STUDIA I ARTYKUŁY

Jacek Błachut, Sławomir Dudzik

Naruszenie ochrony danych osobowych. Problematyka prawna

1. Wprowadzenie

Dane osobowe osób fizycznych podlegają w porządku prawnym Unii Europejskiej[1] ochronie już w prawie pierwotnym. Ochronę tę statuuje zarówno art. 8 ust. 1 Karty Praw Podstawowych Unii Europejskiej[2], jak i art. 16 Traktatu o Funkcjonowaniu Unii Europejskiej[3]. Przypomina o tym pierwszy motyw rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dn. 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)[4], a więc aktu prawnego, który w kompleksowy, szczegółowy i bezpośredni sposób uregulował prawo ochrony danych osobowych obowiązujące w państwach członkowskich Unii Europejskiej[5]. W polskim

1 Dalej UE lub Unia.

2 Wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 389 (dalej: KPP).

3 Wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 47 (dalej: TFUE). W polskim porządku konstytucyjnym ogólną podstawę ochrony danych osobowych statuuje art. 51 Konstytucji Rzeczypospolitej Polskiej z dn. 2 kwietnia 1997 r., Dz.U. 1997, nr 78, poz. 483 ze zm.

4 Dz.U.UE.L.2016.119.1 (dalej: RODO).

5 Ochrony danych osobowych w związku z działalnością instytucji, organów i jednostek organizacyjnych UE dotyczy rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725

porządku konstytucyjnym ogólną podstawę ochrony danych osobowych statuuje art. 51 Konstytucji. Ochrona ta postrzegana jest przy tym jako jeden z przejawów prawa do ochrony prywatności (art. 47 Konstytucji)[6].

Wspomniana ochrona osób fizycznych realizowana jest w przepisach RODO na różnych płaszczyznach. Z jednej strony następuje to poprzez określenie dopuszczalnych przez prawo podstaw przetwarzania danych osobowych oraz zakresu ich przetwarzania, nałożenie obowiązków informacyjnych względem osób, których dane dotyczą oraz przyznanie tym osobom szczegółowych uprawnień związanych z przetwarzaniem. Ma to prowadzić do przetwarzania danych osobowych z zachowaniem wymogów proporcjonalności i adekwatności, przy zapewnieniu zainteresowanym osobom odpowiedniego poziomu wiedzy na temat przetwarzania ich danych osobowych oraz odpowiednich instrumentów (praw) do wpływania na tego rodzaju procesy. Z drugiej strony ochronę osób fizycznych w związku z przetwarzaniem ich danych zapewnić mają obowiązki związane z fizycznym zabezpieczeniem tych danych poprzez stosowanie odpowiednich technicznych i organizacyjnych środków bezpieczeństwa, a także poprzez określone w RODO obowiązki dokumentacyjne i administracyjne, wymagające między innymi prowadzenia odpowiednich rejestrów oraz kontaktów z organem nadzoru lub osobami, których dane dotyczą. Podstawowym celem wprowadzenia tych obowiązków jest dążenie do wykluczenia lub przynajmniej zminimalizowania ryzyka wystąpienia sytuacji, w której zagrożone byłoby bezpieczeństwo przetwarzanych danych osobowych. Do kwestii tej prawodawca unijny przywiązuje

z dn. 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE, Dz.Urz.UE z 2018 r., L 295/39. Poza zakresem niniejszego artykułu pozostaje problematyka ochrony danych osobowych w szeroko rozumianych sprawach karnych. Kwestie te w prawie UE reguluje dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dn. 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz.Urz.UE L 119 z 2016 r., s. 89, a w prawie polskim – ustawa z dn. 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, Dz.U. 2019, poz. 125.

6 Zob szerzej np.: P. Fajgielski, *Prawo*…, s. 32–34; M. Florczak-Wątor, w: *Konstytucja*…, art. 51; K. Łakomiec, *Konstytucyjna*…

szczególną wagę, regulując w sposób szczegółowy problematykę naruszenia ochrony danych osobowych i wskazując już w motywie 85 RODO, że:

> 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.

Celem niniejszego artykułu jest analiza kwestii prawnych związanych z naruszeniem ochrony danych osobowych, w tym odpowiedź na pytanie, czy przepisy prawa (przede wszystkim UE) właściwie chronią prawa jednostki w kontekście takiego naruszenia oraz czy przewidziane w przepisach sankcje i zasady odpowiedzialności z tego tytułu są adekwatne do zaistniałych zagrożeń, a także, czy respektują wymogi praworządności.

2. Naruszenie ochrony danych osobowych

Pojęcie „naruszenie ochrony danych osobowych" (ang. *personal data breach*) posiada w RODO swą definicję legalną. Zgodnie z brzemieniem art. 4 pkt 12 RODO pod pojęciem tym rozumieć należy naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesłanych, przechowywanych lub w inny sposób przetwarzanych[7].

Analizując przywołaną definicję, należy w pierwszej kolejności zwrócić uwagę, że o naruszeniu ochrony danych osobowych można mówić wówczas, gdy spełnione są kumulatywnie dwa zawarte w tej definicji warunki. Po pierwsze, dojść musi do naruszenia bezpieczeństwa. Po drugie, musi

7 Szerzej: Grupa Robocza Art. 29, Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679, przyjęte w dniu 3.10.2017 r., ostatnio zmienione i przyjęte w dniu 6.02.2018 r., WP250rev.01, < https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 >, dostęp: 14 lipca 2021 r. (dalej: Wytyczne); T. Soczyński, *Zgłaszanie*…, s. 40 i n.

wystąpić skutek w postaci przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesłanych, przechowywanych lub w inny sposób przetwarzanych. Skutku tego nie należy jednak utożsamiać z wystąpieniem ryzyka naruszenia praw lub wolności osób fizycznych, które stanowiło konsekwencję zaistnienia takiego skutku (zob. art. 33 ust. 1 oraz art. 34 ust. 1 RODO)[8].

Fakt, że warunkiem zaistnienia naruszenia ochrony danych osobowych jest wystąpienie naruszenia bezpieczeństwa, prowadzi do wniosku, iż nie każde naruszenie zasad przetwarzania danych osobowych będzie kwalifikowało się jako naruszenie zdefiniowane w art. 4 pkt 12 RODO[9]. Przepisy rozporządzenia wprowadzają wiele obowiązków po stronie podmiotów, które dane przetwarzają. Swoistą busolą w tym zakresie jest art. 5 RODO, który precyzuje zasady dotyczące przetwarzania danych osobowych[10]. W przepisie tym formułuje się kolejno następujące zasady:

a. Zasada zgodności z prawem, rzetelności i przejrzystości – art. 5 ust. 1 lit. a) RODO,
b. Zasada ograniczenia celu – art. 5 lit. b) RODO,
c. Zasada minimalizacji danych – art. 5 ust. 1 lit. c) RODO,
d. Zasada prawidłowości – art. 5 ust. 1 lit. d) RODO,
e. Zasada ograniczenia przechowywania – art. 5 ust. 1 lit. e) RODO,
f. Zasada integralności i poufności – art. 5 ust. 1 lit. f) RODO.

Pojęcie naruszenia bezpieczeństwa przetwarzania winno być wiązane z ostatnią z wymienionych tu zasad. Zgodnie z art. 5 ust. 1 lit. f) RODO dane osobowe muszą być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. Wniosek taki potwierdza również tytuł Rozdziału IV Sekcji 2 RODO: „Bezpieczeństwo danych osobowych", w którym

8 W literaturze wskazuje się na próby obiektywizacji stopnia naruszenia danych osobowych. Służyć temu może Indeks Stopnia Naruszenia (Breach Level Index – BLI). Zob. S. Sharma, *Data*…, s. 97–99.

9 Por. również A. Sławińska, *Odpowiedzialność*…, s. 27–28, która wskazuje, że należy rozróżnić pojęcie naruszenia ochrony danych osobowych od naruszenia przepisów RODO.

10 Zob. także: P. Fajgielski, *Prawo*…, s. 61–75.

zawarto przepisy dotyczące technicznych i organizacyjnych środków zapewniających bezpieczeństwo przetwarzania (art. 32 RODO) oraz obowiązków aktualizujących się w przypadku naruszenia ochrony danych osobowych. To właśnie z naruszeniem wymienionej w art. 5 ust. 1 lit. f) RODO integralności i poufności danych winno być wiązane wykorzystane w definicji naruszenia ochrony danych osobowych, pojęcie „naruszenie bezpieczeństwa". Dodać przy tym należy, że przejawem uchybienia wprowadzanej przez ten przepis zasadzie będzie również naruszenie dostępności danych osobowych, polegające na czasowej bądź trwałej utracie lub zniszczeniu danych osobowych (Grupa Robocza Art. 29, a w ślad za nią Urząd Ochrony Danych Osobowych, wyróżnia „naruszenie dostępności" jako odrębny od „naruszenia poufności" i naruszenia integralności typ naruszeń ochrony danych)[11]. Naruszenie innych obowiązków wynikających z RODO, np. obowiązków informacyjnych[12], nie mieści się zatem w pojęciu naruszenia bezpieczeństwa i nie może być uznane za naruszenie ochrony danych osobowych.

Z kolei skutkowy charakter naruszenia ochrony danych osobowych przesądza, że nie każde naruszenie bezpieczeństwa prowadzić będzie do wystąpienia tego rodzaju incydentu. Nie jest zatem wystarczające, że w konkretnej sytuacji zostały naruszone lub zawiodły techniczne czy organizacyjne środki bezpieczeństwa. Wystąpić muszą zdarzenia wyliczone w art. 4 pkt 12 RODO. Przykładowo wskazać można, iż nie będzie stanowiło naruszenia ochrony danych osobowych przygotowanie pakietu informacji dla osoby nieuprawnionej do ich otrzymania, w sytuacji, w której nie zgłosi się ona po ich odbiór lub stworzenie dla osoby nieuprawnionej możliwości dostępu do systemu informatycznego w przypadku, gdy nie zgłosi się ona (nie odbierze) po stosowne hasło

11 Zob. Grupa Robocza Art. 29 w Wytycznych pkt I.B.2. oraz Urząd Ochrony Danych Osobowych, Obowiązki administratorów związane z naruszeniami ochrony danych osobowych, wersja 1.0, czerwiec 2019, pkt 1, < https://uodo.gov.pl/pl/134/1029 >, dostęp 14 lipca 2021 r. (dalej: Poradnik UODO). „Poufność" („Confidentiality"), „Integralność" („Integrity") i „Dostępność" („Availability") to elementy tzw. triady CIA – por. wytyczne Agencji Unii Europejskiej ds. Cyberbezpieczeństwa z grudnia 2016: *Guidelines for SMEs on the security of personal data processing*, s. 10, < https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing >, dostęp: 14 lipca 2021 r. (dalej: Wytyczne ENISA).

