO*, „IAP" 2017, nr 2.

analizy ryzyka i oceny skutków dla ochrony danych osobowych? Celem zaś pracy jest analiza funkcji/następstw stosowania analizy ryzyka i oceny skutków dla ochrony danych osobowych.

2. Model ochrony danych oparty na ryzyku

Wypracowane przez organy unijne Rozporządzenie 2016/679 wprowadza nowy, proaktywny model ochrony danych osobowych przetwarzanych w organizacji, oparty na podejściu bazującym na ryzyku. Stosowanie takiego typu rozwiązania ma na celu ułatwienie administratorowi podjęcie odpowiednich kroków w celu ochrony posiadanych zasobów informacji, w tym w szczególności danych osobowych osób fizycznych. W zależności od oszacowanego poziomu ryzyka dla przetwarzanych danych podmiot przetwarzający powinien wdrażać adekwatne środki minimalizujące negatywne skutki wykorzystania podatności systemów przez mogące wystąpić zagrożenia.

Ryzyko utożsamiane jest z niepewnością, co wynika z faktu, że podmioty nigdy nie działają w warunkach pewności, a jedynie przy większym bądź mniejszym prawdopodobieństwie. Ryzyko może być pojmowane różnorodnie. Na potrzeby niniejszego artykułu należy przytoczyć definicję negatywną, która zakłada, że „ryzyko oznacza możliwość nie osiągnięcia oczekiwanego efektu (poniesienia szkody, straty)"[5]. Można przyjąć również, że ryzyko jest swoistym „scenariuszem, który opisuje zdarzenie i jego konsekwencje, oszacowanym pod względem powagi (wielkości szkody, jakie może przynieść zdarzenie) i prawdopodobieństwa wystąpienia tego zdarzenia, które stanowi naruszenie".

Administratorzy, wypełniając wymogi RODO, powinni rzetelnie przykładać się do kwestii analizy ryzyka i stosować odpowiednie środki zaradcze. Obecnie bowiem to nie ustawodawca decyduje o tym, jakie zabezpieczenia należy wprowadzić, by skutecznie chronić dane, ale taki obowiązek spoczywa na podmiotach, które te dane przetwarzają. Administrator lub procesor musi sam zdecydować, jakie środki ochrony zastosuje. Zatem organ publiczny nie otrzyma szczegółowych wytycznych dla ochrony swoich zasobów. Będzie musiał wykazać się większą elastycznością w ocenie tego, jakie środki winny być stosowane w przypadku rejestru czynności przetwarzania, który posiada[6].

Administrator zobligowany jest wprowadzić ochronę techniczną i organizacyjną przetwarzanych danych, która będzie adekwatna do skali ryzyka, rozpatrywanej pod kątem możliwości utraty atrybutów informacji (tj. dostępności, integralności oraz poufności) przy uwzględnieniu kontekstu, zakresu, celów przetwarzania oraz w szczególności ryzyka naruszenia praw i wolności osób, których dane dotyczą. Ponadto decydując się na zastosowanie określonych środków ochrony, powinien mieć na uwadze

[5] P. Sienkiewicz, *Ewaluacja ryzyka w zarządzaniu kryzysowym*, [w:] *Ryzyko w zarządzaniu kryzysowym*, red. P. Sienkiewicz, M. Marszałek, P. Górny, Wydawnictwo Adam Marszałek, Toruń 2012, s. 25.

[6] *RODO. Przewodnik ze wzorami*, red. M. Gawroński, Wydawnictwo Wolters Kluwer Polska, Warszawa 2018, s. 265.

aktualny stan wiedzy technicznej oraz koszt wdrożenia danego rozwiązania. Wprowadzenie zabezpieczeń dla posiadanych zasobów informacyjnych musi również posiadać uzasadnienie ekonomiczne. Możliwe bowiem jest to, że prowadzenie jakiegoś procesu przetwarzania jest nieopłacalne z uwagi na fakt, że koszty ochrony danych przewyższają zyski z prowadzenia tego procesu. Niemniej jednak odnosząc się do zasobów przetwarzanych w sektorze publicznym, możliwość rezygnacji z pewnych czynności przetwarzania danych może się okazać niemożliwa. Wynika to z faktu, iż podmioty publiczne przetwarzają dane głównie na podstawie przesłanki obowiązku ciążącego na administratorze bądź ważnego interesu publicznego. Sytuacja taka powoduje konieczność wdrożenia często kosztownych rozwiązań, w celu eliminacji podatności na zagrożenia.

