Aleksandra Klich[1]
Uniwersytet Szczeciński
ORCID ID: 0000-0002-2931-712X

Bartosz Skrendo[2]
Szczecin
ORCID ID: 0009-0005-6697-5307

OD NARUSZENIA BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH
DO NAŁOŻENIA KARY PRZEZ PREZESA UODO – ZAGADNIENIA PRAKTYCZNE

ABSTRACT

From a breach of security of processed personal data to the imposition of a penalty by the President of the Office for Personal Data Protection – practical issues

In the study, the authors focus on the practical aspects of personal data security management in the context of Polish legal regulations. They analyzed the concept of a personal data security incident and breach along with the necessary steps leading from a data security breach to the possible imposition of a penalty by the President of the Office for Personal Data Protection (UODO). The authors pointed out that to avoid sanctions, a personal data processor must not only comply with

1 Doktor, adiunkt na Wydziale Prawa i Administracji Uniwersytetu Szczecińskiego, radca prawny w szczecińskiej kancelarii MCM Legal Mazurkiewicz Cieszyński Mazuro, adres do kontaktu: aleksandra.klich@usz.edu.pl.

2 Radca prawny w szczecińskiej kancelarii MCM Legal Mazurkiewicz Cieszyński Mazuro, adres do kontaktu: bartosz.skrendo@mcmlegal.pl.

the minimum legal requirements but also focus on implementing measures to ensure an adequate level of security. The authors indicate the need for effective data protection through monitoring, rapid response to incidents and employee education. The authors point out that awareness of data security risks and effective preventive measures can help avoid sanctions from the President of the UODO. The conclusions of the publication provide a practical guide for data processors seeking to effectively protect personal data in a dynamic legal environment.

Keywords: personal data security, data security breaches, administrative fines, GDPR

Słowa kluczowe: bezpieczeństwo danych osobowych, naruszenia bezpieczeństwa danych, administracyjne kary pieniężne, RODO

1. Wprowadzenie

We współczesnym społeczeństwie cyfrowym, w którym dane osobowe odgrywają coraz większą rolę w życiu codziennym i biznesowym, ich ochrona prywatności i bezpieczeństwa jest niezmiernie istotna. Unijne rozporządzenie ustalające jednolite zasady w zakresie ochrony danych osobowych[3], które weszło w życie w maju 2018 r., wprowadziło nowe standardy ochrony danych osobowych w państwach członkowskich Unii Europejskiej (UE). Celem uchwalenia RODO było bowiem zharmonizowanie i wzmocnienie ochrony danych osobowych w Unii Europejskiej (UE), a także dostosowanie przepisów do zmieniającej się rzeczywistości związanej z przetwarzaniem danych osobowych. Rozporządzenie zostało przyjęte, aby sprostać nowym wyzwaniom związanym z cyfryzacją, globalizacją i rosnącym znaczeniem danych osobowych w gospodarce i społeczeństwie. Jednym z kluczowych elementów RODO jest określenie przesłanek i sposobu nakładania kar. W konsekwencji krajowe organy nadzoru (w przypadku Polski jest to Prezes Urzędu Ochrony Danych Osobowych[4]) legitymowane są do nakładania kar w przypadku naruszeń przepisów dotyczących ochrony danych osobowych.

Nie ulega wątpliwości to, że aktualnie RODO postrzegane jest jako najbardziej konsekwentna zmiana regulacyjna w polityce informacyjnej od pokolenia. Wprowadza ono dane osobowe do złożonego i ochronnego systemu regulacyjnego[5]. Mimo że postanowienia zawarte w unijnym rozporządzeniu nie są nowatorskie, odegrało ono istotną rolę nie tylko na arenie europejskiej w zakresie harmonizacji regulacji ustalających zasady bezpiecznego przetwarzania danych osobowych, ale staje się przedmiotem dyskusji na arenie międzynarodowej. Nie oznacza to, że jest to legislacyjne rozwiązanie pozbawione wadliwości i niespójności.

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

4 Dalej: Prezes Urzędu, PUODO lub Prezes UODO.

5 Ch. J. Hoofnagle, B. van der Sloot, F. Zuiderveen Borgesius, *The European Union general data protection regulation: what it is and what it means*, „Information & Communications Technology Law" 2019, vol. 28, no. 1, DOI: 10.1080/13600834.2019.1573501, s. 65.

Podejmując próbę wyodrębnienia etapów postępowania w przypadku stwierdzenia naruszenia, zasadne wydaje się przyjęcie, że do najważniejszych należą:

I. wykrycie incydentu,
II. ocena incydentu,
III. powiadomienie organu nadzorczego,
IV. powiadomienie osób fizycznych,
V. analiza przyczyn incydentu,
VI. wdrożenie działań naprawczych,
VII. wnioski i raportowanie.

Podstawowym obowiązkiem administratorów danych osobowych jest dbałość o zapewnienie bezpieczeństwa procesów przetwarzania danych osobowych. Naruszenie tego obowiązku skutkować może nałożeniem kary przez Prezesa UODO. Problematyka ta jest przedmiotem licznych zainteresowań przedstawicieli nauki i praktyki. Przedmiotem publikacji jest przedstawienie szczegółowej analizy zasad nakładania kar przez Prezesa UODO w kontekście przepisów unijnego rozporządzenia.

Podstawową hipotezą badawczą, która ma być udowodniona w przygotowanym opracowaniu, jest udowodnienie, że samo stwierdzenie naruszenia bezpieczeństwa danych osobowych nie wiąże się każdorazowo z nałożeniem administracyjnej kary pieniężnej. Dążenie do jej udowodnienia wiąże się z błędnym utożsamianiem faktu stwierdzenia naruszenia z nałożeniem administracyjnej kary pieniężnej. Założeniem autorów jest dokładne omówienie procesu zachodzącego od momentu naruszenia bezpieczeństwa danych osobowych do nałożenia kary przez Prezesa UODO i ustalenie, czy wszczęcie postępowania wyjaśniającego automatycznie wiąże się z nałożeniem kary administracyjnej. Autorzy koncentrują się na analizie przepisów prawnych dotyczących naruszeń bezpieczeństwa danych osobowych, a także regulacji dotyczących kar administracyjnych nakładanych przez Prezesa UODO. Celem jest również przeprowadzenie analizy procesu postępowania przed organem nadzoru, z uwzględnieniem poszczególnych jego etapów, przy jednoczesnym zestawieniu zagadnień teoretycznoprawnych z praktycznymi i sformułowaniu zaleceń dla administratorów danych osobowych. Podstawowym zamierzeniem autorów jest skoncentrowanie się na procedurach i kryteriach, jakimi kieruje się Prezes UODO przy podejmowaniu decyzji o nałożeniu kary, oraz na roli, jaką pełni UODO w egzekwowaniu przepisów o ochronie danych osobowych. Wnioski wypływające z tej analizy mogą być cenne zarówno dla przedstawicieli zawodów prawniczych, jak i pozostałych praktyków zajmujących się ochroną danych osobowych, a także dla przedstawicieli świata nauki, dążących do lepszego zrozumienia mechanizmów egzekwowania przepisów RODO i ich wpływu na zachowanie podmiotów przetwarzających dane osobowe.

2. Skutki wykrycia incydentu bezpieczeństwa

Częstotliwość incydentów naruszeń bezpieczeństwa w zakresie przetwarzanych danych osobowych zależy od wielu czynników, w tym od rodzaju organizacji, rodzaju i zakresu przetwarzanych danych, jak i od poziomu zabezpieczeń oraz działań podejmowanych

w celu ich ochrony. Nie jest możliwe jednoznaczne określenie, jak często dochodzi do incydentów naruszeń bezpieczeństwa, podobnie jak nie jest możliwe stworzenie uniwersalnego modelu umożliwiającego bieżące tworzenie katalogu działań zaradczych. Uzasadnieniem dla tej tezy jest różnorodność źródeł naruszeń, na co wpływ może mieć m.in. region, obszar przetwarzania danych osobowych czy też specyfika danej branży. Nie ulega jednak wątpliwości, że incydenty naruszeń bezpieczeństwa są coraz bardziej powszechne, zwłaszcza w erze cyfrowej, w której wiele organizacji przechowuje i przetwarza duże ilości danych w systemach informatycznych i chmurach obliczeniowych. Przykłady incydentów naruszeń bezpieczeństwa obejmują ataki hakerskie, wycieki danych, utratę sprzętu z danymi, błędy ludzkie czy też naruszenia wynikające z nieprawidłowego postępowania wewnętrznego. Z praktycznego punktu widzenia możliwe jest stwierdzenie, że ponad połowa wszystkich ataków i zagrożeń jest inicjowana przez personel wewnętrzny, jednak duża część będzie również inicjowana przez wspólne działania personelu wewnętrznego i zewnętrznego[6]. Dostrzegalna jest rosnąca świadomość zapewnienia bezpieczeństwa przetwarzanym danym nie tylko wśród administratorów danych, ale i podmiotów oferujących narzędzia wspierające mechanizmy prawidłowego i efektywnego organizowania i ochrony przetwarzanych danych osobowych.

