Pierwsza administracyjna kara pieniężna nałożona na podmiot z sektora publicznego

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie
z dnia 26 sierpnia 2020 r., II SA/Wa 2826/19

1. **Czynności o charakterze techniczno-organizacyjnym leżą w gestii administratora danych osobowych, ale nie mogą być dobierane w sposób całkowicie swobodny i dobrowolny, bez uwzględnienia stopnia ryzyka czy charakteru chronionych danych osobowych. Bez wątpienia środki podejmowane przez skarżącego nie zapewniły bezpieczeństwa, co należycie wykazał organ (…).**
2. **(…) Prawidłowo organ ocenił naruszenie art. 5 ust. 1 lit. e w związku z art. 5 ust. 2, tj. zasady ograniczenia przechowywania oraz art. 24 rozporządzenia 2016/679 poprzez brak odpowiednich polityk, dotyczących przetwarzania danych osobowych w BIP Urzędu Miejskiego w A. pod kątem ich aktualności i celowości publikacji oraz określających terminy usunięcia danych osobowych. Zasada określona mianem „ograniczenia przechowywania", określona w art. 5 ust 1 lit. 3 rozporządzenia 2016/679 stanowi, iż „dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane". Nadto „dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania"). Zgodnie z tą zasadą, po osiągnięciu celów, w jakich przetwarzane są dane osobowe, powinny zostać one usunięte albo skasowane.**

Marlena Sakowska-Baryła
m.sakowskabaryla@kancelariasbc.pl
Uczelnia Łazarskiego
ORCID: 0000-0002-3982-976X

https://doi.org/10.26881/gsp.2021.4.10

Wojewódzki Sąd Administracyjny w Warszawie wyrokiem z dnia 26 sierpnia 2020 r., II SA/Wa 2826/19[1] oddalił skargę Burmistrza Aleksandrowa Kujawskiego na decyzję Prezesa Urzędu Ochrony Danych Osobowych z dnia 18 października 2019 r., ZSPU.421.3.2019, w której organ nadzorczy, stwierdzając szereg naruszeń przepisów RODO[2], obok zastosowania uprawnień naprawczych zastosował administracyjną karę pieniężną w kwocie 40.000 zł. Wskazaną decyzję uznać należy za istotną nie tylko z tego względu, że jest ona pierwszą w Polsce decyzją Prezesa Urzędu Ochrony Danych Osobowych (Prezes UODO), nakładającą administracyjną karę pieniężną w sektorze publicznym. To bowiem jednocześnie decyzja, która odnosi się do kwestii zastosowania przepisów RODO do przetwarzania danych osobowych, jakie ma miejsce przy realizacji prawa dostępu do informacji publicznej, a także dobrze obrazuje kilka innych zagadnień doniosłych przy organizacji systemu ochrony danych osobowych w sektorze publicznym, które wcześniej nie zawsze były postrzegane jako pierwszoplanowe.

W wyroku w sprawie II SA/Wa 2826/19 WSA w Warszawie w pełni podzielił argumentację Prezesa UODO, dlatego też w niniejszej glosie nie sposób obyć się bez sięgania po ustalenia zawarte w tej decyzji. Choć w chwili złożenia tekstu do publikacji przedmiotowy wyrok nie jest prawomocny, to jednak ze względu na istotne wątki podejmowane w sprawie, warto przyjrzeć się ustaleniom dokonanym przez WSA w Warszawie oraz przez organ nadzorczy na kanwie stanu faktycznego, który w znacznej mierze odnosi się do pewnych specyficznych dla sektora publicznego operacji przetwarzania danych osobowych oraz uwarunkowań techniczno-organizacyjnych, które należą do kluczowych dla podmiotów z sektora publicznego.

Stan faktyczny

Jak wynika z analizowanego uzasadnienia wyroku WSA w Warszawie, wydanie decyzji przez Prezesa UODO było poprzedzone kontrolą tego organu, którą objęty został sposób przetwarzania danych osobowych przez Burmistrza Aleksandrowa Kujawskiego (Burmistrz) w ramach procesu wysyłki korespondencji i prowadzenia Biuletynu Informacji Publicznej (BIP), a także sposób prowadzenia rejestru czynności przetwarzania oraz dokumentowania naruszeń ochrony danych osobowych. Na podstawie zgromadzonego materiału dowodowego ustalono, że w procesie przetwarzania danych osobowych Burmistrz, jako administrator, naruszył przepisy o ochronie danych osobowych, w związku z czym Prezes UODO wszczął w tym przedmiocie postępowanie administracyjne zakończone wspomnianą we wstępie decyzją, w której Prezes UODO stwierdził naruszenie przez Burmistrza przepisów:

[1] Wyrok WSA w Warszawie z dnia 26 sierpnia 2020 r., II SA/Wa 2826/19, LEX nr 3067899.