12 Tak słusznie P. Fajgielski, *Ogólne*…, s. 130.

umożliwiające logowanie, a nawet – jak należy uznać – w przypadku, w którym takie hasło otrzyma, ale nie zaloguje się do systemu. W takiej bowiem sytuacji nie dochodzi do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Jeżeli więc podmiot odpowiadający za przetwarzanie danych zorientuje się, że udostępnił osobie nieuprawnionej hasło do zalogowania się do systemu informatycznego i zmienił je zanim taka osoba podjęła próbę uzyskania dostępu, nie dojdzie, w naszej opinii, do naruszenia ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO.

Stwierdziwszy powyższe trzeba jednak zaznaczyć, że chociaż naruszenie zasad bezpieczeństwa nie jest wystarczające dla stwierdzenia wystąpienia jednego ze skutków wskazanych w art. 4 pkt 12 RODO, to jednak w praktyce naruszenie to do takich skutków będzie z reguły prowadzić[13]. Złamanie zasad bezpieczeństwa oceniać trzeba przez pryzmat środków, jakie w danej sytuacji należało stosować, zgodnie z art. 32 RODO[14]. Należy przy tym wyrazić pogląd, że w sytuacji, w której konieczność wdrożenia określonych środków bezpieczeństwa nie mogła zostać rozsądnie przewidziana (uwzględniając w szczególności stan wiedzy technicznej co do danej kwestii, w tym rozwój nowych technologii informatycznych – por. art. 32 ust. 1 RODO)[15], przyjąć będzie trzeba, iż doszło do naruszenia ochrony danych osobowych, jednakże nie będzie podstaw do karania podmiotu mającego zapewnić bezpieczeństwo. Konieczność zakwalifikowania takiego przypadku jako naruszenia ochrony danych osobowych nie powinna budzić wątpliwości, albowiem doszło do naruszenia bezpieczeństwa (art. 4 pkt 12 RODO), a brak takiej kwalifikacji skutkowałby np. brakiem realizacji obowiązków informacyjnych wobec organu nadzorczego i osób, których dane dotyczą (art. 33 i art. 34 RODO). Z drugiej strony

13 Według Poradnika UODO, pkt 1, naruszenie jest skutkiem złamania zasad bezpieczeństwa danych.

14 Słusznie wskazuje A. Sławińska, *Odpowiedzialność*…, s. 29, że naruszenia bezpieczeństwa nie można odnosić jedynie do środków rzeczywiście wdrożonych przez danego administratora, ale konieczne jest odniesienie się do środków, jakie powinny być wdrożone zgodnie z zasadami określonymi w przepisach art. 32 RODO. Zob. także: W. Chomiczewski, w: *RODO*…, s. 264.

15 Por. A. Sławińska, *Odpowiedzialność*…, s. 30.

niemożliwość przewidzenia określonego sposobu złamania stosowanych zabezpieczeń oceniana w sposób obiektywny, wg istniejącego w danym czasie stanu wiedzy, uniemożliwia twierdzenie, by dochodziło w takim przypadku do naruszenia art. 32 RODO i by istniały podstawy do karania danego podmiotu. Oczywiście nie zmienia to nic w tym, że zarówno administrator, jak i podmiot przetwarzający mają obowiązek regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania – art. 32 ust. 1 lit. d) RODO. Naruszenia w tym zakresie prowadzić będą do potencjalnej odpowiedzialności w przypadku naruszenia ochrony danych osobowych, związanego z nieaktualnymi i niewystarczającymi środkami bezpieczeństwa, które nie zostały odpowiednio zaktualizowane, o ile było to w danym momencie obiektywnie przewidywalne[16].

Skutki naruszenia bezpieczeństwa wyliczone w zamkniętym katalogu, zawartym w art. 4 pkt 12 RODO, podzielić można na dwie kategorie, tj.:
a. Naruszające integralność danych oraz
b. Naruszające poufność danych[17].

Do pierwszej kategorii zaliczyć trzeba przypadki zniszczenia, utracenia i zmodyfikowania danych osobowych. Chodzi więc o te sytuacje, w których naruszono samą treść danych osobowych, ich wartość informacyjną.

Przez zniszczenie danych należy rozumieć sytuację, w której dane osobowe przestają istnieć w tym znaczeniu, iż przestają odpowiadać definicji danych osobowych zawartej w art. 4 pkt 1 RODO. Dane osobowe należy uznać za zniszczone, gdy tracą swoją funkcję w postaci identyfikowania określonej osoby. Do zniszczenia danych osobowych będzie zatem dochodziło zarówno wówczas, gdy ulegną one całkowitej likwidacji (np. dojdzie do trwałego skasowania plików; do spalenia papierowych nośników), jak i wówczas, gdy zniszczona zostanie część informacji, wskutek czego niemożliwe stanie się na ich podstawie dokonanie identyfikacji określonej

16 Wybrane przykłady z praktyki orzeczniczej organów nadzorczych z różnych państw członkowskich UE dotyczące niewystarczających zabezpieczeń danych osobowych zawiera praca M. Abu Gholeh, D. Kuźnicka-Błaszkowska, *Nakładanie*…, s. 183–199.

17 Por. podobnie, proponując podział skutków na kategorię naruszenia integralności danych oraz nieuprawnione zapoznanie się z danymi – W. Chomiczewski, w: *RODO*…, s. 265. Z kolei jeżeli przyjąć podział wskazywany przez Grupę Roboczą Art. 29, to należałoby dodać również trzecią kategorię w postaci naruszenia dostępności, do której zaliczyć należałoby zniszczenie i utracenie danych osobowych (zob. pkt I.B.2. Wytycznych).

osoby (np. na nośniku pozostanie wyłącznie informacja o wysokości zarobków, niepozwalająca stwierdzić, którego z pracowników dotyczy)[18].

Od zniszczenia danych osobowych należy odróżnić ich utratę. W takim przypadku dane w dalszym ciągu istnieją, ale nie są już dostępne dla podmiotu, który te dane przetwarzał. Należy więc pod pojęciem tym rozumieć zarówno sytuację, w której podmiot ten fizycznie stracił dane (np. zgubiono nośnik danych), jak i te, w których dane formalnie znajdują się w dyspozycji tego podmiotu, ale nie ma on możliwości ich wykorzystania (np. z uwagi na przejęcie kontroli nad systemem informatycznym przez podmiot trzeci). W istocie więc utratę danych osobowych należy rozumieć przez pryzmat utraty dostępu do tych danych[19].

Z kolei pod pojęciem zmodyfikowania danych osobowych rozumieć należy, w kontekście naruszenia ochrony danych, sytuację, w której dochodzi do zmiany, zniekształcenia lub zdekompletowania danych osobowych (np. zmiany numeru rachunku bankowego osoby fizycznej, pomieszania numerów telefonów).

Jeżeli zaś chodzi o skutki mieszczące się w kategorii naruszenia poufności danych, to wskazać trzeba na nieuprawnione ujawnienie oraz nieuprawniony dostęp do danych. W obu tych przypadkach dochodzi do sytuacji, w której dane stają się dostępne dla podmiotu, który nie jest do tego uprawniony i nie powinien w związku z tym uzyskać takiej możliwości. Przyjmuje się, że różnica pomiędzy tymi pojęciami zasadza się przede wszystkim na tym, w jaki sposób dane stały się dla takiego podmiotu dostępne[20]. W sytuacji ujawnienia, udostępnienie danych jest rezultatem działania lub zaniechania osoby te dane przetwarzającej. Zasadniczo

18 Słusznie stwierdza się w literaturze, że: „Przez to pojęcie należy także rozumieć zniszczenie części nośnika z danymi osobowymi. Przykładem takiego częściowego zniszczenia będzie wycięcie fragmentu dokumentu i jego wprowadzenie do niszczarki albo zamazanie danych osobowych znajdujących się na części dokumentu w sposób uniemożliwiający ich dalsze przetwarzanie" – W. Chomiczewski, w: *RODO*…, s. 198.

19 Por. decyzja Prezesa Urzędu Ochrony Danych Osobowych (dalej: Prezes UODO) z 17 grudnia 2020 r., nr DKN.5130.1354.2020, < https://uodo.gov.pl/decyzje/DKN.5130.1354.2020 >, dostęp: 14 lipca 2021 r., dotycząca sprawy ID Finance Poland sp. z o.o. w likwidacji, w której doszło do zresetowania ustawień oprogramowania, skutkującego tym, że dane osobowe znajdujące się na serwerze stały się publicznie dostępne, baza danych została pobrana i usunięta z pierwotnej lokalizacji przez podmiot trzeci, który wystąpił do administratora z żądaniem zapłaty wynagrodzenia za jej zwrot tej bazy.

20 W. Chomiczewski, w: *RODO*…, s. 265–266.

będą to więc osoby uprawnione do przetwarzania danych osobowych (administrator, podmiot przetwarzający, osoby przez te podmioty upoważnione)[21]. Chodzi więc np. o przypadek pracownika, który wysyła list do niewłaściwej osoby[22] lub firmy, która wskutek wadliwego przeprowadzenia procedury identyfikacji ujawnia informacje dotyczące swojego klienta osobie trzeciej. Tymczasem, w przypadku uzyskania dostępu do danych, chodzi o sytuację, w której dostęp taki jest rezultatem działania osoby innej niż ta, która te dane przetwarza, a więc, co do zasady, osoby nieuprawnionej[23]. Przykładem tego rodzaju sytuacji będzie włamanie do systemu informatycznego albo kradzież teczki z dokumentami. Zasadniczo więc podstawą do rozróżnienia pomiędzy ujawnieniem a uzyskaniem dostępu będzie to, iż pojęcie ujawniania zakłada aktywność po stronie osoby, która określoną informację posiada, w tym przypadku po stronie osoby przetwarzającej dane. Z kolei pojęcie uzyskania dostępu zakłada aktywność po stronie osoby trzeciej.

Ciekawym problemem może być to, czy nieuprawnionym ujawnieniem danych jest ich udostępnienie osobie, która wprawdzie nie była

21 Np.: ujawnienie w sieci Internet nadmiarowych danych osób, którym przyznano licencje sędziego piłkarskiego, por. decyzja Prezesa UODO z 25 kwietnia 2019 r., nr ZSPR.440.43.2019, < https://uodo.gov.pl/decyzje/ZSPR.440.43.2019 >, dostęp: 14 lipca 2021 r.; ujawnienie na platformie e-learningowej nagrań obrazujących przebieg egzaminów praktycznych z pediatrii na uniwersytecie medycznym, por. decyzja Prezesa UODO z 5 stycznia 2021 r., nr DKN.5131.6.2020, < https://uodo.gov.pl/decyzje/DKN.5131.6.2020 >, dostęp: 14 lipca 2021 r.