W związku z tym istotne jest to, aby administratorzy danych osobowych stosowali odpowiednie środki zabezpieczeń, a także prowadzili regularne działania monitorujące, a także audytowo-szkoleniowe pracowników w zakresie ochrony przetwarzanych danych. Wskutek nieuchronnego i dynamicznego postępu i rozwoju technologicznego niezbędne staje się także dokonywanie regularnej oceny ryzyka oraz dostosowanie strategii bezpieczeństwa do zmieniającego się środowiska technologicznego. Nie ulega wątpliwości, że działania z tego obszaru pomagają zmniejszyć ryzyko incydentów naruszeń bezpieczeństwa. Istotna jest także aktywność informacyjna, mająca na celu uświadomienie pracownikom obowiązków wynikających z przetwarzania danych osobowych. W tym celu podstawowe znaczenie mają szkolenia obejmujące przepisy dotyczące ochrony danych osobowych, polityki i procedury organizacji, a także konkretne obowiązki pracowników związane z przetwarzaniem danych osobowych. Z perspektywy występujących naruszeń bezpieczeństwa danych istotne jest bieżące monitorowanie i omawianie zaistniałych w organizacji zdarzeń w celu wyeliminowania ich powstawania w przyszłości. „Pracownicy powinni być także świadomi potencjalnych zagrożeń i ryzyka związanego z przetwarzaniem danych osobowych. W tym celu rekomendacją jest przeprowadzanie kampanii informacyjnych zmierzających do podniesienia świadomości pracowników w zakresie zagrożeń związanych z naruszeniem bezpieczeństwa danych. Kluczowe znaczenie ma także wdrożenie procedur postępowania w przypadku naruszeń. Wszystkie osoby mające styczność z danymi osobowymi powinny być uświadomione o potencjalnych, najbardziej prawdopodobnych naruszeniach ochrony danych osobowych właściwych dla swojego obszaru działania oraz zobowiązane do niezwłocznego powiadamiania o potencjalnych naruszeniach bezpośredniego. Wskazane przykładowo rozwiązania, które powinny być wdrożone przez administratorów danych osobowych, mają charakter wspierający administratora danych osobowych. Pomagają one bowiem pracownikom

6 C. Pelnekar, *Planning for and Implementing ISO 27001*, „ISACA Journal" 2011, t. 4, nr 4, s. 1–8.

zrozumieć, jak powinni oni przestrzegać przepisów dotyczących ochrony danych osobowych, jakie są ryzyka i konsekwencje naruszeń oraz jakie kroki powinni podejmować w przypadku incydentów.

W konsekwencji każda z tych osób, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych w systemie informatycznym lub przetwarzanych w inny sposób, powinna mieć świadomość natychmiastowej konieczności przerwania wykonywania czynności związanych z przetwarzaniem danych osobowych i niezwłocznego poinformowania o tym fakcie administratora, bezpośredniego przełożonego oraz IOD albo inną upoważnioną przez administratora osobę. Osoba zatrudniona przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych, powinna także mieć świadomość o spoczywającym na niej obowiązku niezwłocznego poinformowania o tym administratora, bezpośredniego przełożonego oraz IOD albo inną upoważnioną przez niego osobę. Aby powiadomienie o naruszeniu ochrony danych osobowych było skuteczne, powinno obejmować: opis naruszenia ochrony danych osobowych, określenie sytuacji, miejsca i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych i wszelkich istotnych informacji mogących wskazywać na przyczynę tego naruszenia, a także określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia. Budowanie świadomości wśród zespołu osób przetwarzających dane osobowe skutkować będzie wypracowaniem pozytywnych postaw, związanych m.in. z efektywną umiejętnością podjęcia działań w celu powstrzymania lub ograniczenia dostępu do danych przez osoby niepowołane poprzez np. fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nieuprawnionej, wylogowanie użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych, zmianę hasła do konto IOD i użytkownika, poprzez które uzyskano nielegalny dostęp, w celu uniknięcia ponownej próby włamania, jak również podjęcia innych stosownych do sytuacji działań. Najgorszym bowiem z możliwych rozwiązań jest brak realizacji obowiązku informacyjnego względem administratora i/lub IOD, co niweczy jakąkolwiek możliwość odpowiedniego zareagowania, a w efekcie zwiększa ryzyko nałożenia kary administracyjnej w przypadku zgłoszenia faktu naruszenia do organu nadzoru przez osobę, której dane zostały przetworzone w sposób niezgodny z prawem.

Podjęcie powyższych działań realizowanych na etapie I związanym z wykryciem naruszenia ma charakter czynności sprawdzających, zmierzających do wstępnego ustalenia, czy w istocie administrator ma do czynienia z naruszeniem bezpieczeństwa danych osobowych warunkujących konieczność zgłoszenia tego faktu organowi nadzoru. Na dalszym etapie wdrażania odpowiednich działań naprawczych, zarówno z brzmienia motywu 85, jak i art. 33 ust. 1 RODO, należy zdekodować najbardziej istotne kwestie, aby rozstrzygnąć, kiedy aktualizuje się obowiązek notyfikacji organowi nadzoru zdarzenia mogącego nosić znamiona naruszenia bezpieczeństwa danych. Dopiero po pozytywnym rozstrzygnięciu tego etapu możliwe będzie podjęcie rozważań dotyczących oceny incydentu, a także wdrożenia dalszej procedury postępowania w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych, której ostatecznym etapem jest dokonanie zgłoszenia do organu nadzoru.

3. Rodzaje naruszeń bezpieczeństwa przetwarzania danych a obowiązek notyfikacji

Naruszenia przepisów dotyczących ochrony danych osobowych mogą mieć różne źródła i skutki, a Prezes UODO odgrywa kluczową rolę w egzekwowaniu przepisów krajowych i unijnych, a także w zakresie prowadzenia postępowań wyjaśniających oraz nakładania kar na podmioty, które ich nie przestrzegają. Kary administracyjne są bowiem ważnym narzędziem, mającym na celu zachęcenie podmiotów przetwarzających dane osobowe do przestrzegania przepisów o ochronie danych oraz zapewnienie ochrony prywatności obywateli UE. W praktyce prawodawca unijny niestety komplikuje zagadnienia związane z ochroną danych osobowych poprzez niejednoznaczne sformułowania i złożone zależności między niektórymi artykułami i motywami[7]. Podejmując próbę w zakresie zdefiniowania pojęcia naruszenia bezpieczeństwa danych osobowych, należy wyjść od art. 32 RODO, w którym prawodawca unijny przykładowo wskazuje środki techniczne i organizacyjne, które mogą służyć zapewnieniu odpowiedniego stopnia bezpieczeństwa odpowiadającego ryzyku. Jednym z nich jest zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Prawodawca unijny nie definiuje jednak pojęcia „fizycznego lub technicznego incydentu", pozostawiając w tym zakresie dowolność interpretacyjną. W literaturze przedmiotu dostrzegalna jest próba ustalenia zakresu pojęciowego wskazanego zagadnienia. Zasadne wydaje się to, aby incydenty te rozumieć jako naruszenie fizycznej lub technicznej ochrony danych, ich integralności i/lub poufności[8]. Nie oznacza to jednak, że każdy incydent przesądzać będzie o konieczności jego notyfikacji i utożsamiania z naruszeniem wymagającym zgłoszenia do organu nadzoru w ciągu 72 godzin od jego stwierdzenia. Z tego też względu, podejmując rozważania dotyczące naruszeń bezpieczeństwa przetwarzania danych, niezbędne jest podjęcie próby udzielenia odpowiedzi na pytanie o to, czy każdy incydent to naruszenie?

Podkreślenia wymaga konieczność wyraźnego oddzielenia terminów „incydent i zdarzenie" od „naruszenie ochrony danych osobowych". Naruszenie jest bowiem efektem zaistnienia określonego zdarzenia (incydentu), które osiąga skutek w sposób jednoznacznie kwalifikujący je w kategorii naruszenia wymagającego notyfikacji. W praktyce niejednokrotnie dochodzi do zbyt pochopnego kwalifikowania zgłoszonego incydentu w kategoriach naruszenia wymagającego podjęcia działań, o których mowa w art. 33 i nast. RODO. Z tego też względu słuszne wydaje się być stwierdzenie, że nie każdy incydent przesądza o naruszeniu, zaś każde stwierdzone naruszenie jest skutkiem zaistnienia określonego incydentu. Bezpieczeństwo informacji w sposób naturalny wiąże się z zapewnieniem bezpieczeństwa przetwarzanym danym osobowym. Z tego też względu wyznacznikiem w zakresie próby określenia zakresu wskazanych pojęć mających związek

7 B.-J. Koops, *The trouble with European data protection law*, „International Data Privacy Law" 2014, vol. 4, no. 4, s. 250–261.