[2] 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. Urz. UE L 119, s. 1 ze zm.; dalej: RODO).

1) art. 5 ust. 1 lit. a oraz lit. f w zw. z art. 5 ust. 2 RODO, tj. zasady zgodności z prawem i zasady poufności oraz art. 28 ust. 3 rozporządzenia 2016/679, poprzez udostępnianie danych osobowych na rzecz kilku zewnętrznych podmiotów bez podstawy prawnej, tj. bez uprzedniego zawarcia z ww. podmiotami umów powierzenia danych osobowych, o której mowa w art. 28 ust. 3 rozporządzenia 2016/679, w związku z prowadzeniem strony internetowej BIP Urzędu Miejskiego w Aleksandrowie Kujawskim;
2) art. 5 ust. 1 lit. e w związku z art. 5 ust. 2, tj. zasady ograniczenia przechowywania oraz art. 24 RODO poprzez brak odpowiednich polityk dotyczących przetwarzania danych osobowych w BIP Urzędu Miejskiego w Aleksandrowie Kujawskim pod kątem ich aktualności i celowości publikacji oraz określających terminy usunięcia danych osobowych;
3) art. 5 ust. 1 lit. f w związku z art. 5 ust. 2 RODO, tj. zasady integralności i poufności, zasady prawidłowości, oraz art. 24 RODO poprzez nieprzeprowadzenie analizy ryzyka związanego z korzystaniem przez Burmistrza z kanału YouTube w celu transmisji nagrań z obrad Rady Miasta Aleksandrowa Kujawskiego;
4) art. 5 ust. 1 lit. f w związku z art. 5 ust. 2 RODO, tj. zasady integralności i poufności, oraz art. 32 RODO poprzez niewdrożenie odpowiednich środków technicznych i organizacyjnych mających na celu zabezpieczenie danych osób fizycznych w związku z przechowywaniem nagrań sesji Rady Miasta wyłącznie na serwerach YouTube, bez wykonywania i przechowywania kopii zapasowych tych nagrań w zasobach własnych Urzędu Miejskiego w Aleksandrowa Kujawskiego;
5) art. 5 ust. 2 RODO, tj. zasady rozliczalności oraz art. 30 ust. 1 lit. d oraz lit. f RODO, poprzez niewskazanie w rejestrze czynności przetwarzania danych osobowych, dla czynności związanych z publikacją informacji na stronie BIP Urzędu Miasta w Aleksandrowie Kujawskim, wszystkich odbiorców danych oraz niewskazanie dla tych czynności przetwarzania planowanego terminu usunięcia danych w sposób zapewniający przetwarzanie danych zgodnie z zasadą ograniczonego przechowywania.

W związku z tak scharakteryzowanymi naruszeniami Prezes UODO nakazał Burmistrzowi dostosowanie operacji przetwarzania danych osobowych do przepisów RODO, w terminie 60 dni od dnia, w którym przedmiotowa decyzja stanie się ostateczna, poprzez:

1) zaprzestanie udostępniania danych osobowych na rzecz zewnętrznych podmiotów, bez podstawy prawnej, tj. bez uprzedniego zawarcia umów powierzenia danych osobowych z ww. podmiotami, o której mowa w art. 28 ust. 3 rozporządzenia 2016/679, w związku z prowadzeniem strony internetowej BIP Urzędu Miejskiego w Aleksandrowie Kujawskim;
2) wdrożenie polityk:
   a) określających okresy przetwarzania danych w BIP Urzędu Miejskiego w Aleksandrowie Kujawskim zgodne z przepisami prawa lub niezbędne do realizacji celów, dla których dane są przetwarzane;
   b) zapewniających przestrzeganie terminów usuwania danych;

3) przeprowadzenie analizy ryzyka w związku z publikacją nagrań sesji rady miejskiej i wdrożenie odpowiednich środków organizacyjnych i technicznych w związku z przetwarzaniem danych osobowych na kanale YouTube w związku z transmisją nagrań sesji rady miejskiej oraz przechowywaniem nagrań na serwerach YouTube;
4) wdrożenie odpowiednich środków organizacyjnych i technicznych mających na celu zabezpieczenie danych osób fizycznych pochodzących z nagrań sesji Rady Miasta Aleksandrowa Kujawskiego poprzez zapewnienie dostępności kopii zapasowych w zasobach własnych Urzędu Miejskiego w Aleksandrowie Kujawskim;
5) ujęcie w rejestrze czynności przetwarzania danych osobowych, dla czynności przetwarzania związanych z prowadzeniem BIP, informacji o:
   a) wszystkich odbiorcach danych, którym dane zostały lub zostaną ujawnione, zgodnie z art. 30 ust. 1 lit. d RODO;
   b) planowanych terminach usunięcia danych, zgodnie z art. 30 ust. 1 lit. f RODO.