22 Por. decyzja Prezesa UODO z 11 stycznia 2021 r., nr DKN.5131.7.2020, < https://www.uodo.gov.pl/decyzje/DKN.5131.7.2020 >, dostęp: 14 lipca 2021 ., dotycząca sprawy ENEA SA, w której wysłano do przypadkowego nieuprawnionego odbiorcy wiadomość e-mail wraz z załącznikiem w postaci niezaszyfrowanego pliku zawierającego dane osobowe adresata wiadomości i innych osób (imiona, nazwiska, adresy e-mail, numery telefonów, a także informacje o dacie rejestracji).

23 Np.: pobranie kopii bazy danych Krajowej Szkoły Sądownictwa i Prokuratury, zawierającej dane m.in. sędziów i prokuratorów, przez nieustalone osoby, wskutek niezapewnienia przez administratora odpowiedniego bezpieczeństwa danych, por. decyzja Prezesa UODO z 11 lutego 2021 r., nr DKN.5130.2024.2020 < https://www.uodo.gov.pl/decyzje/DKN.5130.2024.2020 >, dostęp: 14 lipca 2021 r.; nieuprawniony dostęp do baz danych klientów sklepów internetowych, poprzez uzyskanie nieuprawnionego dostępu do panelu pracownika, por. decyzja Prezesa UODO z 10 września 2019 r., nr ZSPR.421.2.2019, < https://uodo.gov.pl/decyzje/ZSPR.421.2.2019 >, dostęp: 14 lipca 2021 r.; kradzież komputera prywatnego z danymi osobowymi kandydatów na studia, por. decyzja Prezesa UODO z 21 sierpnia 2020 r., nr ZSOŚS.421.225.2019, < https://www.uodo.gov.pl/decyzje/ZSO%C5%9AS.421.25.2019 >, dostęp: 14 lipca 2020 r.

uprawniona do ich uzyskania, ale takie dane już wcześniej posiadała (np. ujawnienie wcześniej znanych danej osobie danych jej współmałżonka). Na gruncie różnych dziedzin prawa wyrażane jest w tym kontekście stanowisko, że ujawnić informację wobec kogoś można jedynie wówczas, gdy osoba taka tej informacji wcześniej nie posiadała[24]. Jeżeli zaś wobec takiej osoby nie może dojść do ujawnienia danych, to czy przypadek taki stanowi naruszenie bezpieczeństwa danych w rozumieniu art. 4 pkt 12 RODO? Na tak sformułowane pytanie należy udzielić odpowiedzi twierdzącej. Innymi słowy, naruszeniem bezpieczeństwa danych jest także bezprawne udostępnienie danych osobowych osobie, która dane te posiada z innych (nawet legalnych) źródeł. Przyjęcie odmiennego stanowiska prowadziłoby bowiem do wniosków niemożliwych do zaakceptowania. Przykładowo brak byłoby naruszenia w przypadku działania pracownika banku ujawniającego tajemnicę bankową wobec osoby trzeciej, która posiadała ją już wcześniej z innego źródła. Potencjalnego uzasadnienia dla zastosowania w takim przypadku art. 4 pkt 12 RODO upatrywać można w przyjęciu, iż w tego rodzaju specyficznej sytuacji należy mówić o uzyskaniu dostępu do informacji, pomimo że jego źródłem jest działanie osoby uprawnionej do przetwarzania danych, a nie zachowanie osoby trzeciej (odbiorcy danych).

W obu przypadkach, ujawniania i dostępu do danych, musi dojść do zachowania nieuprawnionego. Tym samym każdorazowego badania wymagać będzie, czy przetwarzanie takie miało podstawę legalizującą, tj. czy spełniona była jedna z przesłanek wymienionych w art. 6 ust. 1 RODO lub art. 9 ust. 2 RODO, względnie czy doszło do powierzenia przetwarzania danych albo udzielenia odpowiedniego upoważnienia.

Kolejno należy zwrócić uwagę, że wystąpienie naruszenia bezpieczeństwa danych osobowych może stanowić rezultat zarówno zachowania umyślnego, jak i nieumyślnego[25]. Istotne jest jedynie obiektywne

24 Por. W. Chomiczewski, w: *RODO*…, s. 196; A. Nerka, w: *Ogólne*…, s. 112; W. Wróbel, D. Zając, w: *Kodeks*…, komentarz do art. 265, teza nr 20: „Pojęcie ujawnienia zakłada bowiem, że sprawca tego czynu zapoznaje dopiero inną osobę z informacjami, do których dotychczas nie miała dostępu". Por. również T. Razowski, w: *Kodeks*…, komentarz do art. 265, teza nr 11 oraz – w kontekście danych, które stały się publicznie znane – A. Lach, w: *Kodeks*…, s. 1131.

25 Zob. także: P. Voigt, A. von dem Bussche, *The EU*…, s. 65; P. Fajgielski, *Ogólne*…, s. 131; W. Chomiczewski, w: *RODO*…, s. 264; L. Tosoni, w: *The EU*…, s. 192.

wystąpienie naruszenia (aczkolwiek istnienie i postać winy będzie miała znaczenie dla reakcji i konsekwencji naruszenia, szczególnie ze strony organu nadzorczego)[26]. Tak bowiem należy rozumieć ten fragment definicji z art. 4 pkt 12 RODO, w którym wskazano, że naruszenie bezpieczeństwa prowadzi do „przypadkowego lub niezgodnego z prawem" wystąpienia omówionych powyżej skutków naruszenia (ang. *accidental or unlawful*, niem. *unbeabsichtigt oder unrechtmäßig*). Odwołanie się do przypadkowego naruszenia bezpieczeństwa przesądza, że pomimo braku zamiaru może mieć miejsce naruszenie ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO. Konkluzja ta znajduje potwierdzenie w przepisie art. 83 ust. 2 lit. b) RODO, w którym wśród dyrektyw wymiaru kary administracyjnej wymieniono umyślny lub nieumyślny charakter naruszenia. Wystąpienie naruszenia nie zostało zatem zawężone wyłącznie do przypadków działania zamierzonego.

3. Skutki naruszenia ochrony danych osobowych

Problematyka naruszenia ochrony danych osobowych zyskała na gruncie przepisów RODO szczególne znaczenie. Potwierdza to szeroki wachlarz konsekwencji wystąpienia takiego naruszenia Wyróżnić należy tu:
a. Skutki organizacyjne,
b. Obowiązki dokumentacyjne i zgłoszeniowe,
c. Administracyjne kary pieniężne,
d. Odpowiedzialność odszkodowawczą.

Wskazane powyżej skutki organizacyjne wiązać trzeba ze wskazaną na wstępie zasadą wyrażoną w art. 5 ust. 1 lit f) RODO. Dane osobowe muszą być przetwarzane w sposób zapewniający ich odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. Nadto, zgodnie z art. 32 ust. 1 RODO, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator

26 A. Sławińska, *Odpowiedzialność*…, s. 30; W. Chomiczewski, w: *RODO*…, s. 264.

i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Wreszcie, zgodnie z art. 32 ust. 2 RODO, oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Wymogi te sprawiają, że każdorazowe naruszenie ochrony danych pociągać musi za sobą weryfikację stosowanych przez dany podmiot środków organizacyjnych i technicznych. W takiej sytuacji istnieje bowiem przynajmniej ryzyko, że nie są one odpowiednie do istniejących zagrożeń i prawdopodobieństwa wystąpienia naruszenia. Rewizji wymagać może zakres udzielonych upoważnień (np. zbyt szeroki zakres uprawnień do przetwarzania danych przyznanych określonej grupie pracowników), dobór podmiotów przetwarzających dane lub zakres prowadzonej z nimi współpracy (np. konieczność zmiany dostawcy usług na takiego, który zapewni lepsze gwarancje zgodnego z prawem przetwarzania lub ograniczenie zakresu przetwarzania powierzonego takiemu dostawcy) czy też współpraca prowadzona z innymi administratorami.

Niezależnie od powyższego, wystąpienie przypadku naruszenia ochrony danych osobowych skutkuje obowiązkami dokumentacyjnymi i zgłoszeniowymi po stronie administratora i – w pewnym zakresie – podmiotu przetwarzającego.

Zgodnie z art. 33 ust. 5 RODO administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania art. 33 RODO. Praktycznym sposobem realizacji tego obowiązku jest prowadzenie przez administratora odpowiedniego rejestru naruszeń, w którym ujmowane będą przynajmniej informacje umożliwiające spełnienie ww. wymogu, a więc informacje na temat okoliczności naruszenia, jego skutkach oraz podjętych działaniach zaradczych. Należy podkreślić, że omawiany obowiązek dokumentacyjny dotyczy każdego przypadku stwierdzonego naruszenia i jest niezależny od tego,

czy konieczne jest zgłoszenie takiego przypadku do organu nadzorczego lub powiadomienie o nim osoby, której dane dotyczą. W każdym również przypadku stwierdzenia naruszenia aktualizuje się, ciążący na podmiocie przetwarzającym (art. 33 ust. 2 RODO), obowiązek zgłoszenia tego faktu administratorowi, bez zbędnej zwłoki.

W zależności od tego, jaki stopień ryzyka naruszenia praw lub wolności osób fizycznych jest skutkiem danego deliktu, na administratorze ciążyć mogą dalsze obowiązki. W przypadku, gdy jest mało prawdopodobne, by naruszenie skutkowało takim ryzykiem, administrator poprzestać może na omówionym powyżej wewnętrznym udokumentowaniu naruszenia. Zdaniem Grupy Roboczej Art. 29, wyrażonym w Wytycznych, przykładem takiego małego prawdopodobieństwa może być sytuacja, w której dane osobowe już są publicznie dostępne i ujawnienie takich danych nie wiąże się z prawdopodobnym ryzykiem dla danej osoby fizycznej[27]. Jako przykład naruszenia, które nie wymagałoby zgłoszenia organowi nadzorczemu, Grupa Robocza Art. 29 wskazuje również przypadek utraty bezpiecznie zaszyfrowanego urządzenia mobilnego, z którego korzystają administrator i jego pracownicy[28]. Stwierdza, iż zakładając, że klucz kryptograficzny jest bezpiecznie przechowywany przez administratora i nie jest to jedyna kopia danych osobowych, dane osobowe będą niedostępne dla atakującego. Oznacza to, że przedmiotowe naruszenie najprawdopodobniej nie będzie wiązało się z ryzykiem naruszenia praw i wolności osób, których te dane dotyczą. Jeżeli później okaże się, że klucz kryptograficzny został złamany lub oprogramowanie albo algorytm szyfrujący ma słabe punkty, poziom ryzyka naruszenia praw i wolności osób fizycznych zmieni się i wówczas zgłoszenie może stać się konieczne. Należy jednak zaznaczyć, że pomimo konstruowania tego rodzaju przykładów w ww. wytycznych, każdy przypadek stwierdzenia naruszenia powinien być analizowany indywidualnie i z uwzględnieniem okoliczności danej sprawy. Grupa Robocza Art. 29 zaleca, by dokonując analizy poziomu ryzyka, brać pod uwagę następujące kryteria: rodzaj naruszenia; charakter, wrażliwość i ilość danych osobowych; łatwość identyfikacji osób fizycznych; wagę konsekwencji dla osób fizycznych; cechy szczególne

27 Pkt II D Wytycznych.

28 Pkt II D Wytycznych.

danej osoby fizycznej; cechy szczególne administratora danych; liczbę osób fizycznych, na które naruszenie wywiera wpływ[29].

4. Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadomienie osoby, której dane dotyczą

W każdym przypadku, w którym prawdopodobieństwo wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych w związku z określonym naruszeniem ochrony danych osobistych jest wyższe od małego, administrator jest zobligowany do dokonania zgłoszenia takiego naruszenia organowi nadzorczemu[30]. W Polsce organem tym jest Prezes Urzędu Ochrony Danych Osobowych[31]. Zgłoszenie powinno nastąpić bez zbędnej zwłoki[32] – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia[33]. W szczególnych przypadkach RODO dopuszcza udzielenie informacji organowi nadzorczemu nie jednorazowo, ale sukcesywnie, a więc w miarę ich

29 Pkt IV B Wytycznych; por. również s. 20–21 Wytycznych ENISA.

30 Zob. art. 33 ust. 1 RODO. Należy pamiętać, że obowiązek zgłoszenia oraz inne specyficzne obowiązki w zakresie naruszeń ochrony danych osobowych mogą wynikać również z przepisów szczególnych (zarówno UE, jak i polskich). Szerzej: Poradnik UODO, pkt 17. Kwestie zgłaszania organowi nadzorczemu naruszeń ochrony danych osobowych oraz zawiadamiania o takich naruszeniach osób, których dane dotyczą, mogą zostać doprecyzowane w kodeksach postępowania przyjmowanych przez zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające – art. 40 ust. 2 lit. i) RODO. Szerzej na temat zgłoszenia naruszenia ochrony danych osobowych zob. C. Burton, w: *The EU*…, s. 641–650.

31 Zob. art. 34 ust. 1 ustawy z dn. 10 maja 2018 r. o ochronie danych osobowych, Dz.U. 2019, poz. 1781, tekst jedn. Na temat pozycji ustrojowej Prezesa UODO zob. np. M. Abu Gholeh, *Pozycja*…, s. 163–181.

32 Jak wskazano w motywie 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. Zgodnie z art. 33 ust. 1 *in fine* RODO: „Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia".

33 Zgodnie z art. 55 ustawy o ochronie danych osobowych Prezes Urzędu może prowadzić system teleinformatyczny umożliwiający administratorom dokonywanie zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 rozporządzenia 2016/679. Więcej na temat sposobów zgłaszania naruszeń Prezesowi Urzędu Ochrony Danych Osobowych: < https://uodo.gov.pl/pl/134/233 >, dostęp: 14 lipca 2021 r. Zob. także: P. Fajgielski, *Informowanie*…, s. 43 i n.

pozyskiwania (sukcesywne dokonywanie zgłoszenia)[34]. Jak wskazuje się w Wytycznych: „administratorzy nie zawsze są w stanie uzyskać dostęp do wszystkich niezbędnych informacji na temat naruszenia w ciągu 72 godzin od stwierdzenia wystąpienia naruszenia, ponieważ pełne i wyczerpujące szczegółowe informacje na temat danego incydentu nie zawsze są dostępne w tym początkowym okresie"[35]. Dotyczy to bardziej złożonych naruszeń, wymagających pogłębionego postępowania wyjaśniającego (analiz kryminalistycznych) ze strony administratora. W takich przypadkach należy zgłosić do organu nadzorczego bez zbędnej zwłoki posiadane informacje cząstkowe lub dane przybliżone[36] oraz uzupełnić zgłoszenie o brakujące informacje niezwłocznie po tym, jak administrator wejdzie w ich posiadanie[37]. Zgłoszenie naruszenia powinno co do zasady obejmować cztery grupy informacji:

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 (art. 33 ust. 3 RODO).

Jak łatwo dostrzec, obowiązek zgłoszeniowy do organu nadzorczego powstaje w momencie „stwierdzenia naruszenia". Pojęcie to może rodzić wątpliwości interpretacyjne, wynikające choćby z tego, że administrator może nie mieć od razu (lub w ogóle nie uzyskać) pewności, że do

34 Art. 33 ust. 4 RODO.

35 Zob. pkt II.B.2. Wytycznych.

36 W Wytycznych wskazuje się na możliwość podania w zgłoszeniu np. przybliżonej liczby osób fizycznych, na które dane naruszenie wywarło wpływ lub przybliżonej liczby wpisów danych osobowych, których dotyczy to naruszenie (pkt II.B.1. Wytycznych).

37 Zob. także: Poradnik UODO, pkt 7.

naruszenia rzeczywiście doszło (np. nie wie, co stało się z segregatorem zawierającym dokument lub identyfikuje ślad w systemie informatycznym, który może, ale nie musi, świadczyć o nieuprawnionej ingerencji w ten system ze strony podmiotu trzeciego). W tym kontekście ponownie zwrócić należy uwagę na Wytyczne opracowane przez Grupę Roboczą Art. 29. W dokumencie tym wskazano m.in., że w opinii Grupy Roboczej Art. 29 należy uznać, że administrator „stwierdził" wystąpienie naruszenia w momencie, w którym uzyskał wystarczającą dozę pewności co do tego, że doszło do wystąpienia incydentu bezpieczeństwa, który doprowadził do ujawnienia danych osobowych[38]. Podniesiono, że to, kiedy dokładnie można uznać, że administrator „stwierdził" wystąpienie określonego naruszenia, będzie zależało od okoliczności, w jakich doszło do tego naruszenia. W niektórych przypadkach wystąpienie naruszenia można stosunkowo łatwo stwierdzić już na początku, natomiast w innych ustalenie, czy doszło do ujawnienia danych osobowych, może wymagać czasu. Grupa Robocza Art. 29 przyjęła, że w tym kontekście powinno się jednak położyć nacisk na szybkie zbadanie danego incydentu w celu ustalenia, czy faktycznie doszło do naruszenia ochrony danych osobowych, a jeżeli tak – podjąć działania zaradcze i, w razie konieczności, zgłosić naruszenie. W Wytycznych stwierdzono, że po otrzymaniu pierwszej informacji o potencjalnym naruszeniu ochrony danych osobowych od osoby fizycznej, organizacji medialnej lub z innego źródła, lub po samodzielnym wykryciu incydentu bezpieczeństwa administrator może przeprowadzić krótkotrwałe postępowanie, aby ustalić, czy faktycznie doszło do danego naruszenia. Do momentu zakończenia tego postępowania nie można uznać, że administrator „stwierdził" wystąpienie naruszenia[39]. Oczekuje się jednak, że wstępne postępowanie powinno

38 Pkt II.A.2. Wytycznych.

39 Grupa Robocza Art. 29 posługuje się m.in. przykładem, w którym osoba fizyczna informuje administratora, że otrzymała wiadomość e-mail, której nadawca podszywa się pod administratora i która zawiera dane osobowe dotyczące (faktycznego) korzystania z usług administratora przez tę osobę i sugeruje, że doszło do złamania środków bezpieczeństwa stosowanych przez administratora. Administrator przeprowadza krótkie postępowanie, w toku którego uzyskuje potwierdzenie, że doszło do włamania do jego sieci, i gromadzi dowody świadczące o nieuprawnionym dostępie do danych osobowych. Jak wskazuje Grupa Robocza Art. 29: „Od tego momentu przyjmuje się, że administrator «stwierdził» wystąpienie naruszenia, a zgłoszenie naruszenia organowi nadzorczemu staje się obowiązkowe, chyba że prawdopodobieństwo, iż

rozpocząć się możliwie jak najszybciej i doprowadzić do ustalenia z wystarczającą dozą pewności, czy w danym przypadku faktycznie doszło do wystąpienia naruszenia; następnie można przeprowadzić bardziej szczegółowe postępowanie.

Podzielając stanowisko Grupy Roboczej Art. 29, należy uznać, że obowiązek zgłoszeniowy powstaje po stronie administratora, gdy stwierdzi on naruszenie ochrony danych osobowych, przy czym owo stwierdzenie może być poprzedzone dokonaniem czynności sprawdzających. W rezultacie moment stwierdzenia naruszenia nie będzie w każdym przypadku równoznaczny z momentem, w którym administrator powziął informację o zdarzeniu, które może świadczyć o wystąpieniu naruszenia. W wielu przypadkach będą to jednak okoliczności praktycznie jednoczasowe, np. w sytuacji zuchwałej kradzieży dokumentów z danymi osobowymi. Przeprowadzane czynności sprawdzające muszą mieć jednak zawsze charakter krótkotrwały. Jeśli nie umożliwiają one rozstrzygnięcia, czy do naruszenia doszło lub też nie umożliwiają dokonania oceny co do stopnia ryzyka związanego z naruszeniem, administrator powinien dokonać zgłoszenia do organu nadzorczego.

Zastrzeżenia budzi przy tym prezentowany w Wytycznych oraz powtórzony w Poradniku UODO pogląd zgodnie z którym: „W przypadku jakichkolwiek wątpliwości administrator powinien zgłosić naruszenie, nawet jeśli taka ostrożność mogłaby się okazać nadmierna”[40]. Rozumiejąc potrzebę uwrażliwienia administratorów na przypadki naruszenia ochrony danych osobowych, szczególnie w pierwszych latach obowiązywania RODO, wydaje się jednak, że takie ukształtowanie obowiązku notyfikacyjnego nie znajduje oparcia w przepisach prawa i może prowadzić do nadmiernego sankcjonowania zaniechań zgłoszenia. Jak słusznie wskazuje również A. Sławińska, może to skutkować także znacznym przeciążeniem UODO[41]. Organ nadzorczy powinien koncentrować się na sprawach istotnych z punktu widzenia ochrony praw jednostek. Konieczność analizy zbędnych z punktu widzenia przepisów RODO zgłoszeń

będzie wiązało się ono z ryzykiem naruszenia praw i wolności osób fizycznych, jest niewielkie”. Zob. pkt II.A.2. Wytycznych.

40 Pkt IV.B. Wytycznych oraz pkt 9.1. Poradnika UODO.

41 A. Sławińska, *Odpowiedzialność*…, s. 37.

oznacza, że część sił i środków pozostających w dyspozycji UODO nie zostanie wykorzystana efektywnie.