8 P. Barta, M. Kawecki, P. Litwiński, *Komentarz do art. 32 RODO*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021, Legalis, Nb. 2.

z naruszeniem bezpieczeństwa danych mogą być normy z rodziny ISO/IEC 27000, pojmowane jako standardy międzynarodowe cieszące się rosnącym uznaniem i przyjęciem. Są one określane jako „wspólny język organizacji na całym świecie" w zakresie bezpieczeństwa informacji, a także charakteryzują się kompleksowym podejściem do problematyki systemu zarządzania bezpieczeństwem informacji[9]. Szczególnie istotne znaczenie ma jednak definicja pojęcia incydentu związanego z bezpieczeństwem zawarta w normie PN-ISO/ IEC 27000, dotyczącej systemów zarządzania bezpieczeństwem informacji (ISMS) i ich wymagań. Zdefiniowano w niej pojęcie incydentu związanego z bezpieczeństwem informacji, rozumianego jako pojedyncze zdarzenie lub seria niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, stwarzających znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażających bezpieczeństwu informacji. Należy pamiętać, że każde naruszenie danych jest również naruszeniem bezpieczeństwa, ale nie każde naruszenie bezpieczeństwa jest zawsze naruszeniem danych osobowych[10].

Mówiąc o incydentach w obszarze bezpieczeństwa informacji w wymiarze praktycznym w obszarze organizacyjnym, dostrzegalne są takie sytuacje jak: gromadzenie danych osobowych bez zgody osoby, której dane dotyczą, i bez poinformowania jej o przysługujących jej prawach, nieprzestrzeganie postanowień ustanowionych procedur bezpieczeństwa w zakresie odzyskiwania danych, nieprzestrzeganie terminów ustalonych w celu rozwiązania i zrealizowania praw osób, których dane dotyczą, nielegalne wykorzystanie danych osobowych. Z kolei w przypadku obszaru technicznego naruszenia mogą polegać na próbie lub naruszeniu fizycznej kontroli dostępu i baz danych, zmianie baz danych (usunięciu, modyfikacji lub dodania danych, które mogą mieć wpływ na jakość bazy danych), usuwaniu danych z nośników bez odpowiedniej autoryzacji, wyodrębnianiu danych na nośnikach innych niż autoryzowane, niewłaściwym zarządzaniu kopiami zapasowymi, utracie aktywów materialnych (telefonu służbowego, laptopa etc.) czy braku możliwości uzyskania dostępu do systemu przy użyciu zwykłej nazwy użytkownika/ hasła lub możliwości naruszenia hasła dostępu.

Podejmując próbę sklasyfikowania grup incydentów w ochronie danych osobowych, można wyróżnić:

1. zdarzenia losowe zewnętrzne (np. pożar, zalanie wodą, utrata łączności czy zasilania),
2. zdarzenia losowe wewnętrzne (awaria komputera/serwera/dysku twardego/oprogramowania, pomyłki informatyków, utrata danych),
3. umyślne incydenty (np. kradzież danych i sprzętu, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie danych, włamanie do systemu informatycznego lub pomieszczeń).

9 K. Bobkowski, *Zarządzanie bezpieczeństwem informacji w ujęciu wybranych aktów normatywnych w zakresie Systemu Zarządzania Bezpieczeństwem Informacji*, „Zarządzanie i Finanse – Journal of Management and Finance" 2018, vol. 16, no. 3, s. 17 i n.

10 Grupa Robocza Art. 29, *Wytyczne dotyczące powiadamiania o naruszeniu ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 z dnia 3 października 2017 r.*, WP250rev.01, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 [dostęp: 29 września 2023 r.].

Istotne znaczenie mają także postanowienia wytycznych koncentrujących się na incydentach naruszenia ochrony danych osobowych oraz na tym, w jaki sposób państwa członkowskie UE muszą być przygotowane nie tylko do skutecznego reagowania i zgodnie ze swoimi zobowiązaniami prawnymi, ale także do proaktywnego zapobiegania takim incydentom. W opinii 03/2014 dotyczącej zgłaszania naruszeń ochrony danych osobowych Grupa Robocza Art. 29 wskazała, że naruszenia można skategoryzować ze względu na trzy powszechnie znane zasady bezpieczeństwa informacji, tj. naruszenie poufności (nieuprawnione lub przypadkowe ujawnienie lub udostępnienie danych osobowych), naruszenie integralności (nieuprawniona lub przypadkowa modyfikacja danych osobowych) oraz naruszenie dostępności (przypadkowa lub nieuprawniona utrata dostępu do danych[11]).

Możliwe jest także stwierdzenie, zgodnie z którym naruszenie bezpieczeństwa informacji, które nie zagraża danym osobowym, również nie wchodzi w zakres tego obowiązku. To, czy naruszenie było zamierzone, czy nie, nie ma w takim przypadku znaczenia. Kwestią mającą fundamentalne znaczenie jest bowiem ustalenie, czy naruszenie to było bezpośrednio związane z zagrożeniem bezpieczeństwa informacji. Jeśli zaś zdarzenie nosiło znamiona incydentu, ale pozostającego poza wpływem na kwestię bezpieczeństwa danych osobowych, a w szczególności potencjalnego zagrożenia prywatności osób, których dane dotyczą, wówczas poza rozważaniami powinna pozostawać kwestia ewentualnego zgłaszania naruszenia organowi nadzoru.

Niewątpliwie ustawodawca, posługując się pojęciami incydentu bezpieczeństwa i naruszenia ochrony danych osobowych, prowadzi do mylnego utożsamiania obu pojęć. O ile w art. 4 pkt 12 RODO określono, że naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych definiowane jest jako naruszenie ochrony danych osobowych, o tyle nie oznacza to, że jest to naruszenie, o którym mowa w art. 33 ust. 1 RODO, którego stwierdzenie aktualizuje konieczność zgłoszenia do Prezesa UODO. Zdarzenia stanowiące incydenty bezpieczeństwa, które podlegają zgłoszeniu, powinny być bowiem każdorazowo analizowane i oceniane z perspektywy skutków, które są z nimi związane. Z tego też względu każdy incydent powinien podlegać zindywidualizowanej ocenie prowadzącej do ustalenia istnienia skutków wyszczególnionych przez prawodawcę unijnego definiującego pojęcie naruszenia danych osobowych. Oznacza to zatem, że dopiero w momencie ustalenia, że dany incydent (np. kradzież laptopa czy zgubienie pendrive`a) skutkuje jednym z rezultatów wymienionych enumeratywnie w art. 4 pkt 12 RODO, np. nieuprawnionym ujawnianiem lub nieuprawnionym dostępem do danych osobowych, aktualizuje się konieczność jego notyfikacji.

Odkąd zaczęło obowiązywać RODO, muszą zostać spełnione nowe wymogi dotyczące powiadomień i komunikacji w przypadku naruszenia danych. Ponieważ każde naruszenie jest inne, odpowiednie postępowanie z nim może okazać się trudne, szczególnie pod względem konsekwencji i oceny ryzyka. Aby ustalić, czy należy powiadomić organ ochrony danych o naruszeniu danych i czy należy o tym poinformować osoby, których

11 Grupa Robocza Art. 29, *Wytyczne dotyczące…*

dane dotyczą, administrator musi ocenić ryzyko naruszenia praw i wolności osób fizycznych zgodnie z art. 33 i 34 RODO. Ocena ta jest również kluczowa dla wdrożenia środków technicznych i organizacyjnych zgodnie z przepisami dotyczącymi odpowiedzialności administratorów, ochrony danych w fazie projektowania i bezpieczeństwa przetwarzania na podstawie art. 24 ust. 1, art. 25 ust. 1 i ust. 2 RODO, a także w celu ustalenia, czy należy przeprowadzić ocenę skutków dla ochrony danych (art. 35 RODO) i czy należy uruchomić mechanizm uprzednich konsultacji, o którym mowa w art. 36 RODO[12]. Działania administratora podejmowane tuż po powzięciu informacji o potencjalnym naruszeniu bezpieczeństwa danych osobowych mogą mieć charakter przygotowawczy, zmierzający do ustalenia, z jakim naruszeniem ma on do czynienia. Etap ten jest niezwykle istotny z praktycznego punktu widzenia, bowiem zgodnie z motywem 85 RODO przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne. Z praktycznego punktu widzenia wydaje się, że większość tych skutków będzie mogła wystąpić z dużym prawdopodobieństwem w przypadku każdorazowego wystąpienia naruszenia bezpieczeństwa danych osobowych.

Z tego względu administrator we wstępnej ocenie zaistniałego zdarzenia musi dokonać analizy stopnia wpływu incydentu na ryzyko naruszenia praw lub wolności osoby, której dane dotyczą. Analiza powinna koncentrować się na tym, jakie ryzyko dla osób fizycznych stwarza naruszenie danych. W przypadku naruszenia danych osobowych prawdopodobieństwo wystąpienia ryzyka związanego z naruszeniem wynosi 100%, pozostawiając wagę jako jedyną zmienną. Potencjalny wpływ na prawa i wolności osób, których dane dotyczą, waha się zatem od braku ryzyka przez ryzyko aż do wysokiego ryzyka[13]. W tym miejscu warto wskazać, że przez „ryzyko naruszenia praw lub wolności" należy rozumieć wszystkie sytuacje, w których incydent bezpieczeństwa może nieść ze sobą istotne negatywne skutki dla osoby, której dane zostały naruszone (np. popełnienie przestępstwa na jej szkodę, kradzież tożsamości, naruszenie dobrego imienia itd.). Prawodawca unijny w motywie 75 RODO uszczegóławia powyższe sformułowanie, konkretyzując je określonymi skutkami, które mogą wystąpić w wyniku przetwarzania danych (np. dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości, strata finansów, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnione odwrócenie pseudonimizacji lub wszelka inna znaczna szkoda gospodarcza lub społeczna).