Ponadto, za naruszenie przepisów art. 5 ust. 1 lit. a, e oraz lit. f, art. 5 ust. 2, art. 28, art. 30 ust. 1 lit. d oraz lit. f, a także art. 32 RODO, Prezes UODO nałożył na Burmistrza karę pieniężną w kwocie 40.000 zł.

Ponieważ, kwestionując decyzję Prezesa UODO, Burmistrz podniósł zarzut naruszenia przy jej wydaniu prawa materialnego, w tym art. 2 ust. 2 lit. a RODO, przez jego niewłaściwe zastosowanie w związku z art. 1 ust. 1 w związku z art. 168 u.o.d.o.[3], co doprowadziło do wydania zaskarżonej decyzji stwierdzającej naruszenie art. 5, WSA w Warszawie argumentację tę uznał za całkowicie nietrafną i wskazał, że wyłączenia, określone w art. 2 ust. 2 lit. a RODO, jako mające charakter wyjątkowy, nie mają zastosowania w analizowanej tu sprawie. Sąd odniósł się zatem do poszczególnych zarzutów dotyczących uchybień w procesie przetwarzania.

Każde z przywołanych ustaleń zasługuje na odnotowanie i refleksję, ponieważ dotyczy organizacji systemu ochrony danych osobowych w procesie współstosowania przepisów RODO z przepisami ustawy o dostępie do informacji publicznej[4], a nadto dotyka specyfiki stosowania RODO w sektorze publicznym, potwierdzając tezę, że nie w każdym przypadku procedury kształtowane w tym zakresie przez ten akt i przepisy krajowe są spójne.

Dostęp do informacji publicznej a zakres zastosowania przepisów RODO

U podstaw analizowanego wyroku WSA w Warszawie oraz poprzedzającej ten wyrok decyzji Prezesa UODO legło generalne założenie, wedle którego przepisy RODO mają zastosowanie w przypadku przetwarzania danych osobowych, jakie ma miejsce przy realizacji prawa dostępu do informacji publicznej. Tym samym, WSA w Warszawie nie

[3] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2019 r. poz. 1781; dalej: u.o.d.o.).

[4] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (tekst jedn.: Dz. U. z 2020 r., poz. 2176 ze zm.; dalej: u.d.i.p., ustawa o dostępie do informacji publicznej).

podzielił zapatrywania, że przetwarzanie danych osobowych na potrzeby dostępu do informacji publicznej nie jest objęte zakresem zastosowania przepisów RODO, co było podstawowym zarzutem wysuwanym przez stronę skarżącą, która oparcia dla tego zarzutu poszukiwała w treści art. 2 ust. 2 lit. a RODO, zgodnie z którym rozporządzenie to nie ma zastosowania do przetwarzania danych osobowych w ramach działalności nieobjętej zakresem prawa UE. Strona skarżąca starała się zatem wykazać, że zasady dostępu do informacji publicznej są przykładem działalności nieobjętej prawem Unii Europejskiej, co powoduje, że w tym zakresie przepisy RODO nie znajdują zastosowania. Tak postawiona teza odzwierciedla jedno z dwóch przeciwstawnych stanowisk, jakie rysują się w tym względzie w polskiej nauce prawa.

W literaturze wyraża się bowiem zarówno takie stanowisko, którego argumentacja przebiega zgodnie z zapatrywaniami wyrażanymi przez stronę skarżącą w analizowanej sprawie[5], jak i odmienne – przyjmowane przez sąd i organ nadzorczy w przedmiotowej sprawie, wedle którego RODO ma zastosowanie do przetwarzania danych osobowych, jakie odbywa się przy realizacji dostępu do informacji publicznej[6]. Dotyczy to przy tym zarówno ujawniania danych osobowych zawartych w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym – do czego wprost odnosi się art. 86 RODO, jak i przetwarzania danych osobowych, które w tym obszarze ma charakter akcesoryjny, a więc odbywa się w związku z obsługą procesów zapewniania dostępu do informacji publicznej w trybach i formach określonych w ustawie o dostępie do informacji publicznej[7].