3. Proces zarządzania ryzykiem w ochronie danych osobowych

Proces zarządzania ryzykiem winien stanowić jedno z kluczowych zagadnień w zarządzaniu organizacją, gdyż odnosi się on do rozmaitych zasobów. W związku z wymaganiami ochrony danych, jakie RODO nakłada na podmioty przetwarzające dane, można wyróżnić następujące obszary, w których analizuje się ryzyko:

- ryzyko w bezpieczeństwie przetwarzania (związane jest z zagrożeniami dla utraty poufności, integralności i dostępności danych, np. ataki DDoS, oprogramowanie *ransomware*),
- ryzyko niewykonania obowiązków formalnych (związane z żądaniami osób, których dane dotyczą, np. prawo do udzielenia informacji o przetwarzanych przez administratora danych, do bycia zapomnianym, sprostowania danych itp.),
- analiza i ocena ryzyka/ocena skutków dla ochrony danych (*Data Protection Impact Assessment* – DPIA) – związana z permanentną oceną wpływu przetwarzania danych na prawa i wolności osób, których dane podmiot przetwarza; wymaga wdrażania przy projektowaniu przetwarzania, jak również w trakcie zarządzania bezpieczeństwem przetwarzania danych[7].

Biorąc pod uwagę tematykę artykułu, warto w tym miejscu przybliżyć definicję ryzyka akceptowalnego. Ryzyko akceptowalne, jak sama nazwa wskazuje, jest to poziom ryzyka uznany za bezpieczny do realizacji celu lub zadań[8].

Zarządzanie ryzykiem bezpieczeństwa informacji nie jest podejściem innowacyjnym i stosuje się je od dawna, dlatego dobrą praktyką jest zastosowanie w analizie ryzyka dla ochrony danych osobowych wypracowanych już rozwiązań. Norma ISO 27005 opisuje metodykę, którą można wdrożyć zarówno w małych, jak i dużych organizacjach. RODO nie wskazuje jednak na istnienie żadnej najlepszej metodyki stosowania

[7] *Poradnik RODO. Podejście oparte na ryzyku*, red. J. Zawiła-Niedźwiecki. cz. 2, GIODO, Warszawa 2017.

[8] K. Szwarc, P. Zaskórski, *Identyfikacja zagrożeń dla ciągłości działania organizacji*, „Studia Bezpieczeństwa Narodowego" 2012, r. 2, nr 3, s. 218.

procesu szacowania ryzyka i postępowania z nim. Ważne jest, by wynikiem procesu była rzetelna i obiektywna ocena poziomu ryzyka.

Zasadnicza różnica w dotychczas stosowanym podejściu polega na tym, że wcześniej stosowane metodyki zarządzania bezpieczeństwem informacji skupiały się na ryzyku i konsekwencjach dla organizacji, natomiast RODO kładzie duży nacisk na kwestie związane z ryzykiem naruszenia praw i wolności osób, których dane dotyczą.

Właściwe zarządzanie ryzykiem wymaga odniesienia się do kontekstu przetwarzania, a następnie przeprowadzenia identyfikacji, estymacji (które składają się na analizę ryzyka) i oceny ryzyka. Po zakończeniu tych etapów należy podjąć decyzję w kwestii postępowania z oszacowanym ryzykiem i akceptacji ryzyka szczątkowego.

Określenie kontekstu wymaga wskazania wszystkich aktywów informacyjnych z uwzględnieniem zakresu, charakteru, celów przetwarzanych danych oraz wyszczególnienia zagrożeń związanych z utratą, zniszczeniem bądź nieuprawnionym dostępem do danych. Identyfikacja i klasyfikacja aktywów informacyjnych w danej organizacji powinna być przeprowadzona na poziomie szczegółowości zapewniającym wyróżnienie niezbędnych informacji dla celów analizy ryzyka. Administrator na tym etapie powinien zwrócić uwagę na aktualny stan posiadanych zabezpieczeń oraz określić kryteria ryzyka akceptowalnego.

Kolejnym krokiem jest identyfikacja potencjalnych zagrożeń oraz wskazanie podatności dla aktywów, wynikających z urzeczywistnienia się tych zagrożeń. W celu oceny ryzyka przypisuje się wartości dla prawdopodobieństwa wystąpienia danego zdarzenia oraz wartości dla potencjalnych skutków materializacji zagrożenia w podziale dla każdego z atrybutów bezpieczeństwa. Szacunek ryzyka stanowi iloczyn tych wartości. W zależności od szacunków podejmuje się decyzje odnośnie do postępowania z poszczególnymi ryzykami (redukcja, zachowanie, unikanie bądź przeniesienie ryzyka)[9].