12 S. Gonscherowski, F. Bieker, *Who You Gonna Call When There's Something Wrong in Your Processing? Risk Assessment and Data Breach Notifications in Practice*, [w:] E. Kosta i in., *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*, 2019, Switzerland: Springer International Publishing AG (IFIP Advances in Information and Communication Technology), s. 35.

13 *Ibidem*, s. 39.

Podsumowując rozważania w tym zakresie, wyraźnego podkreślenia wymaga to, że zanim zaktualizuje się konieczność ewentualnego wszczęcia procedury notyfikacyjnej, administrator musi podjąć działania zmierzające do ustalenia, czy dane zdarzenie nosi znamiona naruszenia bezpieczeństwa danych osobowych. Skuteczność realizacji przez administratora czynności zmierzających do ustalenia potencjalnej konieczności zgłoszenia naruszenia do Prezesa UODO uzależniona jest od uprzedniego wdrożenia procedur i mechanizmów postępowania w przypadku ujawnienia zdarzenia mogącego uzasadniać wątpliwości w zakresie zapewnienia bezpieczeństwa przetwarzanych danych osobowych. Z tego względu rekomendowane jest zwracanie uwagi administratorów na konieczność podnoszenia świadomości prawnej wśród osób przetwarzających dane osobowe w danej organizacji.

4. Ocena incydentu a przesłanki zgłoszenia naruszenia do Prezesa UODO

Mając na uwadze powyższe rozważania, należy odpowiedzieć na pytanie, co w sytuacji, gdy administrator stwierdził, że doszło do incydentu bezpieczeństwa przetwarzania danych osobowych? Jak wskazano, procedura decyzyjna w zakresie ewentualnej notyfikacji stwierdzonego naruszenia jest kilkuetapowa. W przypadku ustalenia przez administratora, że odnotowany incydent nosi znamiona naruszenia generującego konieczność dokonywania zgłoszenia organowi nadzoru, krystalizuje się sposób dalszego postępowania.

Po pierwsze, aby rozważać konieczność zawiadomienia organu nadzorczego o naruszeniu danych, należy takie naruszenie stwierdzić. Zgodnie z opinią Grupy Roboczej Art. 29 moment stwierdzenia incydentu to chwila, w której administrator uzyskał wystarczającą dozę pewności co do tego, że doszło do wystąpienia incydentu bezpieczeństwa, który doprowadził do naruszenia ochrony danych osobowych – czyli stanu naruszenia bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Nie jest zatem tak, że samo powzięcie informacji o potencjalnym incydencie rodzi w sposób automatyczny obowiązek notyfikacyjny. Po powzięciu informacji o potencjalnym naruszeniu ochrony danych osobowych należy bowiem niezwłocznie zbadać okoliczności zgłaszanego zdarzenia. Wydaje się, że optymalnym czasem przeznaczonym na badanie okoliczności zdarzenia powinny być pierwsze 24 godziny liczone od momentu powzięcia informacji o potencjalnym naruszeniu. Oczywiście jest to założenie modelowe, w praktyce uzależnione np. od dnia tygodnia pierwotnego powzięcia informacji o zdarzeniu, jak i od dostępności do infrastruktury kadrowej i zasobowej organizacji, w której do niego doszło. W przypadku zdarzeń wymagających poświęcenia większej ilości czasu na działania wstępne zasadne wydaje się przygotowanie pisemnego uzasadnienia konieczności dłuższego badania.

Analizując drugi etap zmierzający do ustalenia zasadności zgłoszenia faktu naruszenia organowi nadzoru, załóżmy dwa stany faktyczne. W jednym administrator otrzymuje informację od cyberprzestępcy, że ten naruszył poufność przetwarzanych przez niego danych osobowych i wszedł w posiadanie jego listy płac, grożąc upublicznieniem jej, jeżeli nie

zapłaci okupu. W drugim stanie faktycznym ten sam cyberprzestępca dołącza listę płac do ww. wiadomości. W pierwszym stanie faktycznym momentem stwierdzenia naruszenia nie będzie otrzymanie samej wiadomości od cyberprzestępcy, lecz moment jej zweryfikowania – dopiero bowiem po sprawdzeniu systemów IT i ustaleniu, że doszło do incydentu, aktualizuje się obowiązek zawiadomienia organu nadzorczego. W drugim stanie faktycznym momentem tym będzie z kolei moment odczytania wiadomości, jeżeli załączone dane osobowe rzeczywiście zaliczają się do zasobów informacyjnych administratora.

Po drugie, w art. 33 ust. 1 RODO przewidziano wyłączenie obowiązku notyfikowania organowi nadzorczemu naruszeń, gdy jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Stwierdzenia powyższego można przede wszystkim dokonać po analizie konkretnego incydentu – poprzez ustalenie kategorii osób, których dane dotyczą, oraz zakresu ujawnionych danych. Należy podkreślić, że ocena ww. prawdopodobieństwa stanowi jeden z wniosków końcowych przeprowadzonej analizy danego naruszenia – nie można rozważyć prawdopodobieństwa naruszenia praw lub wolności osób fizycznych bez szczegółowej analizy samego naruszenia. Pozytywna odpowiedź na pytanie o to, czy zidentyfikowane naruszenie może powodować ryzyko naruszenia praw i wolności, prowadzi do pozytywnej konkluzji w zakresie konieczności zgłoszenia organowi nadzoru. Co istotne, wobec coraz powszechniejszego niwelowania barier geograficznych możliwe jest przyjęcie, że naruszenie będzie dotyczyło obywateli różnych państw członkowskich UE. W takiej sytuacji, tj. jeśli ma ono znaczny wpływ na osoby fizyczne w więcej niż jednym państwie, należy je zgłosić wiodącemu organowi. W przypadku stwierdzenia braku skutków naruszenia w postaci ryzyka naruszenia praw i wolności obowiązek notyfikacji naruszenia nie powstaje.

Dla zobrazowania analizowanych zagadnień zasadne wydaje się rozważenie kolejnych dwóch stanów faktycznych. W pierwszym podmiot leczniczy (np. przychodnia) stwierdził naruszenie poufności swojej bazy danych, w której przechowywane były imiona i nazwiska pacjentów wraz z wewnętrznym numerem identyfikacyjnym pacjenta. Druga baza danych, zawierająca numery identyfikacyjne pacjenta, dane o historii leczenia, numer PESEL i dane adresowe, pozostała nienaruszona. W drugim stanie faktycznym ta sama placówka medyczna stwierdziła naruszenie poufności bazy danych, w której zbiorczo przechowywano imię i nazwisko pacjenta, numer PESEL, dane adresowe i historię leczenia. W drugim przypadku bez wątpienia istnieje wysokie ryzyko naruszenia praw i wolności osób fizycznych. Nie tylko doszło do ujawnienia danych osobowych szczególnej kategorii, ale także istnieje możliwość wykorzystania tych informacji do nielegalnych działań, takich jak np. wyłudzenie kredytu. W związku z tym w drugim przypadku administrator winien zawiadomić organ nadzorczy o naruszeniu – ryzyko naruszenia praw i wolności osób, których dane dotyczą, jest wysokie. Analizując pierwszy przypadek, trzeba wziąć pod uwagę, że administrator stosował pseudonimizację – przypisał szczegółowe informacje o pacjentach z jednej bazy danych do identyfikatorów pacjentów, które przechowywał w drugiej bazie danych (razem z ich imionami i nazwiskami, które zostały upublicznione).

Oceniając, czy ryzyko naruszenia praw i wolności osób fizycznych jest większe niż małe, trzeba ocenić ewentualne skutki dla pacjentów. Po pierwsze nie zawsze możliwe jest przypisanie konkretnego imienia i nazwiska do danej osoby – informacja, że np.

Adam Nowak jest w bazie danych przychodni, nie musi mieć skutków dla konkretnego Adama Nowaka, który jest jej pacjentem. Ujawnienie wewnętrznego numeru identyfikacyjnego również nie stanowi informacji o Adamie Nowaku, która mogłaby naruszyć jego prawa i wolności. Informacja, że jest on w bazie danych przychodni, również nie. W analizowanym przypadku obowiązek notyfikacyjny nie powstaje głównie dzięki stosowaniu pseudonimizacji przez administratora, gdyż baza danych, w której przechowywane są szczegółowe informacje o pacjentach, pozostała nienaruszona. Oczywiście powyższy przykład jest uproszczony – gdyby ujawniono informacje, że osoba o unikatowym imieniu i nazwisku (które można przypisać wyłącznie do jednej osoby fizycznej) jest pacjentem prywatnej kliniki onkologicznej, to zdarzenie to mogłoby nieść ze sobą ryzyko naruszenia jej praw lub wolności. Z powyższego należy wyciągnąć wniosek, że każde zdarzenie należy szczegółowo przeanalizować, biorąc pod uwagę kontekst danego procesu przetwarzania, którego bezpieczeństwo zostało naruszone.