Dodatkowy obowiązek ciąży na administratorze wówczas, gdy stwierdzone naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (Grupa Robocza Art. 29, wskazuje tu jako przykład sytuację, w której szpitalna dokumentacja jest niedostępna przez 30 godzin w wyniku cyberataku)[42]. W takim bowiem przypadku, co do zasady, administrator ma obowiązek poinformowania o naruszeniu osobę, której dane dotyczą (art. 34 ust. 1 RODO). Jasnym, prostym językiem należy opisać charakter naruszenia ochrony danych osobowych oraz podać przynajmniej informacje, o których mowa w art. 33 ust. 3 lit. b) – d) RODO[43]. Nie wystarczy przy tym, odwołując się do wymogu opisania możliwych konsekwencji naruszenia ochrony danych osobowych – art. 33 ust. 3 lit. c) w zw. z art. 34 ust. 2 RODO – wskazać ogólnie zainteresowanej osobie np., że osoba trzecia może posłużyć się jej danymi. Konieczne jest wskazanie konkretnych obszarów życia społeczno-gospodarczego lub okoliczności, w których takie sytuacja może nastąpić (np. możliwość posłużenia się cudzym imieniem i nazwiskiem oraz numerem PESEL w celu wyłudzenia kredytu lub pożyczki albo ubezpieczenia lub środków z ubezpieczenia, skorzystania ze świadczeń zdrowotnych, uzyskania informacji o stanie zdrowia danej osoby, udziału w głosowaniu nad budżetem partycypacyjnym)[44]. Również informacja o zastosowanych lub proponowanych przez administratora środkach zaradczych – art. 33 ust. 3 lit. d) w zw. z art. 34 ust. 2 RODO – powinna być dostatecznie konkretna i odnosić się do sytuacji, w której znalazła się osoba poszkodowana na skutek ujawnienia jej danych[45].

42 Pkt VII.B.viii Wytycznych.

43 To jest: imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji; opis możliwych konsekwencji naruszenia ochrony danych osobowych; opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków. Na temat praktycznych kwestii związanych z poinformowaniem o naruszeniu zob. np. A. Bevitt, P. Carey, *Data*…, s. 103.

44 Zob. np. decyzja Prezesa UODO z 20 listopada 2018 r., ZWAD.405.11.2018, < https://uodo.gov.pl/decyzje/ZWAD.405.11.2018 >, dostęp: 14 lipca 2021 r.

45 Przykładowo – w związku z ujawnieniem imienia i nazwiska danej osoby, jej danych kontaktowych wraz z miejscem zamieszkania oraz innymi informacjami ujawnionymi na załączonych

Obowiązek zawiadomienia osób, których dane dotyczą, nie zachodzi w przypadkach wymienionych w art. 34 ust. 2 RODO (zawiadomienie nie jest wymagane), tj.:

a. Gdy administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony, i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie, jak szyfrowanie uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych (wg Grupy Roboczej Art. 29 może to na przykład obejmować zabezpieczenie danych osobowych za pomocą najnowocześniejszego szyfrowania lub tokenizacji)[46],
b. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą (wg Grupy Roboczej Art. 29 w niektórych sytuacjach administrator mógł natychmiast zidentyfikować osobę fizyczną, która uzyskała dostęp do danych osobowych, i podjąć wobec niej działania zanim mogła ona w jakikolwiek sposób wykorzystać te dane)[47],
c. Wymagałoby ono niewspółmiernie dużego wysiłku, przy czym w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób (wg Grupy Roboczej Art. 29 np. archiwum urzędu statystycznego uległo zalaniu, a dokumenty zawierające dane osobowe przechowywano tylko w formie papierowej)[48].

Należy przy tym mieć na uwadze – co jest aktualne w odniesieniu do każdego stopnia ryzyka, o którym mowa w art. 33 i 34 RODO – że nie jest wymagane, by wysokie ryzyko się zmaterializowało i by faktycznie doszło do naruszenia praw lub wolności. Nie ma znaczenia, czy

fotografiach z życia rodzinnego – Prezes UODO wskazał na konieczność zasugerowania przez administratora osobie, której dane dotyczą ostrożności przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu lub telefonu oraz zachowania ostrożności przez dzieci oraz członków najbliższej rodziny na kontakty z nieznajomymi osobami. Zob. decyzja Prezesa UODO z 27 marca 2019 r., nr ZWAD.405.1383.2018, < https://uodo.gov.pl/decyzje/ZWAD.405.1383.2018 >, dostęp: 14 lipca 2021 r.

46 Pkt III.D. Wytycznych.

47 Pkt III.D. Wytycznych.

48 Pkt III.D. Wytycznych.

ostatecznie ich naruszenie nastąpi[49]. Wystarczy samo pojawienie się wysokiego ryzyka naruszenia.

5. Sankcje z tytułu naruszenia ochrony danych osobowych

Niezależnie od konsekwencji organizacyjnych oraz obowiązków dokumentacyjnych i zgłoszeniowych, naruszenie ochrony danych osobowych pociągać może za sobą sankcje związane z wystąpieniem danego incydentu.

Naruszenie ochrony danych osobowych wiązać może się z administracyjną karą pieniężną nakładaną przez organ nadzorczy w wysokości wynikającej z przepisów RODO[50]. Kara ta nie ma jednak charakteru obligatoryjnego odnośnie do każdego naruszenia określonych przepisów RODO[51]. Jest sankcją o charakterze fakultatywnym – por. art. 83 ust. 2: „Decydując, czy nałożyć administracyjną karę pieniężną (…)". W każdym przypadku naruszenia organ nadzorczy powinien bowiem rozważyć nie tylko wysokość kary pieniężnej, ale przede wszystkim to, czy ze środka tego w ogóle należy skorzystać, a więc, czy nałożyć karę za dane naruszenie. Decyzja w tej sprawie zależeć ma od okoliczności każdego indywidualnego przypadku (art. 83 ust. 2 RODO)[52]. Okoliczności te mogą przy tym wskazywać, że wystarczające jest np. zastosowanie innych środków naprawczych (uprawnień naprawczych) oddanych do dyspozycji organu nadzorczego, w tym przede wszystkim różnego rodzaju nakazów skierowanych do administratora – zob. art. 58 ust. 2 lit. i) RODO. Jak wskazano w motywie 148 RODO: „Jeżeli naruszenie jest niewielkie lub jeżeli grożąca kara pieniężna stanowiłaby dla osoby fizycznej nieproporcjonalne obciążenie, można zamiast tego udzielić upomnienia". W tym ostatnim przypadku nałożenie kary pieniężnej uznać należałoby za sprzeczne z wymogami proporcjonalności i prawnie niedopuszczalne[53]. Organ nadzorczy powinien zatem rozważyć w każdym przypadku, które z określonych

49 Por. W. Chomiczewski, w: *RODO*…, s. 721.

50 Odrębne zasady dotyczące nakładania kar administracyjnych przewidziano w ustawie z dn. 10 maja 2018 r. o ochronie danych osobowych, w odniesieniu do jednostek sektora finansów publicznych, instytutów badawczych i Narodowego Banku Polskiego.

51 J. Łuczak, w: *RODO*…, s. 1060; P. Fajgielski, *Ogólne*…, s. 656.

52 Również art. 58 ust. 2 lit. i) RODO wskazuje, że zastosowanie przez organ nadzorczy administracyjnej kary pieniężnej następuje „zależnie od okoliczności konkretnej sprawy".

53 Zob. także: W. Kotschy, w: *The EU*…, s. 1189.

w art. 58 ust. 2 RODO uprawnień naprawczych należy zastosować, a swój wybór należycie uzasadnić[54].

Inne stanowisko zdaje się prezentować w tej sprawie Wojewódzki Sąd Administracyjny w Warszawie. W wyroku z 28 lutego 2020 r. uznał bowiem, że: „zgodnie z art. 58 ust. 2 lit. i RODO, każdemu organowi nadzorczemu przysługuje uprawnienie do zastosowania, oprócz lub zamiast innych środków naprawczych przewidzianych w art. 58 ust. 2 RODO, administracyjnej kary pieniężnej na mocy art. 83 rozporządzenia, zależnie od okoliczności konkretnej sprawy. Organ nie ma zatem obowiązku uzasadnienia dlaczego nie zastosował innego środka naprawczego. Ma natomiast obowiązek uzasadnienia nałożenia administracyjnej kary finansowej"[55]. Środki naprawcze w postaci upomnienia oraz określonych nakazów zachowania (bez nałożenia jednak kary pieniężnej) zostały zastosowane przez Prezesa UODO np. w decyzji z 12 listopada 2020 r. dotyczącej naruszenia ochrony danych osobowych przez U. Sp. z o.o.[56] Sprawa ta dotyczyła ujawienia listy osób, które przebywają na kwarantannie. Zdaniem organu informacja o skierowaniu danej osoby na kwarantannę należy przy tym do kategorii danych dotyczących zdrowia (art. 4 pkt 15 RODO)[57]. Naruszenie to trudno jest uznać zatem za niewielkie. Przeciwnie, ujawnienie danych wielu osób dotyczących wrażliwej kwestii skierowania na kwarantannę generalnie powinno być oceniane jako poważne. Trudno zatem zgodzić się ze stanowiskiem, że upomnienie połączone

54 Jak wskazuje Grupa Robocza Art. 29 w swych wytycznych dotyczących administracyjnych kar pieniężnych z 2017 r.: „Zachęca się organy nadzorcze do stosowania rozważnego i wyważonego podejścia w zakresie stosowania środków naprawczych, tak aby reakcja na dane naruszenie była zarówno skuteczna i odstraszająca, jak również proporcjonalna. Celem nie jest tu traktowanie kar pieniężnych jako ostateczności, czy też powstrzymywanie się od ich stosowania, lecz nakładanie ich w sposób uniemożliwiający podważanie ich skuteczności jako narzędzia" – pkt II.3. wytycznych w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679 przyjętych w dniu 3 października 2017 r.

55 Wyrok WSA w Warszawie z 28 lutego 2020 r., II SA/Wa 1511/19 (sprawa Dolnośląskiego Związku Piłki Nożnej), wyrok nieprawomocny. Analogiczne stanowisko zawarł WSA w Warszawie w wyroku z 3 września 2020 r., II SA/Wa 2559/19 (sprawa Morele.net sp. z o.o.), wyrok nieprawomocny.

56 Decyzja nr DKN.5101.25.2020, < https://uodo.gov.pl/decyzje/DKN.5101.25.2020 >, dostęp: 14 lipca 2021 r.

57 Kwestia takiej kwalifikacji prawnej informacji o objęciu danej osoby kwarantanną może być jednak dyskusyjna. Zob. J. Błachut, S. Dudzik, D. Olczyk, *Ochrona*…, s. 50–51.

z nakazami dotyczącymi zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony danych osobowych było adekwatną odpowiedzią organu na stwierdzone naruszenie[58].