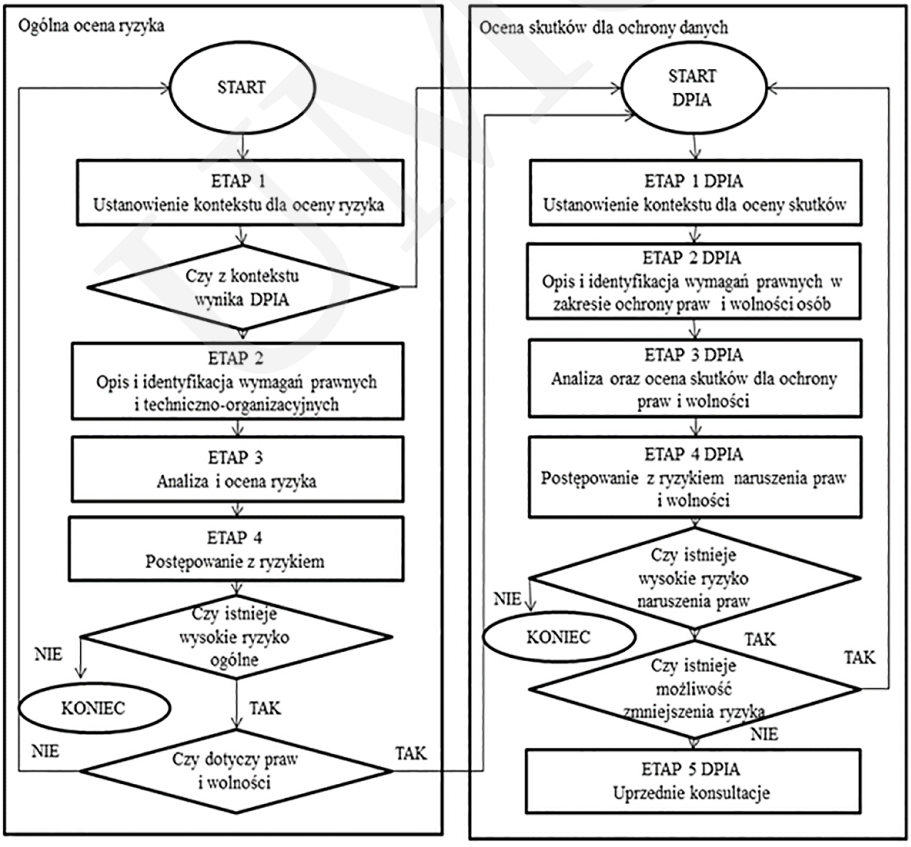
Analiza ryzyka dla przetwarzanych danych osobowych stanowi punkt wyjścia do decyzji o konieczności przeprowadzenia dalszej, bardziej sformalizowanej analizy ryzyka. Na mocy art. 35 Rozporządzenia 2016/679 wprowadzono pojęcie „oceny skutków dla ochrony danych osobowych". Przeprowadzenie tego procesu wymagane jest w przypadku, gdy przetwarzanie może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. O ile nie istnieje formalny wymóg przeprowadzania analizy ryzyka wszystkich czynności przetwarzania, w praktyce stanowi ona konieczność z uwagi na ocenę, czy określony proces przetwarzania nie jest narażony na wysokie ryzyko, a co za tym idzie nie wymaga od administratora przeprowadzenia oceny skutków dla ochrony danych osobowych. Zatem nałożenie nowego obowiązku powoduje, że w praktyce podmioty przetwarzające dane osobowe muszą nieustannie przeprowadzać analizę i ocenę ryzyka dla przetwarzanych danych. Działania, obejmujące kontekst przetwarzania, mechanizmy kontrolne, szacowanie ryzyka, postępowanie z ryzykiem stale się zapętlają i mają na celu permanentne monitorowanie i ulepszanie procesu (koło Deminga).

[9] *Poradnik RODO. Podejście…*, cz. 2, s. 5–25.