Argumentując za zastosowaniem RODO do przetwarzania danych osobowych przy realizacji dostępu do informacji publicznej, WSA w Warszawie wskazał, że art. 2 RODO wyznacza materialny zakres jego stosowania, zaś wykładnia wyłączenia wynikającego z art. 2 ust. 2 lit. a tego aktu musi zostać dokonana z uwzględnieniem wykładni systemowej i celowościowej, co prowadzi do wniosku, że intencją prawodawcy unijnego nie było zawężenie stosowania ochrony danych osobowych, a wręcz przeciwnie – zwiększenie jej zakresu i stosowania, zaś sposób interpretacji przyjęty przez skarżącego spowodowałoby, że dane osobowe właściwie nie podlegałyby ochronie.

---

[5] Zob. P. Barta, P. Litwiński, *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021, s. 607–609; WSA w Olsztynie w wyroku z dnia 19 października 2018 r., II SA/Ol 542/18, CBOSA, wskazał, że przepisy RODO nie znajdują zastosowania do udostępniania danych osobowych w ramach dostępu do informacji publicznej, ale bez wskazania szerszego uzasadnienia tak postawionej tezy.

[6] Zob. G. Sibiga, I. Małobęcka-Szwast, *Relacje prawa do informacji publicznej oraz prawa do ochrony danych osobowych w świetle ogólnego rozporządzenia o ochronie danych (RODO)* [w:] *Polskie przepisy o ochronie danych osobowych. Aktualne problemy prawnej ochrony danych 2019*, red. G. Sibiga, M. Praw. 2019, nr 22 – dodatek, s. 61–66; M. Jabłoński, *Rola i znaczenie RODO w procesie definiowania gwarancji niezależności i spójności krajowego systemu ochrony danych osobowych* [w:] M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda, *Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym*, Wrocław 2017; M. Sakowska-Baryła, komentarz do art. 86 [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. *eadem*, Warszawa 2018, s. 611–612.

[7] Zob. M. Sakowska-Baryła, komentarz do art. 86 [w:] *Ogólne rozporządzenie*…, s. 612.

Sąd podniósł, że ustawodawca konkretyzuje wyłączenia stosowania przepisów w art. 6 RODO, a przeciwna wykładnia przepisów – w sposób przyjęty przez skarżącego – prowadziłaby do interpretacji *ad absurdum*, gdzie zastosowanie przepisów RODO ograniczone byłoby do bardzo wąskiego zakresu obowiązywania prawa Unii Europejskiej. Tymczasem – jak wskazuje WSA w Warszawie – wprowadzenie RODO miało na celu zwiększenie, a nie drastyczne ograniczenie ochrony danych osobowych. Jednocześnie argumentów na rzecz stosowania przepisów RODO do przetwarzania danych osobowych przy zapewnianiu dostępu do informacji publicznej, WSA poszukuje w treści art. 8 ust. 1 Karty praw podstawowych UE[8], zgodnie z którym każdy ma prawo do ochrony danych osobowych, które go dotyczą, oraz w art. 16 ust. 1 TFUE[9] stanowiącym, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących, jak również w przepisach Konstytucji RP[10], wskazując na zakładaną przez te akty „szeroką ochronę danych osobowych".

W ślad za wywodem organu nadzorczego, WSA w Warszawie przyjął, że norma wynikająca z art. 16 ust. 1 TFUE (oraz analogiczna z art. 8 Karty Praw Podstawowych UE), ma status normy bezpośrednio skutecznej, stając się autonomiczną podstawą uprawnień osób fizycznych w zakresie ochrony danych osobowych. Bezpośrednio skuteczna norma traktatowa chroni osoby fizyczne również w sytuacjach, kiedy nie będą one mogły korzystać z ochrony gwarantowanej przez akty prawa wtórnego. Treść art. 16 ust. 2 TFUE jednoznacznie wskazuje, że zasady ochrony danych osobowych określone w treści aktów prawa wtórnego będą miały zastosowanie w odniesieniu do danych osobowych osób fizycznych przetwarzanych przez instytucje, organy, jednostki organizacyjne Unii Europejskiej oraz państwa członkowskie, ale jedynie w zakresie, w jakim działania te będą służyć stosowaniu prawa Unii Europejskiej.

Choć tak wyrażone stanowisko zasadniczo zasługuje na aprobatę, to jednak sposób argumentacji przyjęty przez WSA może wzbudzać pewien niedosyt, ponieważ – przywołując przepisy UE oraz powołując się na względy słuszności – sąd ten wyczerpująco nie wyjaśnia, co przemawia za tym, by nie podzielić stanowiska strony skarżącej. Znacznie bardziej pogłębionych analiz w tym względzie dokonali Grzegorz Sibiga i Iga Małobęcka-Szwast, wychodząc od założenia, że udostępnianie danych osobowych w dokumentach urzędowych podlega przepisom RODO jako szczególna kategoria przetwarzania, o której mowa w jego rozdziale IX – Przepisy dotyczące szczególnych sytuacji związanych z przetwarzaniem, w art. 86, pomimo tego, że prawo unijne nie reguluje wprost dostępu do informacji publicznej w państwach członkowskich. Jednak w przypadku gdy ujawnieniu w ramach krajowych systemów dostępu do informacji publicznej podlegają dane osobowe, to RODO znajduje zastosowanie przez wzgląd

[8] Karta praw podstawowych Unii Europejskiej (Dz. Urz. UE C 303 z 2007 r., s. 1 ze zm.).