Wysokość kary może być różna w zależności od rodzaju naruszenia, a w pewnym zakresie również w zależności od charakteru podmiotu, który dopuścił się naruszenia. W przypadkach wskazanych w art. 83 ust. 4 RODO może to być wysokość do 10 000 000 €, a w przypadku przedsiębiorstwa w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa. W przypadkach z kolei, o których mowa w art. 83 ust. 5 RODO, zagrożenie wzrasta, odpowiednio, do 20 000 000 € i 4% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Ograniczenie wysokości kar pieniężnych, które mogą być nakładane względem jednostek sektora finansów publicznych, instytutów badawczych oraz Narodowego Banku Polskiego, przewiduje art. 102 ustawy o ochronie danych osobowych. W tym przypadku kara nie może przekroczyć 100 000 zł, a w przypadku państwowych i samorządowych instytucji kultury – 10 000 zł.

Nie jest przy tym w pełni jasne, która z podanych w art. 83 RODO podstaw prawnych nałożenia kary pieniężnej znajduje zastosowanie do przypadków naruszenia ochrony danych osobowych. Zgodnie bowiem z art. 83 ust. 4 RODO niższemu zagrożeniu podlega m.in. naruszenie przepisów dotyczących obowiązków administratora i podmiotu przetwarzającego, o których mowa w art. 25–39 RODO, a więc m.in. przepisów dotyczących bezpieczeństwa danych osobowych (art. 32 RODO). Z kolei, zgodnie z art. 83 ust. 5 RODO, wyższemu zagrożeniu podlega m.in. naruszenie dotyczące podstawowych zasad przetwarzania, o których to zasadach i warunkach mowa jest m.in. w art. 5 RODO – a więc m.in. w zakresie integralności i poufności – art. 5 ust. 1 lit. f) RODO. Powstaje więc pytanie, czy w przypadku naruszenia ochrony danych dochodzi do kolizji tych dwóch podstaw wymiaru kary. Możliwa wydaje się bowiem argumentacja, w myśl której w przypadku, w którym naruszenie stanowiło rezultat niezapewnienia właściwego bezpieczeństwa przetwarzania

58 Upomnienie zastosował Prezes UODO również w decyzji z 11 stycznia 2021 r., nr DKN. 5130.2815.2020 w sprawie U. SA. W tym przypadku zastosowany środek (przynajmniej *prima facie*) nie budzi poważniejszych zastrzeżeń.

(art. 32 RODO), a w szczególności niezapewnienia odpowiednich do ryzyka środków organizacyjnych i technicznych, zastosowanie winien znaleźć art. 83 ust. 4 RODO na zasadzie *lex specialis* wobec art. 83 ust. 5 RODO, który odnosi się do naruszeń ogólnych zasad przetwarzania. Niemniej jednak na uwadze mieć należy, że zgodnie z art. 83 ust. 3 RODO, jeżeli administrator lub podmiot przetwarzający narusza umyślnie lub nieumyślnie w ramach tych samych lub powiązanych operacji przetwarzania kilka przepisów RODO, całkowita wysokość administracyjnej kary pieniężnej nie przekracza wysokości kary za najpoważniejsze naruszenie. Uwzględniając ten przepis, Prezes Urzędu Ochrony Danych Osobowych, wydając decyzję z 25 kwietnia 2019 r. w sprawie Dolnośląskiego Związku Piłki Nożnej[59] oraz decyzję z 10 września 2019 r. w sprawie Morele.net sp. z o.o.[60], zastosował art. 83 ust. 5 RODO (wyższe zagrożenie), pomimo jednoczesnego stwierdzenia naruszenia art. 5 ust. 1 lit. f) RODO oraz przepisów art. 32 RODO.

Należy zwrócić uwagę, że RODO wyraźnie wprowadza dyrektywy wymiaru kary administracyjnej. W art. 83 ust. 2 RODO wskazano, że administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego indywidualnego przypadku, oprócz lub zamiast środków, o których mowa w art. 58 ust. 2 lit. a) – h) oraz j) RODO (uprawnienia naprawcze organu nadzorczemu inne niż administracyjne kary pieniężne). Decydując zaś, czy nałożyć administracyjną karę pieniężną oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę m.in. na: umyślny lub nieumyślny charakter naruszenia – art. 83 ust. 2 lit. b) RODO; działania podjęte w celu zminimalizowania szkody poniesionej przez osobę, której dane dotyczą – art. 83 ust. 2 lit. c) RODO; stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32 RODO [art. 83 ust. 2 lit. d) RODO; *privacy by design, privacy by default*, techniczna i organizacyjna ochrona danych]; sposób, w jaki organ nadzorczy dowiedział się

59 Decyzja Prezesa UODO nr ZSPR.440.43.2019, < https://uodo.gov.pl/decyzje/ZSPR.440.43.2019 >, dostęp: 14 lipca 2021 r.

60 Decyzja Prezesa UODO nr ZSPR.421.2.2019, < https://uodo.gov.pl/decyzje/ZSPR.421.2.2019 >, dostęp: 14 lipca 2021 r.

o naruszeniu – art. 83 ust. 2 lit. h) RODO[61]. Nie ulega przy tym wątpliwości, że wskazane wyżej przesłanki są ogólne i pozostawiają organowi nadzorczemu szeroką swobodę w zakresie ich uwzględnienia w konkretnym przypadku, przypisania im odpowiedniej wagi na potrzeby stosowanej administracyjnej kary pieniężnej, a w końcu ustalenia wysokości samej kary. Pozostawienie tak dużej swobody po stronie organu co do wymiaru kary pieniężnej budzi jednak wątpliwości. Krytycznie o systemie administracyjnych kar pieniężnych w RODO wypowiada się m.in. B. Sołtys. Wskazuje on w szczególności na nieprecyzyjność obowiązków sankcjonowanych karami pieniężnymi oraz ich nazbyt ocenny charakter. Podnosi także, że kary te są nadmiernie dotkliwe oraz łączą się ze zbyt szeroką swobodą orzekania po stronie organów wymierzających kary[62]. Należy podkreślić, iż wad tych nie koryguje dotychczasowe orzecznictwo sądów administracyjnych. Przykładowo WSA w Warszawie w wyroku z 28 lutego 2020 r., II SA/Wa 1511/19, uznał za niezasadny podniesiony w skardze zarzut, że organ nie sprecyzował, w jaki sposób określił wysokość administracyjnej kary pieniężnej np. poprzez wskazanie wyjściowej wysokości kary. Zdaniem sądu: „Przesłanki nałożenia administracyjnej kary pieniężnej określa bowiem art. 83 RODO. Wysokość nałożonej kary pieniężnej jest wypadkową uwzględnia przesłanek określonych w art. 83 ust. 2 i 3 RODO, w tym okoliczności, że (…) nie przetwarza danych osobowych w celach zarobkowych, nie prowadzi działalności gospodarczej oraz analizy rocznego sprawozdania finansowego za 2017 r.". Podobnie przyjął WSA w Warszawie w wyroku z 3 września 2020 r., II SA/Wa 2559/19: „Zarzut podniesiony w skardze, że organ nie sprecyzował, w jaki sposób określił wysokość administracyjnej kary pieniężnej, np. poprzez wskazanie wyjściowej wysokości kary, jest niezasadny. Przesłanki nałożenia administracyjnej kary pieniężnej określa bowiem art. 83 RODO. Wysokość nałożonej kary pieniężnej jest wypadkową przesłanek określonych w art. 83 ust. 2 i 3 RODO". Trafne jest oczywiście wskazanie przez sąd na wynikające z przepisów RODO przesłanki, które należy wziąć pod uwagę przy wymiarze kary pieniężnej. Problemem jest jednak to,

61 Zob. także pkt III wytycznych w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679.

62 B. Sołtys, *Wątpliwości*…, s. 42–29.

że przesłanki te (ich wypadkowa) nie pozwalają w najmniejszym nawet stopniu przewidzieć wysokości kary. Tym samym również kontrola sądowa w zakresie wysokości zastosowanej kary pieniężnej jest poważnie utrudniona. Zapewne trudno w tym zakresie oczekiwać rychłej zmiany RODO. Istotną pomocą mogłyby być tutaj wytyczne Europejskiej Rady Ochrony Danych (EROD) dotyczące m.in. określania wysokości administracyjnych kar pieniężnych – art. 70 ust. 1 pkt k) RODO. Niestety, przyjęte jeszcze przez Grupę Roboczą Art. 29 wytyczne z 2017 r. w niewielkim tylko stopniu prowadzą do większej harmonizacji w zakresie stosowania sankcji w całej UE oraz zwiększenia pewności prawnej w tym obszarze. Są one dokumentem nazbyt ogólnym i trudnym do operacjonalizacji.

Z praktyki orzeczniczej Prezesa UODO zdaje się wynikać, że naruszenia ochrony danych osobowych mają zwykle charakter nieumyślny i wynikają z niedochowania przez administratora należytej staranności w zakresie ochrony danych osobowych[63]. Zdarzą się jednak również sprawy, w których Prezes UODO stwierdza działania umyślne. Tak było w przypadku Głównego Geodety Kraju (GGK). W decyzji z 24 sierpnia 2020 r. Prezes UODO uznał, że GKK nie miał podstaw prawnych do pozyskiwania informacji z ewidencji gruntów i budynków (w tym numerów ksiąg wieczystych) prowadzonych przez starostów celem ich publikacji na GEOPORTAL2 (geoportal.gov.pl)[64]. Braku tego nie usunęły przy tym zawierane przez GGK ze starostami porozumienia. Dla uniknięcia wątpliwości zaznaczyć należy, że sprawa ta dotyczyła przetwarzania danych bez wymaganej podstawy prawnej – art. 5 ust. 1 lit. a) i art. 6 ust. 1 RODO, a nie wprost naruszenia ochrony danych osobowych. Może być jednak ilustracją szerszego problemu zawinienia w przypadku

63 Tak np. powołane wyżej decyzje Prezesa UODO w sprawie Dolnośląskiego Związku Piłki Nożnej, Morele.net sp. z o.o. oraz ENEA SA W niektórych przypadkach Prezes UODO dopatruje się po stronie administratora wręcz rażącego zaniedbania skutkującego naruszeniem poufności danych – zob. powołane wcześniej decyzje Prezesa UODO w sprawie ID Finance Poland Sp. z o.o. w likwidacji oraz w sprawie Krajowej Szkoły Sądownictwa i Prokuratury w Krakowie. W tym ostatnim przypadku, mimo zakwalifikowania danego naruszenia jako nieumyślnego, wysokość kary może być znaczna (w ww. sprawie ID Finance Poland była to kwota przekraczająca 1 mln złotych; w przypadku Krajowej Szkoły Sądownictwa i Prokuratury kara sięgnęła 100 000 zł, a więc maksymalnego pułapu kary dla tego rodzaju podmiotu).