4. Ocena skutków dla ochrony danych

Ocena skutków dla ochrony danych powinna być przeprowadzana w przypadku, gdy istnieje duże prawdopodobieństwo wysokiego ryzyka dla naruszenia praw i wolności osób, których dane przetwarza administrator. Zastosowanie powinna znaleźć w szczególności w przypadku przetwarzania danych z wykorzystaniem nowych technologii. Niezależnie od tego wyróżniono kilka przypadków, które zawsze wymagają przeprowadzenia pogłębionej analizy ryzyka. Zalicza się do nich:

- podejmowanie decyzji na podstawie danych przetwarzanych w sposób zautomatyzowany, na podstawie kompleksowej i systematycznej oceny czynników osobowych osób fizycznych (w tym również profilowanie),
- przetwarzanie danych wrażliwych oraz danych o wyrokach skazujących i naruszeniach prawa na dużą skalę,



Rysunek 1. Ogólna ocena ryzyka oraz ocena skutków dla ochrony danych.
Źródło: *Poradnik RODO. Podejście*…, cz. 2.

Zgodnie z przedstawionym schematem ocenę skutków dla ochrony danych przeprowadza się po dokonaniu ogólnej oceny ryzyka, w przypadku oszacowania wysokiego ryzyka ogólnego, chyba że wymóg realizacji pogłębionej analizy wynika z przepisów prawa. Konsultacje z Prezesem Urzędu Ochrony Danych Osobowych są wymagane w sytuacji, gdy administrator nie ma możliwości, by zmniejszyć ryzyko naruszenia praw i wolności osób fizycznych w wyniku przetwarzania ich danych.

Wprowadzony wymóg analizy ryzyka jest objęty taką powagą, iż w przypadku wystąpienia wysokiego poziomu ryzyka naruszenia praw i wolności osób fizycznych, a podjęte przez administratora środki administracyjno-techniczne nie są w stanie zmniejszyć ryzyka do akceptowalnego poziomu, z takiej operacji przetwarzania podmiot zmuszony będzie zrezygnować.

Administrator, w szczególnych przypadkach, zanim rozpocznie operację przetwarzania, musi zasięgnąć opinii osób fizycznych, których dana operacja będzie dotyczyć, ich przedstawicieli bądź ekspertów. O opinie można wystąpić w dowolny sposób. Takie konsultacje mają na celu uwzględnienie perspektywy innych osób. Zaleca się jednak, aby w sytuacji wątpliwości tego, czy ocena skutków powinna być prowadzona, rekomendowano jej wdrożenie.

Przeprowadzenie przez administratora oceny skutków dla ochrony danych osobowych jest wymagane przed rozpoczęciem przetwarzania danego zbioru danych. Wynika to z zasad uwzględnienia ochrony danych w fazie projektowania (ang. *privacy by design*) oraz domyślnej ochrony danych (ang. *privacy by default*). DPIA jest procesem ciągłym, który umożliwia weryfikację adekwatności zastosowanych środków ochrony oraz poprawę zabezpieczeń nieodpowiednich do dynamicznie zmieniających się zagrożeń. Trzeba również zauważyć, iż w przypadku DPIA nie ma możliwości przeniesienia ryzyka przetwarzania na inny podmiot w drodze postępowania z ryzykiem, dlatego istotną kwestią jest przyłożenie szczególnej wagi do ochrony praw osób fizycznych nie tylko w momencie planowania określonej operacji przetwarzania, ale domyślnie, także w trakcie całego przetwarzania[10].

5. Ocena skutków dla ochrony danych w podmiotach sektora publicznego

Jak wspomniano we wcześniejszej części artykułu, obowiązek przeprowadzenia oceny skutków dla ochrony danych osobowych jest wymagany w przypadku, gdy czynności przetwarzania wypełniają przesłanki wskazane w art. 35 RODO lub kryteria wskazane w Komunikacie Prezesa Urzędu Ochrony Danych Osobowych w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony. W odniesieniu do podmiotów sektora publicznego, prowadzenie DPIA wymagane jest przykładowo w urzędach pracy w przypadku dokonywania profilowania osób bezrobotnych pod kątem dostępu do rozmaitych form pomocy, bez ich zgody. Ocenie skutków dla ochrony danych podlega również moni-

[10] K. Pszczółkowski, *Metodyka zarządzania ryzykiem w ochronie danych osobowych*, Fundacja Bezpieczeństwa Informacji Polska, Warszawa 2018, s. 31.

toring, realizowany za pomocą kamer umieszczonych na mundurach funkcjonariuszy publicznych, np. policji, straży miejskiej, straży pożarnej, gdyż wykorzystuje on elementy rozpoznawania właściwości i cech obiektów na obszarze objętym monitorowaniem. Co więcej, nagrywanie przez funkcjonariusza przebiegu interwencji może się wiązać z przetwarzaniem szczególnych kategorii danych, a więc również podlega obowiązkowi pogłębionej oceny ryzyka.