[9] Traktat ustanawiający Europejską Wspólnotę Gospodarczą (Dz. U. z 2004 r. Nr 90, poz. 864/2 ze zm.) zmieniony przez art. G lit. A pkt 1 Traktatu o Unii Europejskiej (Dz.U.04.90.864/30) w związku z przystąpieniem Polski do Unii Europejskiej; zmieniony przez art. 2 pkt 1 Traktatu z Lizbony zmieniającego Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską (Dz.U.UE.C.07.306.1) z dniem 1 grudnia 2009 r.

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

na kilka przesłanek uzasadniających zajęcie takiego właśnie stanowiska[11]. Autorzy ci słusznie wskazują, że w zakresie, w jakim w ramach dostępu do informacji publicznej dochodzi do ujawnienia danych osobowych, ma miejsce również przetwarzanie danych osobowych i ingerencja w prawo do ochrony danych osobowych, a co za tym idzie – ma się tu do czynienia z ingerencją w prawo podstawowe, gwarantowane każdemu w art. 16 TFUE oraz art. 8 KPP. Stąd w tym wąskim zakresie, w jakim dochodzi do ujawnienia danych osobowych, krajowy system dostępu do informacji publicznej odzwierciedlony w Polsce głównie w przepisach u.d.i.p. podlega prawu unijnemu, które chroni prawo podstawowe do ochrony danych osobowych, a gwarancje ochrony tego prawa uszczegóławia RODO. Taka konkluzja pozostaje uzasadniona ze względu na brzmienie art. 86 i wskazany wyżej tytuł rozdziału IX RODO, w którym ów przepis się znajduje. W ten sposób prawo oddziałuje zatem na tę część krajowego systemu dostępu do informacji publicznej, w której dochodzi do ujawnienia danych osobowych, a więc kolizji między ochroną danych osobowych a dostępem do informacji publicznej i RODO i znajduje zastosowanie w tego rodzaju sprawach właśnie z tego względu, że w ramach dostępu do informacji publicznej może dochodzić do ingerencji w prawo do ochrony danych osobowych[12]. Tezę o zastosowaniu RODO do ujawniania danych osobowych zawartych w „dokumentach urzędowych" potwierdzają również te przepisy RODO, które odwołują się wprost do rozdziału IX. Ma to miejsce w treści art. 6 ust. 2 i 3, a także w art. 83 ust. 5 lit. d RODO, przez co prawodawca unijny wprost ustanawia wymagania względem podstaw prawnych przetwarzania danych osobowych w sytuacjach związanych z przetwarzaniem, takich jak udostępnianie danych osobowych w dokumentach urzędowych, o którym mowa w art. 86 RODO. Nadto, na tle analizowanego wyroku istotna jest właśnie regulacja zawarta w art. 83 ust. 5 lit. d RODO, który przewiduje możliwość nałożenia przez organ nadzorczy administracyjnej kary pieniężnej w przypadku naruszenia wszelkich obowiązków wynikających z prawa państwa członkowskiego przyjętego na podstawie rozdziału IX, w tym art. 86 RODO. Stąd naruszenie obowiązków wynikających z prawa krajowego, przyjętych na podstawie art. 86 RODO, może pociągnąć za sobą odpowiedzialność w postaci nałożenia na administratora przez organ nadzorczy administracyjnej kary pieniężnej[13].

Argumentów na rzecz dopuszczalności stosowania RODO do przetwarzania danych osobowych przy dostępie do informacji publicznej doszukiwać się można także w bliskim powiązaniu systemu dostępu i ponownego wykorzystywania informacji sektora publicznego, które z założenia jest oparte właśnie na systemie dostępu do informacji publicznej. Choć prawo unijne nie zawiera kompleksowej regulacji dotyczącej dostępu do informacji publicznej, to poprzednio w dyrektywie 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego[14], zaś obecnie w dyrektywie Parlamentu Euro-

[11] Zob. G. Sibiga, I. Małobęcka-Szwast, *Relacje*…, s. 63.
[12] *Ibidem*, s. 64.
[13] *Ibidem*.
[14] Dz. Urz. UE L 345, s. 90 ze zm.

pejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (wersja przekształcona)[15] dookreśla się zasady takiego dostępu w sprawie ponownego wykorzystywania informacji sektora publicznego.