Po trzecie z art. 33 ust. 1 RODO wynika obowiązek niezwłocznego reagowania na incydenty bezpieczeństwa. Zgodnie z motywem 87 RODO to, czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem w szczególności charakteru i wagi naruszenia ochrony danych osobowych, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą. Powyższe wynika z faktu, że – jak wskazano – zgodnie z motywem 85 RODO przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem licznych negatywnych skutków odczuwalnych przez osobę, której dane dotyczą. Naturalną konsekwencją stwierdzenia naruszenia bezpieczeństwa danych osobowych, przy uwzględnieniu pozostałych pozytywnych przesłanek uzasadniających dokonanie zgłoszenia organowi nadzoru, jest zatem powinność natychmiastowego zgłoszenia organowi nadzorczemu stwierdzonego naruszenia ochrony danych osobowych. Powinno to nastąpić bez zbędnej zwłoki, jeżeli to wykonalne, nie później niż w terminie 72 h po stwierdzeniu naruszenia. Wyjątkiem od tej zasady jest sytuacja, w której administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. Treść motywu 85 jest zgodna z brzmieniem art. 33 ust. 1 RODO. Jednocześnie prawodawca unijny określa, że jeżeli nie można dokonać zgłoszenia w terminie 72 h, zgłoszeniu powinno towarzyszyć wyjaśnienie przyczyn opóźnienia, a informacje mogą być przekazywane stopniowo, bez dalszej zbędnej zwłoki. Za dokonanie zgłoszenia z nieuzasadnioną zwłoką lub po 72 h od stwierdzenia naruszenia RODO nie przewiduje sankcji, jednakże może to mieć wpływ na ewentualną wysokość kary administracyjnej nałożonej na administratora. Na marginesie należy odnotować, że prawodawca unijny nie określił precyzyjnie terminu, w jakim podmioty przetwarzające winny raportować incydenty administratorowi – wskazano jedynie, że ma to nastąpić bez zbędnej zwłoki. Z uwagi na powyższe w sytuacji, gdyby naruszenie ochrony danych osobowych miało miejsce u podwykonawców administratora, np. firmy hostingowej, to termin 72 h na zgłoszenie naruszenia przez administratora biegnie dopiero od momentu, w którym powziął on wiedzę o incydencie, tj. od momentu, w którym został on zawiadomiony przez hostingodawcę o naruszeniu bezpieczeństwa jego zasobów informacyjnych i przeprowadził procedurę zmierzającą do zidentyfikowania naruszenia bezpieczeństwa danych.

Warte podkreślenia jest również to, że niezależnie od tego, czy dany incydent skutkuje zawiadomieniem organu nadzorczego, czy też nie, każde takie zdarzenie kwalifikuje się jako incydent na gruncie RODO i winno zostać udokumentowane, zgodnie z art. 33 ust. 5 RODO. Incydenty te nie tylko powinny być dokumentowane, ale i analizowane oraz oceniane pod kątem możliwych lub niezbędnych ulepszeń systemu bezpieczeństwa[14]. Proces zarządzania incydentami związanymi z bezpieczeństwem informacji służy bowiem do wykrywania, zgłaszania, oceny, reagowania na incydenty związane z bezpieczeństwem informacji, radzenia sobie z nimi i wyciągania z nich wniosków. Wynikiem tego procesu są zidentyfikowane incydenty, które są wykorzystywane w różnych procesach o charakterze naprawczym, w tym w procesie zarządzania zmianami w bezpieczeństwie informacji i procesie zapewniającym niezbędną świadomość[15]. Skrupulatność administratora w tego rodzaju sytuacjach postrzegana jest korzystnie z perspektywy ustalenia stopnia jego świadomości w odniesieniu do zdefiniowanych procesów przetwarzania, a także wdrożenia mechanizmów organizacyjno-technicznych zapewniających realizowanie odpowiednich procedur zmierzających do zapewnienia wysokiego poziomu zapewnienia bezpieczeństwa przetwarzanym danym osobowym.

5. Zgłoszenie naruszenia do PUODO – uwagi praktyczne

Zgłoszenie naruszenia do organu nadzorczego należy przekazać elektronicznie lub listownie, zgodnie z wymaganiami art. 33 ust. 3 RODO. Zgodnie z tym przepisem zgłoszenie powinno co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków;

oraz zawierać wyjaśnienie przyczyn opóźnienia art. 33 ust. 1 zd. 2 RODO, jeżeli przekazano je po upływie 72 h od stwierdzenia naruszenia ochrony danych osobowych.

Wskazany wyżej przepis zawiera minimalny zakres informacji dotyczących stwierdzonego naruszenia. Nic nie stoi na przeszkodzie, aby taki zakres poszerzyć – najczęściej

14 G. Disterer, *ISO/IEC 27000, 27001 and 27002 for Information Security Management*, „Journal of Information Security" 2013, nr 4, s. 98.

15 K. Haufe i in., *A process framework for information security management*, „International Journal of Information Systems and Project Management" 2016, t. 4, nr 4, s. 33.

będzie to miało miejsce w sytuacji, gdy administrator będzie chciał udokumentować swoje starania w kontekście minimalizacji skutków incydentu lub udokumentować sposób przeprowadzenia analizy możliwych konsekwencji naruszenia. Nie jest bowiem tak, że każde zgłoszenie doprowadzi do wszczęcia postępowania administracyjnego przez organ nadzorczy – szerokie opisanie stanu faktycznego może czasem uchronić administratora od wyjaśniania szczegółów zdarzenia w toku takiego postępowania. Zakres zgłoszenia uzależniony będzie od efektywności zastosowania uprzednio wdrożonych procedur postępowania w przypadku stwierdzenia naruszenia. Jeżeli bowiem administrator po uzyskaniu informacji o zdarzeniu mogącym nosić znamiona naruszenia bezpieczeństwa danych osobowych żądał wyjaśnień od członków personelu bądź przeprowadził konsultacje (w tym zewnętrznych podmiotów), informacje o tych działaniach powinny znajdować się w zgłoszeniu, w części dotyczącej zastosowanych środków. Nadto administrator, opisując zdarzenie oraz zastosowane narzędzia organizacyjno-techniczne, powinien w zgłoszeniu także opisać sposób postępowania.

Istotne jest bowiem to, aby w kontakcie z organem nadzoru przedstawić argumentację uwiarygadniającą to, że do naruszenia doszło w sposób przypadkowy i nie nosiło ono znamion działania zamierzonego i świadomego, przy założeniu, że w rzeczywistości taka sytuacja miała miejsce. Z perspektywy postępowania przed Prezesem UODO istotne jest bowiem uwypuklenie stopnia świadomości i umiejętności identyfikowania zagrożeń i niebezpieczeństw przez pracowników organizacji. Z tego względu istotny praktyczny wymiar będzie miało opisanie w zgłoszeniu sposobu postępowania personelu niezwłocznie po zidentyfikowaniu incydentu mogącego stanowić naruszenie bezpieczeństwa danych osobowych (np. czy choćby wstępnie udokumentowane zostało zaistniałe zdarzenie, jakie czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia zostały podjęte, czy zabezpieczone zostało miejsce zdarzenia, a także jakie działania zostały podjęte stosownie do objawów i komunikatów towarzyszących naruszeniu).

Należy zauważyć, że jeżeli nie jest możliwe udzielenie wszystkich informacji określonych w art. 33 ust. 3 RODO w przesłanym do organu nadzorczego zgłoszeniu, istnieje możliwość przekazywania ich sukcesywnie, lecz bez zbędnej zwłoki, na podstawie art. 33 ust. 4 RODO. Prawodawca unijny nie definiuje terminu „bez zbędnej zwłoki", co prowokuje do przyjęcia, że w przypadku naruszenia bezpieczeństwa danych osobowych administrator musi niezwłocznie, czyli możliwie jak najszybciej, powiadomić właściwy organ nadzoru. W praktyce oznacza to, że administrator nie może zwlekać z przekazaniem informacji o naruszeniu danych, ale musi wręcz działać bezzwłocznie po stwierdzeniu takiego naruszenia. Uprawnienie, o którym mowa w art. 33 ust. 3 RODO, w zakresie sukcesywnego przekazywania informacji organowi nadzoru sprzyja kompleksowemu wyjaśnieniu okoliczności i faktów mających znaczenie dla oceny sytuacji i ewentualnej winy administratora w naruszeniu bezpieczeństwa danych osobowych. Wydaje się, że formularz zgłoszenia naruszenia ochrony danych osobowych dostępny na stronie Urzędu Ochrony Danych Osobowych jest skonstruowany w intuicyjny sposób, dzięki czemu podmiot zgłaszający naruszenie powinien przedstawić kompleksowe informacje dotyczące opisywanego zdarzenia. Zasadne jest jednak zastosowanie metody optymalnej szczegółowości opisu, dzięki czemu możliwe będzie dokładne przybliżenie nie tylko

sytuacji stanowiącej przedmiot zgłoszenia, ale i stosowanych procedur i zabezpieczeń. Z tego też względu w części przeznaczonej na opisanie zdarzenia praktyką zasługującą na aprobatę jest uwzględnienie wyników postępowania wyjaśniającego i zabezpieczającego, a także przedstawienie konkluzji płynących z raportu naruszenia.