64 Decyzja Prezesa UODO z 24 sierpnia 2020 r., nr DKN.5112.13.2020, w sprawie Głównego Geodety Kraju, < https://uodo.gov.pl/decyzje/DKN.5112.13.2020 >, dostęp: 14 lipca 2021 r.

deliktów administracyjnych na gruncie RODO. W decyzji wskazano, że GKK, decydując się na publikację na ww. portalu informacji o numerach ksiąg wieczystych: „zdawał sobie sprawę, że w ocenie organu nadzorczego numer księgi wieczystej podlega przepisom o ochronie danych osobowych i w związku z tym ich przetwarzanie powinno być zgodne z tymi przepisami. Z zaistniałych okoliczności niniejszej sprawy wynika bezspornie, że Główny Geodeta Kraju pomimo, że wiedział o stanowisku organu nadzorczego w tej sprawie zdecydował się wbrew temu stanowisku na publikację numerów ksiąg wieczystych na GEOPORTAL2". O przypisaniu umyślności po stronie GGK zdecydowało zatem działanie wyraźnie sprzeczne ze znanym GGK stanowiskiem Prezesa UODO, a więc z pełną świadomością bezprawności swego zachowania. Z podobną oceną umyślności działania administratora spotkać się można również w decyzji Prezesa UODO z 9 grudnia 2020 r. w sprawie TUiR WARTA SA[65] Organ nadzorczy uznał w niej, że spółka ta podjęła świadomą decyzję, by początkowo nie zawiadamiać o naruszeniu ochrony danych osobowych Prezesa UODO, jak i osób, których dane dotyczą. Uczyniła tak, mając nie tylko odpowiednie informacje o zdarzeniu, ale także znając treść kierowanych do niej pism Prezesa UODO, wskazujących na możliwość zaistnienia w niniejszej sprawie wysokiego ryzyka naruszenia praw lub wolności osób, których dotyczyło naruszenie[66]. Spółka już wcześniej dokonywała przy tym zgłoszeń podobnych naruszeń do Prezesa UODO, a zatem była świadoma ciążących na niej obowiązków. Wbrew literalnemu brzmieniu art. 83 ust. 2 lit. b) RODO, nakazującemu uwzględnienie w każdym indywidualnym przypadku umyślnego lub nieumyślnego charakteru naruszenia, kwestia umyślności bywa czasami pomijana w decyzjach Prezesa UODO nakładających kary pieniężne. Przykładem może być tu decyzja Prezesa UODO z 21 sierpnia 2020 r. w sprawie Szkoły Głównej Gospodarstwa Wiejskiego w Warszawie[67].

65 Decyzja nr DKN.5131.5.2020, < https://uodo.gov.pl/decyzje/DKN.5131.5.2020 >, dostęp: 14 lipca 2021 r.

66 Podobne okoliczności zdecydowały o zakwalifikowaniu naruszenia za umyślne w decyzji Prezesa UODO z 5 stycznia 2021 r. nr DKN.5131.6.2020 w sprawie Śląskiego Uniwersytetu Medycznego w Katowicach, < https://uodo.gov.pl/decyzje/DKN.5131.6.2020 >, dostęp: 14 lipca 2021 r.

67 Decyzja nr ZSOŚS.421.25.2019, < https://www.uodo.gov.pl/decyzje/ZSO%C5%9AS.421.25.2019 >, dostęp: 14 lipca 2021 r. Na obowiązek wskazania w uzasadnieniu decyzji kończącej

Zgodnie z art. 189g § 1 Kodeksu postępowania administracyjnego[68] administracyjna kara pieniężna nie może zostać nałożona, jeżeli upłynęło pięć lat od dnia naruszenia prawa albo wystąpienia skutków naruszenia prawa. Przepisu tego nie stosuje się do spraw, w przypadku których przepisy odrębne przewidują termin, po upływie którego nie można wszcząć postępowania w sprawie nałożenia administracyjnej kary pieniężnej lub stwierdzenia naruszenia prawa, w następstwie którego może być nałożona administracyjna kara pieniężna (art. 189g § 2 kpa). Zgodnie z art. 189g § 3 kpa administracyjna kara pieniężna nie podlega egzekucji, jeżeli upłynęło pięć lat od dnia, w którym kara powinna być wykonana.

Naruszenie ochrony danych osobowych skutkować może również odpowiedzialnością cywilnoprawną, wskutek podniesienia roszczeń z tego tytułu przez osoby, których dane dotyczą[69]. W aktualnym stanie prawnym brak jest już wątpliwości co do istnienia samodzielnej podstawy takich roszczeń, opartej tylko o naruszenie zasad przetwarzania danych osobowych (wątpliwości takie mogły występować wcześniej, szczególnie na gruncie wykładni przepisów o ochronie dóbr osobistych). Zgodnie z art. 79 ust. 1 RODO bez uszczerbku dla dostępnych administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa do wniesienia skargi do organu nadzorczego, każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna ona, że prawa przysługujące jej na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem niniejszego rozporządzenia. Z kolei, zgodnie z art. 82 ust. 1 RODO, każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia RODO, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę[70]. Zgodnie z ust. 2 tego przepisu każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem

postępowanie w sprawie przesłanek określonych w art. 83 ust. 2 RODO, na których Prezes UODO oparł się, nakładając administracyjną karę pieniężną oraz ustalając jej wysokość, wskazuje art. 72 ustawy o ochronie danych osobowych.

68 Ustawa z dn. 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, Dz.U. 2020, poz. 256, tekst jedn. ze zm. (dalej: kpa).

69 Szerzej: R. Strugała, *RODO*…, s. 914 i n.

70 Na temat pojęcia szkody na tle art. 82 RODO zob. A. Pązik, *Szkoda*…, s. 133–145.

naruszającym RODO. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które RODO nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom. W zasadzie niespornym w literaturze prawniczej jest, że odpowiedzialność odszkodowawcza w ramach art. 82 RODO ma charakter odpowiedzialności deliktowej[71]. W świetle polskiej wersji językowej RODO okolicznością wyłączającą odpowiedzialność odszkodowawczą ww. podmiotów ma być przy tym brak winy po ich stronie. Jak stanowi bowiem art. 82 ust. 3 RODO: „Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody"[72]. W literaturze wskazuje się jednak, że oparcie odpowiedzialności odszkodowawczej dotyczącej ochrony danych osobowych na przesłance winy w polskiej wersji RODO jest wynikiem błędu translatorskiego[73]. Inne wersje RODO do tej przesłanki się bowiem nie odwołują. Zwolnienie z odpowiedzialności byłoby zatem możliwie nie w przypadku udowodnienia braku winy za określone zdarzenie szkodzące, ale w przypadku udowodnienia, że dany podmiot nie ponosi odpowiedzialności za szkodę (niem. „wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist"; ang. „if it proves that it is not in any way responsible for the event giving rise to the damage")[74]. Odpowiedzialność odszkodowawcza administratora lub procesora miałaby zatem charakter odpowiedzialności obiektywnej, niezależnej od subiektywnie pojmowanej winy[75]. Stanowisko to uznać należy generalnie za trafne. Problemem może być jedynie to, że polska wersja językowa RODO może w tym zakresie rodzić po stronie jednostek określone oczekiwania co do kształtu ich odpowiedzialności

71 Szerzej: M. Gumularz, *Wpływ*…, s. 33–35.

72 Również motyw 146 RODO wskazuje m.in., że: „Administrator lub podmiot przetwarzający powinni jednak zostać zwolnieni z odpowiedzialności prawnej, jeżeli udowodnią, że szkoda w żadnym razie nie powstała z ich winy".

73 F. Morawski, *Odpowiedzialność*…, s. 85–87.

74 Zob. także: G. Zanfir-Fortuna, w: *The EU*…, s. 1176.

75 Uznaje się, że art. 82 ust. 1 RODO ustanawia domniemanie winy (*presumption of fault*) po stronie administratora i podmiotu przetwarzającego. Zob. E. Truli, *The General*…, s. 322–323.

z tytułu pełnionych funkcji administratora lub procesora. Może również odwodzić od lub utrudniać dochodzenie odszkodowania w sytuacjach, gdy sprawca deliktu (z powołaniem się na polską wersję RODO) wskazuje na rzekomą przesłankę egzoneracyjną w postaci brak winy po jego stronie. Wadliwe tłumaczenie RODO może zatem w praktyce obniżać poziom ochrony poszkodowanych, wymaga zatem pilnych zmian.

Jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający, lub uczestniczy w nim zarówno administrator, jak i podmiot przetwarzający, i zgodnie z art. 82 ust. 2 i 3 RODO odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania (art. 82 ust. 4 RODO). Administrator lub podmiot przetwarzający, który zgodnie z art. 82 ust. 4 RODO zapłacił odszkodowanie za całą wyrządzoną szkodę, ma prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność, zgodnie z warunkami określonymi w art. 82 ust. 2 (art. 82 ust. 5 RODO).

Zgodnie z art. 93 ustawy z dn. 10 maja 2018 r. o ochronie danych osobowych w sprawach o roszczenia z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i art. 82 RODO, właściwy jest sąd okręgowy.

Obowiązująca ustawa z dn. 10 maja 2018 r. o ochronie danych osobowych nie zawiera natomiast przepisu karnego penalizującego niezapobieżenie naruszeniu ochrony danych osobowych[76]. Ewentualna odpowiedzialność karna poszczególnych osób mających związek z takim naruszeniem uzależniona jest od konkretnych okoliczności faktycznych (np. możliwa jest odpowiedzialność osoby przełamującej zabezpieczenia w celu uzyskania dostępu do danych osobowych). Polska ustawa penalizuje jedynie[77] przetwarzanie danych w sytuacji, gdy jest to niedopuszczalne lub do którego dana osoba nie jest uprawniona (art. 107 ust. 1 ustawy

76 Por. także W. Mincewicz-Podrecka, *Prawnokarna*…, s. 96.

77 Szerzej: W. Mincewicz-Podrecka, *Prawnokarna*…; J. Łuczak-Tarka, w: *Ustawa*…; P. Fajgielski, *Ogólne*…, s. 884 i n.; M. Zimna, *Odpowiedzialność*…, s. 57 i n.; B. Sołtys, *Wątpliwości*…

z dn. 10 maja 2018 r. o ochronie danych osobowych oraz art. 107 ust. 2 tej ustawy w przypadku, gdy chodzi o szczególne kategorie ochrony danych osobowych, wymienione w art. 9 ust. 1 RODO)[78], a także udaremnianie lub utrudnianie kontrolującemu prowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych (art. 108 ust. 1 ww. ustawy). Penalizowane jest również niedostarczanie danych niezbędnych do określenia podstawy administracyjnej kary pieniężnej lub dostarczanie danych, które uniemożliwiają ustalenie takiej podstawy, w związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej (art. 108 ust. 2 ww. ustawy).