Zarówno w RODO, jak i w powyższych dyrektywach wskazuje się, że dostęp do informacji publicznej i ponowne wykorzystanie informacji sektora publicznego tworzą razem nierozerwalną całość, a ponowne wykorzystanie informacji sektora publicznego nie mogłoby istnieć bez krajowych systemów dostępu do dokumentów urzędowych. W RODO zatem oba te reżimy względem prawa do ochrony danych osobowych potraktowane są łącznie, co powoduje, że przepisy regulujące publiczny dostęp do dokumentów urzędowych oraz ponowne wykorzystanie informacji sektora publicznego mają przewidywać niezbędne uwzględnienie prawa do ochrony danych osobowych na podstawie RODO, co – siłą rzeczy – odbywa się poprzez uwzględnianie zasad wynikających z tego rozporządzenia przy wykonywaniu obu tych praw dostępowych. Powyższe argumenty można zestawić również z orzecznictwem TSUE dotyczącym zakresu zastosowania Karty Praw Podstawowych, z którego wynika m.in., że choć dana działalność nie wiąże się z wykonywaniem i nie narusza norm prawa UE, może ona mieścić się „w zakresie prawa UE", ponieważ istnieje wystarczający związek („łącznik") między aktem prawa krajowego a aktem prawa unijnego[16].

Przywołana argumentacja zdaje się potwierdzać słuszność przyjęcia przez WSA w Warszawie, że w analizowanej sprawie nie zachodzi wyłączenie stosowania RODO, o jakim mowa w art. 2 ust. 2 lit. a RODO, choć jednocześnie – dla uzupełnienia tychże ustaleń – wskazać należy, że wypełniając zapowiedź z art. 86 RODO, państwa członkowskie powinny stworzyć szczególne regulacje w zakresie dostępu i ujawniania dokumentów urzędowych, spełniające wytyczne zawarte w art. 6 ust. 2 i 3 RODO, a wcześniejsze normy regulujące dostęp do dokumentów urzędowych i ich ujawnianie mogą nadal obowiązywać, pod warunkiem że wypełniają wymogi określone w tychże przepisach[17]. Biorąc pod uwagę treść art. 5 ust. 2 u.d.i.p., w którym mowa wyłącznie o prywatności osoby fizycznej jako przesłance ograniczenia dostępu do informacji publicznej oraz fakt, że w rzeczonej ustawie w ogóle nie posłużono się taką kategorią pojęciową, jak „dane osobowe", można mieć wątpliwości co do tego, czy u.d.i.p. w obecnym kształcie odpowiada wymogom wynikającym z RODO. Taki stan rzeczy powoduje, że w dalszym ciągu aktualne są postulaty wprowadzenia do tej ustawy przepisów mających na celu dostosowanie określonych w niej mechanizmów ochrony sfery informacyjnej jednostki do wymogów RODO. W orzecznictwie sądów administracyjnych relacje prawa do informacji oraz prawa do ochrony danych osobowych w dalszym ciągu ustala się zatem w oparciu o jego powiązania z prawem do prywatności[18]. Z pewnością nie

[15] Dz. Urz. UE L 172, s. 56.

[16] *Ibidem*, s. 65–66 i przywołane tam orzecznictwo.

[17] Zob. N. Zawadzka, komentarz do art. 86, uw. 5 [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.

[18] Zob. G. Sibiga, *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych osobowych – wybrane zagadnienia*

jest to rozwiązanie zadowalające choćby z tego względu, że prawo do ochrony danych osobowych oraz prawo do prywatności stanowią osobne prawa podstawowe, mające podobny, ale nie ten sam przedmiot ochrony, a nadto ochrona danych osobowych rozciąga się nie tylko na dane osobowe ze sfery prywatności, ale obejmuje także te, które nie należą do tej sfery[19]. W tym stanie rzeczy znacznie bardziej adekwatna wydaje się konstrukcja współstosowania RODO oraz u.d.i.p. jako aktów zabezpieczających wykonywanie dwóch informacyjnych uprawnień jednostki, które niekiedy pozostają ze sobą w konflikcie[20], ale zasadniczo wymagają jednoczesnego wykonywania w aspekcie proceduralnym, na co wskazują zarówno analizowane ustalenia decyzji Prezesa UODO, jak i potwierdzające je argumenty wysuwane w uzasadnieniu glosowanego wyroku WSA w Warszawie.

Współstosowanie przepisów RODO i u.d.i.p.