Mimo że podstawowym skutkiem stwierdzenia naruszenia jest poinformowanie o tym fakcie organu nadzoru. Nie należy zapominać jednak o konieczności realizacji obowiązku informacyjnego względem osób, których dane zostały naruszone. Procedując zgłoszenie naruszenia ochrony danych osobowych, administrator powinien również pamiętać o obowiązkach wynikających z treści art. 34 ust. 1 RODO, zgodnie z którym, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Z regulacji należy wywnioskować, że w sytuacji, gdy ocena danego incydentu, dokonana przez administratora, doprowadziła do wniosku, że ryzyko naruszenia praw lub wolności osób fizycznych jest wysokie, to należy takie osoby o tym fakcie poinformować. Jest to uzasadniona praktyka z perspektywy możliwości wdrożenia odpowiednich działań zapobiegawczych, co potwierdza wprost brzmienie motywu 86 RODO. Prawodawca unijny także i w tym przypadku nie określił przy tym terminu, w którym zawiadomienie takie powinno zostać dokonane. W konsekwencji należy przyjąć, że zgodnie z omawianym przepisem należy to uczynić niezwłocznie, co leży w najlepszym interesie administratora, ponieważ potencjalnie może ograniczyć ilość i wysokość roszczeń cywilnoprawnych osób, których dane dotyczą. Przykładowo informując osobę, której dane dotyczą, o fakcie, że ujawnione zostały jej dane osobowe, które mogą potencjalnie pozwolić na wyłudzenie kredytu lub skutkować kradzieżą tożsamości w innych aspektach (np. dane tożsamości, numer i seria dowodu osobistego oraz numer PESEL), administrator umożliwia takiej osobie skorzystanie z usług biura informacji kredytowej, tak aby mogła ona otrzymać alert ostrzegawczy informujący o procedurach kredytowych podejmowanych na jej rzecz przez banki.

Reasumując, sposób postępowania w przypadku naruszeń ochrony danych osobowych jawi się jako skomplikowany i sformalizowany. Administratorzy, zgodnie ze stanowiskiem Grupy Roboczej Art. 29, powinni ustanowić wewnętrzne procedury umożliwiające wykrycie i zaradzenie naruszeniom, na przykład poprzez stosowanie oprogramowania do analizy przepływu danych i logów oprogramowania. Ponadto personel powinien być odpowiednio przeszkolony, aby mógł zidentyfikować potencjalne naruszenia ochrony danych osobowych. W przypadku wykrycia naruszenia w ramach prowadzonego postępowania wyjaśniającego i zabezpieczającego administrator powinien działać niezwłocznie, co oznacza, że powinien dysponować procedurą reagowania na incydenty. Powinien wiedzieć, kto i w jaki sposób będzie oceniał prawdopodobieństwo naruszenia praw lub wolności osób fizycznych, których dane dotyczą. Trudno bowiem sobie wyobrazić, aby w ciągu 72 h od stwierdzenia incydentu administrator miał czas na poszukiwanie specjalisty ds. ochrony danych osobowych oraz ds. bezpieczeństwa IT, który pomoże mu przejść przez procedurę w wymaganym czasie, dokonać niezbędnej analizy i zgłoszenia do organu nadzorczego połączonego z zawiadomieniem z art. 34 ust. 1 RODO.

6. Zasady nakładania administracyjnych kar pieniężnych na administratora danych osobowych

Niestety w dalszym ciągu w praktyce dostrzegalna jest akceptacja poglądu, zgodnie z którym każdorazowe obowiązkowe zgłoszenie naruszenia danych wiąże się automatycznie z nałożeniem kary pieniężnej. Teza ta jest zbyt daleko idąca. Oczywiście każdy incydent podlegający zgłoszeniu organowi nadzorczemu wiążę się z ryzykiem sankcji administracyjnych, w tym kar finansowych, do których nakładania RODO uprawnia organ nadzorczy[16]. Nieprawidłowe jest jednak twierdzenie, jakoby w sposób automatyczny naruszenie implikowało skutek w postaci nałożenia przez organ nadzorczy kary pieniężnej.

Nie ulega wątpliwości, że dokonanie zgłoszenia organowi nadzoru w sposób naturalny skutkować może koniecznością przeprowadzenia kontroli prawidłowości realizacji procesów przetwarzania. Każdorazowo w sytuacji ujawnienia działania niezgodnego z przepisami unijnymi i krajowymi w zakresie ochrony danych osobowych aktualizuje się konieczność dokonania oceny źródeł i ustalenia ich charakteru (w tym ustalenia poziomu umyślności dla danego działania lub zaniechania), a także przyczyn i powodów naruszenia bezpieczeństwa. Pod uwagę należy wziąć także historię ewentualnych naruszeń z przeszłości. Zgodnie z art. 60 UODO postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych jest prowadzone przez Prezesa UODO. Być może źródłem praktyki polegającej na utożsamianiu wszczęcia postępowania przez organ nadzoru z oczekiwaniem na wymierzenie kary pieniężnej jest analiza brzmienia polskiej ustawy o ochronie danych osobowych, w której ustawodawca odnosi się do zasad nakładania administracyjnych kar pieniężnych, pomijając przy tym dopuszczalność podejmowania innych rozstrzygnięć, także zmierzających do mobilizacji w zakresie przetwarzania danych osobowych zgodnie z przepisami prawa. Pamiętać należy jednak o tym, że ogólne reguły dotyczące uprawnień krajowych organów nadzoru do podejmowania działań zawarte są w unijnym rozporządzeniu.

Uszczegółowieniem przyjętych regulacji unijnych są postanowienia krajowej ustawy o ochronie danych osobowych, w której w art. 60–74 UODO ustawodawca określił zasady prowadzenia przez Prezesa UODO postępowania w sprawie naruszenia przepisów o ochronie danych osobowych. Jednocześnie ustawodawca w art. 78–91 UODO sformułował zasady prowadzenia postępowania kontrolnego, które jest głównym przedmiotem zainteresowania z uwagi na cel i zakres niniejszego opracowania, bowiem jego wynik przesądza o (nie)zasadności wszczęcia i prowadzenia postępowania administracyjnego mogącego skutkować nałożeniem administracyjnej kary pieniężnej. Niestety krajowy ustawodawca, systematyzując regulacje prawne odnoszące się do nadzorowania prawidłowości przestrzegania norm prawnych dotyczących ochrony danych osobowych, dokonał swoistego rozdrobnienia regulacji, co przy konieczności łącznego analizowania postanowień RODO nie sprzyja ich czytelności. Nadto porządek, w jakim uregulowane

16 A. Kamiński, K. Dąbek, *Nowe zagrożenia dla działalności przedsiębiorstw w świetle Rozporządzenia Parlamentu Europejskiego o ochronie danych osobowych (RODO)*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, Uniwersytet Ekonomiczny we Wrocławiu" 2017, nr 487, DOI: 10.15611/pn.2017.487.12, s. 140.

zostały kwestie naruszenia danych osobowych, a także prowadzenia postępowania kontrolnego, może skutkować mylnym przyjęciem błędnej kolejności w zakresie czynności podejmowanych przez organ nadzoru. Nie ulega jednak wątpliwości, że wskazane przepisy stanowią *lex specialis* względem rozwiązań przyjętych w unijnym rozporządzeniu, choć – jak wskazano – nie przesądza to o kompleksowym uregulowaniu zasad prowadzenia postępowania wskutek zawiadomienia organu o naruszeniu ochrony danych osobowych. Uzasadnieniem dla tego stanowiska jest zakres przedmiotowy regulacji wprost odnoszących się do postępowania w sprawie naruszenia przepisów o ochronie danych osobowych, postępowania kontrolnego, a także brzmienie art. 7 UODO, zgodnie z którym w sprawach nieuregulowanych w ustawie do postępowań administracyjnych przed Prezesem Urzędu stosuje się przepisy Kodeksu postępowania administracyjnego, zaś postanowienia wydane w postępowaniach są zaskarżalne skargą do sądu administracyjnego, przy jednoczesnym uwzględnieniu licznych wątpliwości dotyczących dwuinstancyjnego charakteru postępowania przed Prezesem UODO.