6. Zakończenie

Ogólne rozporządzenie o ochronie danych przyjmuje szerokie ujęcie naruszenia ochrony danych osobowych. Mieszczą się w nim wszelkiego rodzaju incydenty ingerujące w bezpieczeństwo danych i wywołujące równocześnie określone w przepisach skutki w postaci naruszenia integralności lub poufności danych. Dla kwalifikacji danego zdarzenia jako ww. naruszenia bez znaczenia są kwestie winy lub jej braku po stronie administratora lub podmiotu przetwarzającego. Decydujące jest obiektywne wystąpienie naruszenia, a nie np. przyczyny takiego zdarzenia (zewnętrzne lub wewnętrzne względem administratora lub podmiotu przetwarzającego), zamiar lub stopień staranności, który przejawiał administrator lub podmiot przetwarzający. Ujęcie to sprzyja zapewnieniu właściwej ochrony praw jednostek dotkniętych danym incydentem.

Jednostka ma w szczególności prawo do adekwatnej, zarówno pod względem formy, jak i treści, informacji o zdarzeniu, które może powodować wysokie ryzyko naruszenia jej praw lub wolności. Umożliwia to jej nie tylko podjęcie własnych działań zaradczych chroniących

78 Art. 107. 1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch. 2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.

przed skutkami zaistniałego incydentu, ale także łatwiejsze wniesienie powództwa o odszkodowanie zarówno za szkodę majątkową, jak i niemajątkową. Polska wersja językowa RODO powinna przy tym, zgodnie z innymi wersjami językowymi, wyraźnie odwoływać się w tym zakresie do odpowiedzialności o charakterze obiektywnym, niezależnej od winy po stronie naruszyciela.

Skuteczność przepisów RODO dotyczących naruszenia ochrony danych osobowych ulega istotnemu wzmocnieniu również dzięki przekazaniu przez prawodawcę w ręce organu nadzorczego uprawnień naprawczych, a przede wszystkim możliwości zastosowaniu różnego rodzaju nakazów określonego zachowania oraz administracyjnych kar pieniężnych. Określona przepisami RODO i polskiej ustawy o ochronie danych osobowych maksymalna wysokość tych kar wydaje się generalnie adekwatna do powagi deliktów dotyczących danych osobowych. Wątpliwości z punktu widzenia zasady pewności prawa i ochrony praw przedsiębiorców budzi jednak szeroki zakres swobody po stronie organu co do wymiaru kary pieniężnej w poszczególnych przypadkach. W tej sytuacji sądy rozpatrujące środki odwoławcze w tego rodzaju sprawach powinny stawiać organowi nadzorczemu wysokie wymagania co do uzasadnienia zarówno samej konieczności zastosowania kary pieniężnej *ad casum*, jak i jej wysokości. Umożliwi to rzeczywistą, a nie tylko formalną kontrolę sądową działań organu nadzorczego.

Aprobująco odnieść należy się do rezygnacji ustawodawcy z zamieszczania w ustawie o ochronie danych osobowych szczególnych przepisów karnych dotyczących naruszenia ochrony takich danych. Prawo karne powinno być środkiem *ultima ratio*. Winno ono wkraczać wyłącznie w te obszary, dla których regulacje innych dziedzin prawa są niewystarczające. W analizowanym przypadku sytuacja taka nie ma miejsca. Wynika to w szczególności z wprowadzonych przepisami RODO sankcji administracyjnych. Jednocześnie pamiętać należy o rozdziale XXXIII Kodeksu karnego – „Przestępstwa przeciwko ochronie informacji". W przepisach tego rozdziału spenalizowano szereg typów czynów zabronionych, często towarzyszących naruszeniu ochrony danych, np. bezprawne uzyskanie informacji (por. przepisy art. 267 kk), czy udaremnienie lub utrudnianie zapoznania się z informacją (por. przepisy art. 268 kk). Przepisy te

zapewniają dodatkową ochronę osobom, których dane dotyczą. Opisane w nich występki są przy tym w istotnej części ścigane na wniosek pokrzywdzonego, co należy ocenić pozytywnie, jako że to właśnie osoba, której dane dotyczą, winna być inicjatorem ewentualnego postępowania karnego. To ona bowiem jest głównym beneficjentem ochrony i gwarancji zawartych w przepisach prawa ochrony danych osobowych.

Personal Data Breach. Legal Issues

The subject of this article is the issue of personal data breach, primarily in the context of the provisions of the General Data Protection Regulation (2016/679). The aim of the publication is, in particular, to answer the following questions: do the regulations properly protect the rights of an individual in the event of a breach? do the sanctions and liability rules provided for by these regulations are adequate to the threats? do the sanctions and liability rules respect the requirements of the rule of law? The authors analyze the concept of a personal data breach in detail, including the magnitude of consequences necessary to determine occurrence of a security breach. The article also extensively analyzes the consequences of such breach for entities responsible for personal data processing (organizational effects, documentation and reporting obligations, liability for damages, administrative fines). Particular attention is paid to the decisions of the Polish President of the Personal Data Protection Office regarding violations and the jurisprudence of administrative courts in these types of cases. In conclusion, an assessment is made of the principles of personal data protection against breaches introduced in the General Data Protection Regulation. While approving the generally introduced legal solutions, doubts related to the excessively broad scope of discretion on the part of the authority as to the amount of fines in individual cases are indicated.

Keywords: General Data Protection Regulation, personal data breach, consequences of a data breach, administrative fines

Jacek Błachut – doktor, adwokat.

Sławomir Dudzik – profesor doktor habilitowany, kierownik Katedry Prawa Europejskiego Uniwersytetu Jagiellońskiego, numer ORCID: 0000–0001–7726–8978.

Bibliografia

Abu Gholeh M., Kuźnicka-Błaszkowska D., *Nakładanie administracyjnych kar pieniężnych w rozporządzeniu o ochronie danych osobowych. Aspekty praktyczne*, Warszawa 2020.

Abu Gholeh M., *Pozycja ustrojowa organu nadzorczego ochrony danych osobowych na przykładzie Polski*, „Przegląd Prawa Konstytucyjnego" 2019, nr 4 (50).

Bevitt A., Carey P., *Data Security and Breach Notifications*, w: *Data Protection A Practical Guide to UK and EU Law*, red. P. Carey, Oxford 2018.

Błachut J., Dudzik S., Olczyk D., *Ochrona danych osobowych pracownika w warunkach epidemii (wybrane zagadnienia)*, „Europejski Przegląd Sądowy" 2020, nr 5.

Burton C., w: *The EU General Data Protection Regulation (GDPR). A Commentary*, red. Ch. Kuner, L.A. Bygrave, Ch. Docksey, Oxford 2020.

Chomiczewski W., w: *RODO. Ogólne rozporządzenia o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.

Fajgielski P., *Informowanie o naruszeniu ochrony danych osobowych w świetle przepisów ogólnego rozporządzenia o ochronie danych*, „Monitor Prawniczy" (dodatek) 2016, nr 20.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Fajgielski P., *Prawo ochrony danych osobowych. Zarys wykładu*, Warszawa 2019.

Florczak-Wątor M., w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Tuleja, Warszawa 2019.

Gumularz M., *Wpływ regulacji odpowiedzialności odszkodowawczej w ogólnym rozporządzeniu o ochronie danych osobowych na systemy prawa prywatnego państw członkowskich*, „Europejski Przegląd Sądowy" 2017, nr 5.

Kotschy W., w: *The EU General Data Protection Regulation (GDPR). A Commentary*, red. Ch. Kuner, L.A. Bygrave, Ch. Docksey, Oxford 2020.

Lach A., w: *Kodeks karny. Komentarz*, red. V. Konarska-Wrzosek, Warszawa 2016.

Łakomiec K., *Konstytucyjna ochrona prywatności. Dane dotyczące zdrowia*, Warszawa 2020.

Łuczak J., w: *RODO. Ogólne rozporządzenia o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.

Łuczak-Tarka J., w: *Ustawa o ochronie danych osobowych. Komentarz*, red. D. Lubasz, LEX/el. 2019.

Mincewicz-Podrecka W., *Prawnokarna odpowiedzialność administratorów*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2020, nr 1.
Morawski F., *Odpowiedzialność cywilna administratora danych osobowych i podmiotu przetwarzającego według ogólnego rozporządzenia o ochronie danych osobowych*, „Acta Iuris Stetinensis" 2019, nr 2 (26).
Nerka A., w: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018.
Pązik A., *Szkoda wynikająca z naruszenia przepisów RODO. Wybrane problemy*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej" 2020, nr 3.
Razowski T., w: *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, LEX 2014.
Sharma S., *Data Privacy and GDPR Handbook*, Hoboken, New Jersey 2020.
Sławińska A., *Odpowiedzialność administratora w przypadku naruszenia ochrony danych osobowych*, „Wojskowy Przegląd Prawniczy" 2020, nr 3.
Soczyński T., *Zgłaszanie naruszeń ochrony danych – nowy obowiązek administratorów danych*, „Monitor Prawniczy" (dodatek) 2017, nr 20.
Sołtys B., *Wątpliwości wokół konstytucyjności sankcji karnych i administracyjno-karnych za naruszenie przepisów o ochronie danych osobowych*, „Przegląd Sejmowy" 2019, nr 5.
Strugała R., *RODO a odpowiedzialność odszkodowawcza. Podstawowe problemy odpowiedzialności za szkodę spowodowaną nieprawidłowym przetwarzaniem danych osobowych*, „Monitor Prawniczy" 2018, nr 17.
Tosoni L., w: *The EU General Data Protection Regulation (GDPR). A Commentary*, red. Ch. Kuner, L.A. Bygrave, Ch. Docksey, Oxford 2020.
Truli E., *The General Data Protection Regulation and Civil Liability*, w: *Personal Data in Competition, Consumer Protection and Intellectual Property Law Towards a Holistic Approach?*, red. M. Bakhoum, B. Conde Gallego, M.-O. Mackenrodt, G. Surblytė-Namavičienė, Springer 2018.
Voigt P., von dem Bussche A., *The EU General Data Protection Regulation (GDPR). A Practical Guide*, Springer 2017.
Wróbel W., Zając D., w: *Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. 212–277d*, red. W. Wróbel, A. Zoll, LEX 2017.
Zanfir-Fortuna G., w: *The EU General Data Protection Regulation (GDPR). A Commentary*, red. Ch. Kuner, L.A. Bygrave, Ch. Docksey, Oxford 2020.
Zimna M., *Odpowiedzialność karna za naruszenie ochrony danych osobowych*, „Prokuratura i Prawo" 2020, nr 1.