Z ochroną praw i wolności osób, których dane dotyczą, jest bezpośrednio związany obowiązek zabezpieczenia przetwarzanych danych, zawarty w art. 35 RODO. Poziom zabezpieczeń stosowany w sektorze publicznym budzi niepokój, o czym może świadczyć przeprowadzona w ubiegłym roku (tj. 2018 r.) kontrola NIK w zakresie ochrony elektronicznych zasobów informacyjnych. Skontrolowano wówczas 31 jednostek samorządowych na Podlasiu. W niemalże wszystkich jednostkach poziom zabezpieczeń systemów informatycznych i usług sieciowych był na niezadowalającym albo bardzo niskim poziomie[11]. Taki poziom ochrony stanowi ryzyko nieuprawnionego dostępu, kradzieży, utraty danych. Może zatem prowadzić do naruszenia prywatności i mienia obywateli, których dane są przetwarzane w systemach informatycznych.

Współcześnie niewiele podmiotów sektora publicznego posiada wystarczającą świadomość w sferze ochrony danych, których są administratorem. Nadal kwestie bezpieczeństwa informacji są lekceważone, a wymagania ogólnego rozporządzenia – oparte na analizie ryzyka przetwarzanych danych – nieprzestrzegane.

Jak wynika z ostatniego sprawozdania z działalności Prezesa Urzędu Ochrony Danych Osobowych w 2018 r., przeprowadził on kontrolę w zakresie przetwarzania danych osobowych w ramach miejskiego monitoringu wizyjnego w dwóch jednostkach samorządu terytorialnego. W toku kontroli ustalono uchybienia polegające na tym, że nie przeprowadzono oceny skutków dla ochrony danych przetwarzanych w ramach monitoringu. Dane przetwarzane za pomocą kamer wizyjnych, z uwagi na brak funkcjonalności rozpoznawania twarzy oraz śledzenia osoby, nie stanowią danych szczególnej kategorii (biometrycznych). Jednakże, mając na względzie, że kamery obejmują znaczną część miasta, przetwarzanie danych w postaci wizerunku obywateli odbywa się na szeroką skalę, wymaga zatem przeprowadzenia oceny skutków dla ochrony danych. Zgodnie bowiem z art. 35 ust. 3 lit c) RODO przeprowadzenie tej oceny jest wymagane w szczególności w przypadku systematycznego monitorowania na dużą skalę miejsc publicznie dostępnych[12].

Dodatkowo w sprawozdaniu podkreślono, że w dokumentacji z przeprowadzonej analizy ryzyka nie opisano działań naprawczych oraz nie dokonano oceny ryzyka dla poszczególnych zagrożeń, zidentyfikowanych dla czynności przetwarzania wymagających przeprowadzenia oceny skutków dla ochrony danych osobowych.

[11] *Informacje o obywatelach przechowywane przez instytucje samorządowe nie są bezpieczne*, 2018, https://www.cyberdefence24.pl/bezpieczenstwo-informacyjne/informacje-o-obywatelach-przechowywane-przez-instytucje-samorzadowe-nie-sa-bezpieczne, inf. 15 VI 2019.

[12] Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych, https://uodo.gov.pl/437, inf. 15 IX 2019.

Kolejnym przykładem uchybień w administracji publicznej okazały się ujawnione w związku z wprowadzeniem przez Ministra Finansów portalu e-PIT zagrożenia wynikające z doboru autoryzacji do portalu. Dostęp do deklaracji PIT podatnika był możliwy po podaniu kwoty przychodów za poprzednie lata oraz numeru PESEL podatnika. Taki katalog informacji niezbędnych do autoryzacji powodował, że krąg osób mogących uzyskać dostęp do danych mógł rozszerzyć się o pracodawcą czy księgową[13].