Choć w analizowanym wyroku WSA w Warszawie sąd nie posługuje się tym pojęciem, jego ustalenia w sprawie w istocie stanowią odzwierciedlenie tezy, że także w bieżącym stanie prawnym przepisy o ochronie danych osobowych oraz o dostępie do informacji publicznej są współstosowane[21]. Stanowisko to ma rację bytu właśnie w warunkach sprawy analizowanej przez WSA w Warszawie oraz decyzji Prezesa UODO, wydanej w związku z niezgodnym z RODO przetwarzaniem danych osobowych przez Burmistrza, która to niezgodność dotykała zarówno sfery dopuszczalności przetwarzania – jego niezbędności i zgodności z prawem dokonywanych operacji przetwarzania danych, jak i obszaru rozwiązań techniczno-organizacyjnych.

Wyrok WSA w Warszawie, a wcześniej poprzedzająca go decyzja Prezesa UODO, odnosi się do zagadnienia współstosowania RODO oraz u.d.i.p. jako aktów, które regulują procedury dysponowania informacjami charakteryzowanymi jako dane osobowe oraz informacje publiczne w pewnym wspólnym obszarze oddziaływania, i których przepisy zasadniczo mają być realizowane równocześnie, urzeczywistniając odpowiednio prawo do ochrony danych osobowych oraz prawo dostępu do informacji publicznej. Trzeba mieć na względzie, że RODO i u.d.i.p. regulują odmienną materię, poprzez wskazanie procedur postępowania z informacjami innego rodzaju, w innych celach oraz dla

---

[w:] *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych*, red. *idem*, „Biblioteka Monitora Prawniczego" 2016, s. 20; wyrok WSA w Warszawie z dnia 29 września 2020 r., II SAB/Wa 225/20, LEX nr 3077523; wyrok WSA w Szczecinie z dnia 15 października 2020 r., II SA/Sz 624/20, LEX nr 3088437.

[19] Zob. M. Czerniawski, *Ochrona danych osobowych w prawie międzynarodowym* [w:] *Ochrona danych osobowych*, red. D. Lubasz, Warszawa 2020, s. 21; M. Wilbrandt-Gotowicz, *Prywatność osoby fizycznej jako ograniczenie jawności informacji publicznych (w świetle orzecznictwa sądów administracyjnych)* [w:] *Jawność i jej ograniczenia. Znaczenie orzecznictwa*, red. G. Szpor, t. 4, red. M. Jaśkowska, Warszawa 2014, s. 165.

[20] Zob. P. Fajgielski, komentarz do art. 86 [w:] *idem*, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, LEX/el.

[21] M. Sakowska-Baryła, komentarz do art. 86 [w:] *Ogólne rozporządzenie*…, s. 612.

realizacji zasadniczo odmiennych interesów – indywidualnego jednostki oraz interesu publicznego, do którego zresztą RODO odnosi się wprost w motywie 154, wskazując, że publiczny dostęp do dokumentów urzędowych można uznać za interes publiczny.

Unormowania te mają pewien wspólny obszar, który rysuje się wyraźniej, gdy ujawnieniu podlegać mają dane osobowe, ale obejmuje także sferę organizacji i zabezpieczeń we wszystkich przypadkach, gdy przy zapewnianiu dostępu do informacji publicznej w rachubę wchodzi przetwarzanie danych osobowych. Sfera rozwiązań organizacyjnych i technicznych na sam zakres ujawnianych w ramach dostępu do informacji publicznej może mieć pośredni wpływ, czego dobrym przykładem jest odpowiednie udokumentowanie powierzenia przetwarzania w związku z prowadzeniem BIP w infrastrukturze informatycznej zewnętrznego podmiotu, co miało miejsce w analizowanej sprawie. Może być i tak, że przetwarzanie odbywa się nie tyle w ramach ujawniania danych osobowych zawartych w informacji publicznej, ale ma miejsce akcesoryjnie, jak dzieje się chociażby z danymi osobowymi osób wnioskujących o udostępnienie informacji publicznej. Wszakże i ich prawo do ochrony danych osobowych musi być respektowane.

Współstosowanie przepisów RODO i u.d.i.p. oznacza stan, w którym jednocześnie podmioty zobowiązane na gruncie u.d.i.p. powinny realizować przewidziane w tej ustawie uprawnienia dostępowe, przestrzegając jednocześnie zasad ochrony danych uregulowanych w RODO poprzez ocenę dopuszczalności przetwarzania danych oraz wprowadzenie odpowiednich zabezpieczeń, powołanie inspektora ochrony danych, prowadzenie adekwatnej dokumentacji pozwalającej wykazać zgodność działania z RODO, wykonywanie praw osób, których dane dotyczą, prowadzenie rejestru czynności przetwarzania, wdrażanie polityk z zakresu ochrony danych osobowych itp.