Pierwszym z etapów postępowania skutkującego potencjalnym nałożeniem administracyjnej kary pieniężnej jest postępowanie kontrolne, prowadzone w oparciu o art. 78 UODO, przy uwzględnieniu zatwierdzonego przez Prezesa Urzędu planu kontroli lub na podstawie uzyskanych przez Prezesa UODO informacji lub w ramach monitorowania przestrzegania stosowania rozporządzenia[17]. Ustawodawca w sposób dość szczegółowy określa zasady prowadzenia postępowania, z uwzględnieniem zasad dotyczących podmiotu kontrolującego (art. 79–81 UODO), udziału osób trzecich (art. 82 UODO), a także przebiegu kontroli (art. 83 UODO). Na uwypuklenie zasługują jednak postanowienia dotyczące przebiegu i uprawnień podmiotów kontrolujących, z których wprost wynika, że kontrolujący mają szerokie uprawnienia w zakresie dostępu do dokumentów i informacji mających bezpośredni związek z zakresem przedmiotowym kontroli, a także do przeprowadzania oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych, jak również do żądania złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwania w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego, a także zlecania sporządzenia ekspertyz i opinii. Informacje zgromadzone w postępowaniu kontrolnym przesądzają o zasadności lub niezasadności wszczęcia postępowania, o którym mowa w art. 60 UODO. Odmówienie wszczęcia postępowania wydaje się uzasadnione w przypadku stwierdzenia braku przesłanek do nadania sprawie biegu. W takiej sytuacji, działając na podstawie art. 61a § 1 k.p.a. w zw. z art. 7 ust. 1 UODO, Prezes Urzędu powinien odmówić wszczęcia postępowania administracyjnego. Jeśli zaś Prezes UODO uzna, że mogło dojść do naruszenia przepisów o ochronie danych osobowych, obowiązany jest do niezwłocznego jego wszczęcia (art. 90 UODO). Wówczas aktualizują się postanowienia zawarte w art. 60–74 UODO, odnoszące się do postępowania w przedmiocie stwierdzonego naruszenia, które prowadzone jest na podstawie przepisów Kodeksu postępowania administracyjnego, z uwzględnieniem uprawnień, o których mowa chociażby w art. 68 UODO odnoszącym się do konieczności uzupełnienia dowodów. Istotne jest

17 Tak też: P. Litwiński, [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. P. Litwiński, Warszawa 2018, Legalis.

bowiem to, aby efektem prowadzonego postępowania było jednoznaczne stwierdzenie zasadności nałożenia administracyjnej kary pieniężnej wobec braku zasadności wymierzenia pozostałych kar czy mechanizmów przewidzianych w art. 58 RODO.

Zgodnie z art. 83 ust. 2 RODO administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego indywidualnego przypadku, oprócz lub zamiast środków naprawczych, o których mowa w art. 58 ust. 2 RODO, z wyjątkiem zastosowania kary pieniężnej. Decydując, czy nałożyć administracyjną karę pieniężną oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na rodzaj i charakter naruszenia, a także na podejmowane przez podmiot naruszający działania naprawcze, informacyjne, a przede wszystkim na sposób komunikacji i współpracy z organem nadzoru. Jeżeli bowiem podmiot, przeciwko któremu wszczęto postępowanie, kwestionuje nie tylko zasadność, ale i rozmiar naruszenia, bezkrytycznie przyjmując dotychczasowe działania za prawidłowe, naraża się w większym stopniu na próbę zdyscyplinowania go przez organ nadzoru w postaci nałożenia na niego administracyjnej kary pieniężnej. Analizując decyzje Prezesa UODO, możliwe jest wyprowadzenie wniosku, z którego w uproszczeniu wynika, że gdyby administrator lub procesor uwzględnili zalecenia organu nadzoru, nie byłoby konieczne nakładanie administracyjnej kary pieniężnej.

W art. 58 RODO prawodawca unijny sformułował ogólne reguły, na mocy których każdemu organowi nadzorczemu przysługują określone uprawnienia, wśród których należy wyróżnić uprawnienia w zakresie prowadzonych postępowań, naprawcze, a także w zakresie wydawania zezwoleń i uprawnienia doradcze. Redakcja wskazanego przepisu przesądza o tym, że zakres uprawnień przyznany organom nadzoru ma charakter zamknięty. Jednocześnie prawodawca unijny w ust. 6 tego przepisu dopuszcza możliwość indywidualnego rozszerzenia wskazanego katalogu przez państwa członkowskie UE. Z perspektywy przedmiotu niniejszego opracowania najistotniejsze znaczenie mają kompetencje organu nadzoru w zakresie prowadzonych postępowań oraz uprawnienia naprawcze. Kumulatywna analiza art. 58 ust. 1 i ust. 2 RODO prowadzi do wniosku, że samo stwierdzenie naruszenia przez administratora danych nie skutkuje w sposób automatyczny koniecznością nałożenia administracyjnej kary pieniężnej. Dostrzegalne jest bowiem to, że w pierwszym etapie organ nadzoru powinien przeprowadzić czynności wyjaśniające, w trakcie których jest on uprawniony m.in. do nakazania administratorowi i procesorowi, a w stosownym przypadku ich przedstawicielom, dostarczenia wszelkich informacji potrzebnych organowi nadzorczemu do realizacji swoich zadań, jak również prowadzenia postępowań w formie audytów ochrony danych. Warte podkreślenia jest to, że zastosowanie jednego lub kilku z uprawnień naprawczych określonych w art. 58 ust. 2 RODO nie eliminuje wprost możliwości wymierzenia kary pieniężnej, ale sposób współpracy administratora z organem może przesądzać o jej znacznym obniżeniu bądź przyczynić się do wyłączenia konieczności jej zastosowania. Prawodawca unijny legitymuje bowiem organy nadzoru do tego, aby kara pieniężna była wymierzana obok pozostałych kar albo zamiast nich – samodzielnie. Organ może udzielać upomnień podmiotowi przetwarzającemu w przypadku naruszenia przepisów RODO, jak również nakazać, aby administrator dostosował operacje przetwarzania do RODO, co w stosownych przypadkach może wiązać się z wyznaczeniem konkretnego sposobu działania i terminu realizacji. Organ może także nakazać czasowe lub całkowite ograniczenie przetwarzania, w tym

zakazu przetwarzania. W relacjach z osobami, których dane są przetwarzane, organ uprawniony jest do nakazania realizacji praw osób, których dane dotyczą, a także nakazania zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych czy sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania. Wskazany wyżej zakres przedmiotowy kompetencji organu w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych nie uzasadnia równoważenia nakładania administracyjnej kary pieniężnej każdorazowo w przypadku stwierdzenia w wyniku postępowania kontrolnego naruszenia bezpieczeństwa danych osobowych. Administrator i podmiot przetwarzający mogą zostać zwolnieni z odpowiedzialności tylko wtedy, gdy udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody. Tym samym RODO odchodzi od upowszechnionej w prawie cywilnym zasady, iż ciężar dowodu spoczywa na osobie występującej z roszczeniem.

Zgodnie z wytycznymi administracyjne kary pieniężne powinny w stosowny sposób odpowiadać charakterowi, wadze i konsekwencjom naruszenia, a organy nadzorcze muszą dokonywać oceny okoliczności faktycznych danej sprawy w sposób spójny i obiektywnie uzasadniony. Ocena tego, co jest skuteczne, proporcjonalne i odstraszające, w każdym przypadku będzie musiała również odzwierciedlać cel wybranego środka naprawczego, którym jest przywrócenie zgodności z przepisami lub ukaranie za bezprawne zachowanie (lub oba te cele)[18]. Co istotne, w Polsce środki z administracyjnej kary pieniężnej stanowią dochód budżetu państwa. Nie zasilają one samego Urzędu Ochrony Danych Osobowych. Polski ustawodawca ostatecznie zdecydował się więc wpływy z tych kar uczynić w całości dochodem budżetu państwa, pomimo że na etapie projektowania ustawy krajowej rozważane było, aby 1% środków pochodzących z tych kar był przeznaczany na działalność nowego funduszu celowego (Funduszu Ochrony Danych Osobowych). Środki te miały być wówczas przeznaczane na finansowanie działalności polegającej na upowszechnianiu wiedzy z zakresu ochrony danych osobowych[19]. Maksymalna wysokość kar ustalona w RODO osiąga granice maksymalne nieporównywalne do żadnych innych kar administracyjnych nakładanych dotychczas w Polsce. Wydaje się, że dotyczy to także pozostałych krajów UE[20].

Konkludując poczynione rozważania, należy podkreślić, że ustawodawca wyeliminował możliwość złożenia wniosku o ponowne rozpoznanie sprawy[21], przesądzając o jednoinstancyjnym charakterze postępowania przed organem w art. 7 ust. 2 UODO. W konsekwencji na postanowienia wydawane przez organ służy skarga do sądu administracyjnego, jednak strona pozbawiona jest możliwości odwołać się od decyzji, jak również nie ma możliwości wniesienia zażalenia na postanowienie[22]. Mimo dostrzegalnego

18 Grupa Robocza Art. 29, *Wytyczne dotyczące…*, s. 6.

19 J. Łuczak, [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 1059; D. Antonów, *Administracyjne kary pieniężne za naruszenia ochrony danych osobowych*, „Prawo Budżetowe Państwa i Samorządu" 2020, nr 8(3), s. 33.

20 A. Klich, *Personal data protection in the energy services market-selected issues*, „Journal of Modern Science" 2023, vol. 51, nr 2, s. 660.

21 Tak też: P. Fajgielski, *Komentarz do ustawy o ochronie danych osobowych*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, red. P. Litwiński, Warszawa 2018, LEX.