Wprowadzenie nowego rozwiązania związanego z przetwarzaniem danych osobowych milionów podatników powinno zostać poprzedzone przeprowadzeniem oceny skutków dla ochrony danych osobowych. Co prawda, dane zawarte w e-PIT nie stanowią z definicji danych szczególnej kategorii, jednakże biorąc pod uwagę podejście Polaków do kwestii wynagrodzeń – informacje te mają zwykle ważkie znaczenie i stanowią tę kategorię danych, które zwykle chronimy bardziej. Ryzyko dla praw i wolności podatników związane z przetwarzaniem ich danych powinno zostać uwzględnione już w fazie projektowania portalu (*privacy by design*). Być może taka analiza pozwoliłaby na zidentyfikowanie ryzyka, które zostało ujawnione na etapie użytkowania portalu. Dodatkowo dawałaby możliwość reakcji i minimalizacji prawdopodobieństwa wystąpienia negatywnych konsekwencji dla użytkowników portalu. Nawet jeśli podstawowa analiza wykazałaby wysoki poziom ryzyka naruszenia praw i wolności, to obowiązkowe konsultacje z organem nadzorczym mogłyby pomóc w identyfikacji słabych elementów projektowanego rozwiązania. Aktualnie kwestie zapewnienia prywatności użytkowników powinny stanowić element kluczowy przy projektowaniu nowych systemów informatycznych. Ma to ogromne znaczenie zwłaszcza dla systemów wykorzystywanych w administracji, głównie ze względu na skalę, w jakiej dane są przetwarzane. Dokonanie szczegółowej i rzetelnej analizy ryzyka oraz (w uzasadnionych przypadkach) oceny skutków dla ochrony danych osobowych pozwala reagować na ewentualne zagrożenia jeszcze w fazie produkcji, a dzięki temu zapobiegać materializacji zagrożeń zidentyfikowanych dla poszczególnych procesów przetwarzania.

Jak wynika z powyższych przykładów, prowadzenie analizy ryzyka i oceny skutków dla ochrony danych w sektorze publicznym nadal stanowi poważne wyzwanie. Biorąc pod uwagę fakt, że podmioty sektora publicznego przetwarzają dane osobowe wszystkich obywateli, a z poszczególnych procesów przetwarzania zwykle nie mają możliwości zrezygnować z uwagi na wysoki poziom oszacowanego ryzyka, przetwarzanie często będzie wymagało dodatkowych nakładów środków finansowych na zabezpieczenia.

6. Podsumowanie

Analiza ryzyka i ocena skutków ochrony danych osobowych stanowią użyteczne narzędzie dla administratorów danych, służące do wdrażania operacji przetwarzania zgodnych z obowiązującymi przepisami prawa. Proaktywne podejście do ochrony danych, oparte na zarządzaniu ryzykiem nie powinno być zatem traktowane jak przykry obo-

[13] S. Wikariak, *Niebezpieczeństwa wycieku informacji można było uniknąć*, https://prawo.gazetaprawna.pl/artykuly/1399802,niebezpieczenstwa-wycieku-informacji-mozna-bylo-uniknac.html, inf. 15 IX 2019.

wiązek, ale wsparcie w ochronie praw osób, których dane są przetwarzane. Obserwując złożoność procesów zarządzania informacjami w sektorze publicznym, implementacja metodyk szacowania ryzyka dla ochrony danych osobowych do istniejących systemów zarządzania ryzykiem wydaje się niezbędna.

Bez wątpienia zachowanie bezpieczeństwa przetwarzanych danych, mające na celu minimalizację ryzyka dla praw i wolności osób fizycznych wiąże się nie tylko z koniecznością prowadzenia oceny skutków dla ochrony danych osobowych, ale również analizy w obszarach związanych z możliwością utraty poufności, integralności, dostępności zasobów informacyjnych czy związanych z żądaniami osób na podstawie przepisów RODO. Tylko holistyczne podejście pozwoli administratorowi na wywiązanie się z ciążących na nim obowiązków i możliwości wykazania rozliczalności.

Jednostki sektora publicznego, zgodnie z Krajowymi Ramami Interoperacyjności, dla zapewnienia bezpieczeństwa informacji powinny być dostosowane do minimalnych wymagań dla rejestrów publicznych, wymiany informacji w postaci elektronicznej oraz systemów teleinformatycznych[14]. Te ogólnokrajowe wytyczne funkcjonują już od 2012 r., jednak jak wskazano w artykule, niektóre instytucje realizujące zadania publiczne wciąż mają problemy z zarządzaniem systemami informatycznymi. Stosunek kadry zarządzającej w podmiotach sektora publicznego (zwłaszcza w małych jednostkach) do kwestii zapewnienia bezpieczeństwa informacjami budzi niepokój.

Należy mieć na uwadze, że właściwe zarządzanie bezpieczeństwem danych osobowych w podmiotach sektora publicznego jest niezwykle trudnym zadaniem. Wynika to chociażby z faktu, że wiele urzędów ma bardzo rozbudowaną strukturę organizacyjną i skomplikowane procesy przetwarzania. Ponadto przetwarzają szczególne kategorie danych oraz dane na temat wyroków, wymagające wdrożenia szczególnych środków ochrony, co przy często ograniczonym budżecie może się okazać karkołomnym wyzwaniem. Abstrahując, stosowanie odpowiednich środków ochrony zmniejsza prawdopodobieństwo wystąpienia naruszeń, powodujących roszczenia klientów i utratę reputacji. Przeprowadzenie analizy ryzyka pozwala na identyfikację potencjalnych zagrożeń oraz podjęcie decyzji co do postępowania w przypadku jego wystąpienia. Dzięki rzetelnej analizie skraca się czas reakcji administratora w momencie materializacji jakiegoś zagrożenia, przez co osoby, których dane naruszono, mają większe możliwości, by zminimalizować ewentualne, negatywne skutki tego zdarzenia. W efekcie podmiot bazujący na modelu opartym na ryzyku ma większy wpływ na poziom bezpieczeństwa przetwarzanych danych osobowych, a co za tym idzie bezpieczeństwo osób, których dane przetwarza.

Konkludując, podmioty sektora publicznego, z uwagi na zakres, skalę i kategorie przetwarzanych danych osobowych osób fizycznych, powinny stale monitorować poziom zabezpieczeń przetwarzanych zasobów informacyjnych. Stosowanie analizy ryzy-

[14] Rozporządzenie 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 (Dz.U. 2012 poz. 526).

ka i oceny skutków dla ochrony danych stanowi instrument pozwalający ocenić, jakie działania należy podejmować dla ochrony praw i wolności obywateli. Wykorzystywanie metodyk szacowania ryzyka pozwala nie tylko wypełnić wymogi RODO, ale też podwyższać standardy funkcjonowania organizacji.

Niemniej jednak, pomimo iż nowe przepisy o ochronie danych osobowych funkcjonują już ponad rok, przytoczone przykłady przeprowadzonych kontroli w podmiotach sektora publicznego oraz wprowadzanie rozwiązań technologicznych z pominięciem zasad ochrony danych osobowych wskazują, że nie wszystkie podmioty posiadają już wypracowane i sprawdzone analizy ryzyka. Zatem opracowanie rzetelnych i adekwatnych analiz ryzyka i oceny skutków dla ochrony danych osobowych stanowi w dalszym ciągu aktualne wyzwanie dla podmiotów sektora publicznego, na których spoczywa obowiązek ochrony prywatności wszystkich osób, których dane przetwarzają.

~

Streszczenie: Wypracowane na szczeblu unijnym 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 danych oraz uchylenia dyrektywy 95/46/WE wprowadziło nowy, proaktywny model ochrony danych osobowych przetwarzanych w organizacji, oparty na podejściu bazującym na ryzyku. Nałożyło ono na administratorów nowe obowiązki, związane z prowadzeniem analiz ryzyka naruszenia praw i wolności osób, których dane przetwarzają. Biorąc pod uwagę zakres, skalę i kategorie przetwarzanych danych osobowych osób fizycznych, podmioty sektora publicznego stoją przed ogromnym wyzwaniem, by sprostać restrykcjom unijnego ustawodawcy. Dodatkowym utrudnieniem jest często bardzo rozbudowana struktura organizacyjna, skomplikowane procesy przetwarzania, ograniczone środki finansowe i niedostosowane systemy informatyczne. Artykuł porusza kwestie analizy ryzyka i oceny skutków dla ochrony danych osobowych przetwarzanych w sektorze publicznym, służącej spełnieniu wymagań RODO. Kluczową kwestią w tym zakresie jest przyjęcie odpowiedniej metodyki w procesie szacowania ryzyka, właściwie bowiem przeprowadzona umożliwia wdrożenie zabezpieczeń adekwatnych do potencjalnych zagrożeń.
Słowa kluczowe: analiza, ryzyko, ochrona, dane, RODO

Risk Analysis and Data Protection Impact Assessment Conducted in the Public Sector