22 Tak też: L. Kępa, *Ochrona danych osobowych. Praktyczny przewodnik dla przedsiębiorców*, Warszawa 2018, s. 487.

w doktrynie stanowiska odmiennego[23], zgodnie z którym możliwe jest złożenie wniosku o ponowne rozpoznanie sprawy, zasadne wydaje się zaaprobowanie poglądu, zgodnie z którym nie ma możliwości wniesienia odwołania od decyzji organu. Kluczowe w tym zakresie jest to, że ustawodawca nie przewidział organu wyższego stopnia w stosunku do Prezesa UODO. W ustawie krajowej nie został także wskazany jakikolwiek organ mogący orzekać w przedmiocie odwołania od decyzji Prezesa Urzędu[24]. Kumulatywna analiza wskazanych przesłanek prowadzi jednoznacznie do stanowiska, że polski ustawodawca skonstruował postępowanie jednoinstancyjne, które w przypadku niezadowolenia strony może zostać jedynie przeniesione na drogę rozstrzygania przez sąd administracyjny, wskutek wniesienia skargi do wojewódzkiego sądu administracyjnego.

7. Podsumowanie

Analizując brzmienie przepisów unijnego rozporządzenia, a także regulacji krajowych, należy przede wszystkim zwrócić uwagę na to, iż podmioty przetwarzające dane osobowe, u których doszło do stwierdzenia naruszenia, mogą zderzać się nie tylko z problemem w zakresie umiejętności interpretowania tych przepisów, ale i w rozeznaniu co do procedury kontrolnej i zmierzającej do wydania decyzji przez organ nadzoru. Aktualnie obowiązujące regulacje stawiają bowiem przed podmiotami przetwarzającymi dane osobowe coraz większe wyzwania, wymagając jednocześnie od nich szybkiej reakcji na ewentualne naruszenia bezpieczeństwa danych.

Z tego też względu w pierwszej kolejności należy w sposób umiejętny dokonywać oceny i analizy w zakresie zasadności realizacji obowiązku notyfikacji naruszenia organowi nadzoru. W tym zakresie na podmiocie przetwarzającym dane osobowe spoczywa obowiązek weryfikacji, czy ma on do czynienia z naruszeniem podlegającym obowiązkowi notyfikacji organowi nadzorczemu. W tym celu konieczne jest jednak dokonanie weryfikacji, czy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osoby, której dane dotyczą. Oznacza to, że na administratorze lub procesorze, u którego zdefiniowano incydent bezpieczeństwa danych, spoczywa obowiązek ustalenia, czy doszło do sytuacji, które mogą nieść ze sobą istotne negatywne skutki dla osoby, której dane zostały naruszone (np. popełnienie przestępstwa na jej szkodę, kradzież tożsamości, naruszenie dobrego imienia itd.). W takiej sytuacji zawiadomienie jest konieczne przede wszystkim z uwagi na niezbędność zabezpieczenia interesów osoby, której dane zostały przetworzone w sposób naruszający zasady bezpieczeństwa. Na tym etapie istotne jest to, aby podmiot przetwarzający dane podejmował na bieżąco w organizacji działania zmierzające do podnoszenia świadomości wśród osób upoważnionych do przetwarzania danych osobowych, aby w razie zaobserwowania

23 B. Marcinkowski, [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. B. Marcinkowski, Warszawa 2018, LEX.

24 T. Kuczyński, *Postępowanie przed Prezesem Urzędu Ochrony Danych Osobowych w świetle zasady dwuinstancyjności postępowania administracyjnego*, „Studia Iuridica Toruniensia" 2021, t. XXIX, s. 151.

incydentu realizowały obowiązek notyfikacyjny względem bezpośredniego przełożonego w celu przeprowadzenia wewnętrznego posiedzenia wyjaśniającego. Podmioty przetwarzające dane muszą bowiem być gotowe nie tylko na zapobieganie incydentom, ale również na skuteczną reakcję w przypadku ich wystąpienia. Z tego względu znacząca rola przypisana jest – jak wskazano – działaniom edukacyjnym i świadomościowym pracowników, którzy są kluczowymi uczestnikami w procesie bezpieczeństwa danych. Jest to istotne, bowiem jak wskazano w postawionej hipotezie badawczej – utożsamianie stwierdzonego naruszenia z automatycznym nałożeniem kary pieniężnej przez organ nadzoru jest praktyką błędną. W przeciwnym razie zniweczona byłaby zasadność prowadzenia postępowania kontrolnego, w trakcie którego podmiot, u którego stwierdzono naruszenie, ma możliwość wykazania aktywności zmierzającej nie tylko do usunięcia powstałego naruszenia, ale i zapobiegania podobnym naruszeniom w przyszłości.

Mając na uwadze powyższe, warte podkreślenia jest to, że już na etapie prowadzenia kontroli istotne jest to, aby podmiot przetwarzający dane osobowe prezentował postawę świadczącą o skutecznym zarządzaniu bezpieczeństwem danych osobowych w kontekście nowych regulacji i norm prawnych. Aktualnie na podmiotach przetwarzających dane osobowe spoczywa konieczność holistycznego podejścia do ochrony danych, biorąc pod uwagę zarówno aspekty techniczne, jak i organizacyjne. W praktyce, aby uniknąć sankcji ze strony organu nadzoru, podmioty przetwarzające dane powinny skoncentrować się nie tylko na spełnianiu podstawowych wymagań prawnie określonych, ale również na wdrażaniu proaktywnych działań z zakresu cyberbezpieczeństwa. Wprowadzenie skutecznych procedur monitoringu, szybkiego reagowania na incydenty oraz edukacji pracowników w zakresie bezpiecznego przetwarzania danych staje się współcześnie kluczowe.

Podsumowując poczynione rozważania, należy podkreślić, że wdrożenie skutecznej strategii postępowania w przypadku stwierdzenia naruszenia, a także przyjęcie modelu współpracy z organem nadzoru może zapobiec nałożeniu administracyjnej kary pieniężnej. Ci administratorzy i procesorzy, którzy dostrzegają wadliwości zastosowanych zabezpieczeń technicznych i organizacyjnych, uwzględniając wnioski i rekomendacje organu nadzoru, mogą uniknąć lub zminimalizować wymiar nałożonej na nich kary pieniężnej.

Bibliografia

Antonów D., *Administracyjne kary pieniężne za naruszenia ochrony danych osobowych*, „Prawo Budżetowe Państwa i Samorządu" 2020, nr 8 (3).

Barta P., Kawecki M., Litwiński P., *Komentarz do art. 32 RODO*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021, Legalis.

Bobkowski K., *Zarządzanie bezpieczeństwem informacji w ujęciu wybranych aktów normatywnych w zakresie Systemu Zarządzania Bezpieczeństwem Informacji*, „Zarządzanie i Finanse – Journal of Management an Finance" 2018, vol. 16, no. 3.

Disterer G., *ISO/IEC 27000, 27001 and 27002 for Information Security Management*, „Journal of Information Security" 2013, nr 4.

Fajgielski P., *Komentarz do ustawy o ochronie danych osobowych*, [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, red. P. Litwiński, Warszawa 2018, LEX.

Gonscherowski S., Bieker F., *Who You Gonna Call When There's Something Wrong in Your Processing? Risk Assessment and Data Breach Notifications in Practice*, [w:] E. Kosta i in., *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*, 2019, Switzerland: Springer International Publishing AG (IFIP Advances in Information and Communication Technology).

Grupa Robocza Art. 29, *Wytyczne dotyczące powiadamiania o naruszeniu ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 z dnia 3 października 2017 r.*, WP250rev.01. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

Haufe K. i in., *A process framework for information security management*, „International Journal of Information Systems and Project Management" 2016, t. 4, nr 4.

Hoofnagle Ch.J., van der Sloot B., Zuiderveen Borgesius F., *The European Union general data protection regulation: what it is and what it means*, „Information & Communications Technology Law" 2019, vol. 28, no. 1, DOI: 10.1080/13600834.2019.1573501.

Kamiński A., Dąbek K., *Nowe zagrożenia dla działalności przedsiębiorstw w świetle Rozporządzenia Parlamentu Europejskiego o ochronie danych osobowych (RODO)*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, Uniwersytet Ekonomiczny we Wrocławiu" 2017, nr 487, DOI:10.15611/pn.2017.487.12, s. 140.

Kępa L., *Ochrona danych osobowych. Praktyczny przewodnik dla przedsiębiorców*, Warszawa 2018.

Klich A., *Personal data protection in the energy services market-selected issues*, „Journal of Modern Science" 2023, vol. 51, nr 2.

Koops B.-J., *The trouble with European data protection law*, „International Data Privacy Law" 2014, vol. 4, no. 4.

Kuczyński T., *Postępowanie przed Prezesem Urzędu Ochrony Danych Osobowych w świetle zasady dwuinstancyjności postępowania administracyjnego*, „Studia Iuridica Toruniensia" 2021, t. XXIX.

Litwiński P., [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. P. Litwiński, Warszawa 2018.

Łuczak J., [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.
Marcinkowski B., [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. B. Marcinkowski, Warszawa 2018.
Pelnekar C., *Planning for and Implementing ISO 27001*, „ISACA Journal" 2011, t. 4, nr 4.