Abstract: The European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and the repeal of Directive 95/46/EC, introduced a new one, a proactive model of protection of personal data processed in the organization, based on a risk-based approach. It imposed some new obligations on the administrators, related to conducting analysis of the risk of violation of the rights and freedoms of the persons, whose data they process. Considering the scope, scale and categories of personal data processed, public sector entities face a huge challenge to meet the restrictions of the EU legislator. An additional difficulty is often a very extensive organizational structure, complicated

processing processes, limited financial resources and unadjusted IT systems. The article discusses the issues of risk analysis and impact assessment for the protection of personal data processed in the public sector, in order to meet the requirements of the GDPR. The key issue in this respect is the adoption of an appropriate methodology in the risk estimation process, because properly carried out, it enables the implementation of security measures adequate to potential threats.
Keywords: analysis, risk, protection, data, RODO, GDPR

Анализ рисков и оценка воздействия на защиту данных в государственном секторе

Аннотация: Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных и о свободном потоке данных, а также об отмене Директивы 95/46 / ЕС, разработанной на уровне ЕС, ввел новую, проактивную модель защиты персональных данных, обрабатываемых в организации, на основе подхода, основанного на оценке рисков. Это возложило на контролеров новые обязанности, связанные с проведением анализа риска нарушения прав и свобод лиц, данные которых они обрабатывают. Учитывая объем, масштаб и категории обрабатываемых персональных данных физических лиц, организации государственного сектора сталкиваются с огромной проблемой соблюдения ограничений законодательного органа ЕС. Дополнительной трудностью часто является очень сложная организационная структура, сложные процессы обработки, ограниченные финансовые ресурсы и неадекватные ИТ-системы. В статье рассматриваются вопросы анализа рисков и оценки воздействия на защиту персональных данных, обрабатываемых в государственном секторе, направленных на выполнение требований GDPR. Ключевым вопросом в этом отношении является принятие соответствующей методологии в процессе оценки рисков, поскольку при правильном проведении она позволяет реализовать меры защиты, адекватные потенциальным угрозам.
Ключевые слова: анализ, риск, защита, данные, GDPR

Bibliografia

Byczkowski M., *Zabezpieczanie danych osobowych w RODO*, „IAP" 2017, nr 2.

Informacje o obywatelach przechowywane przez instytucje samorządowe nie są bezpieczne, 2018, https://www.cyberdefence24.pl/bezpieczenstwo-informacyjne/informacje-o-obywatelach-przechowywane-przez-instytucje-samorzadowe-nie-sa-bezpieczne.

Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P. 2019 poz. 666).

Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Wydawnictwo CH Beck, Warszawa 2016.

Litwiński P., *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Wydawnictwo CH Beck, Warszawa 2017.

Lubasz D., *RODO. Zmiany w zakresie ochrony danych osobowych. Porównanie przepisów. Praktyczne uwagi*, Wydawnictwo Wolters Kluwer, Warszawa 2018.

Poradnik RODO. Podejście oparte na ryzyku, red. J. Zawiła-Niedźwiecki, cz. 1, GIODO, Warszawa 2017.

Poradnik RODO. Podejście oparte na ryzyku, red. J. Zawiła-Niedźwiecki, cz. 2, GIODO, Warszawa 2017.

Pszczółkowski K., *Metodyka zarządzania ryzykiem w ochronie danych osobowych*, Fundacja Bezpieczeństwa Informacji Polska, Warszawa 2018.

RODO. Przewodnik ze wzorami, red. M. Gawroński, Wydawnictwo Wolters Kluwer, Warszawa 2018.

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 (*Dz.U.* L 119/1 z 4.5.2016).

Rozporządzenie 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 (Dz. U. 2012 poz. 526).

Sienkiewicz P., *Ewaluacja ryzyka w zarządzaniu kryzysowym*, [w:] *Ryzyko w zarządzaniu kryzysowym*, red. P. Sienkiewicz, M. Marszałek, P. Górny, Wydawnictwo Adam Marszałek, Toruń 2012.

Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych, https://uodo.gov.pl/437.

Szwarc K., Zaskórski P., *Identyfikacja zagrożeń dla ciągłości działania organizacji*, „Studia Bezpieczeństwa Narodowego" 2012, r. 2, nr 3.

Wikariak S., *Niebezpieczeństwa wycieku informacji można było uniknąć*, https://prawo.gazetaprawna.pl/artykuly/1399802,niebezpieczenstwa-wycieku-informacji-mozna-bylo-uniknac.html.

Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679 (WP 248 rev.01), http://www.giodo.gov.pl/pl/file/12864.

Zawiła-Niedźwiecki J., *Analiza ryzyka służąca spełnianiu wymagań RODO*, 2018, https://sip.legalis.pl/document-view.seam?documentId=mjxw62zogi3damjzhaydooa.