Stosowanie procedur ochrony danych osobowych pod rządami RODO w związku z zapewnianiem dostępu do informacji publicznej, podobnie jak w poprzednim stanie prawnym, dotyczy zatem dwóch obszarów – pierwszy to obszar ustaleń dotyczących dopuszczalności ujawniania danych osobowych wchodzących w skład informacji publicznej; drugi to obszar procedur technicznio-organizacyjnych, który można określić „administrowaniem”[22]. Analizowany wyrok WSA w Warszawie oraz poprzedzająca go decyzja Prezesa UODO dobrze obrazują założenie, że organy i podmioty zobowiązane na gruncie u.d.i.p. oraz sądy orzekające w sprawach przetwarzania danych osobowych przy wykonywaniu praw dostępowych muszą brać pod uwagę m.in. zasady rozliczalności wynikające z art. 5 ust. 1 RODO, w tym m.in. zasadę minimalizacji danych, zgodnie z którą dane osobowe mają być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane czy też zasadę ograniczenia czasowego przetwarzania, co siłą rzeczy ma istotny wpływ na zakres udostępnianych danych osobowych, w tym danych o osobach pełniących funkcje publiczne, co dobrze

[22] Zob. M. Sakowska-Baryła, *Dostęp do informacji publicznej a ochrona danych osobowych*, Wrocław 2014, s. 76 i n.; *eadem*, *Problem współstosowania ustawy o dostępie do informacji publicznej i ustawy o ochronie danych osobowych* [w:] *Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość*, red. A. Mednis, Warszawa 2016, s. 173 i n.

zobrazowane zostało w ustaleniach dokonanych przez sąd i organ nadzorczy w analizowane sprawie[23].

Zakres stwierdzonych przez Prezesa UODO uchybień w procesie przetwarzania danych osobowych przez Burmistrza, pozwala na wskazanie pewnych obszarów stosowania procedur ochrony danych osobowych przy realizacji dostępu do informacji publicznej, gdzie właśnie można mówić o współstosowaniu przepisów RODO i u.d.i.p.

Stosowanie zasad rozliczalności przetwarzania danych osobowych

Wyrok wydany w sprawie II SA/Wa 2826/19 przez WSA w Warszawie potwierdza argumentację Prezesa UODO w zakresie zastosowania przy realizacji dostępu do informacji publicznej określonych w art. 5 RODO zasad dotyczących przetwarzania danych osobowych nazywanych zwykle „zasadami rozliczalności przetwarzania". W ten sposób WSA w Warszawie wyraził aprobatę dla szerokiego zastosowania procedur ochrony danych osobowych do procesów udostępniania informacji publicznej, nie ograniczając go tylko do samego aktu ujawniania danych osobowych zawartych w dokumentach urzędowych, które posiada organ lub podmiot publiczny, lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym. Zasady rozliczalności przetwarzania danych osobowych są bowiem sformułowane w sposób na tyle szeroki i uniwersalny, że oddziałują nie tylko na obszar ustaleń co do dopuszczalności przetwarzania danych osobowych – w tym konkretnym przypadku ich udostępnienia w ramach informacji publicznej, ale również na ten obszar, który odnosi się do kwestii organizacyjnych, dokumentacyjnych, technicznych zabezpieczeń, wprowadzanych procedur. Warto zatem wspomnieć, że zgodnie z art. 5 ust. 1 RODO dane osobowe muszą być:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami („ograniczenie celu");
3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");
5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one

[23] M. Sakowska-Baryła, komentarz do art. 86 [w:] *Ogólne rozporządzenie*…, s. 612.

przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");

6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

Jak natomiast stanowi art. 5 ust. 2 RODO, administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność").

Ustalenia dokonane przez WSA w Warszawie, a wcześniej przez Prezesa UODO, pozwalają wyrazić pogląd, że zarówno ten sąd, jak i organ nadzorczy stoją na stanowisku, że RODO oddziałuje i na tę część krajowego systemu dostępu do informacji publicznej, w której dochodzi do ujawnienia danych osobowych, i na ten obszar, w którym procedury ochrony danych osobowych mają za zadanie określić sposób powinnego zachowania podmiotu zobowiązanego w obszarze niejako administracyjnym, gdzie należy:

- dokonać odpowiednich czynności mających na celu zabezpieczenie danych osobowych i systemów informatycznych, służących ich przetwarzaniu;
- dokonać oceny ryzyka naruszeń praw lub wolności osób fizycznych, sporządzić polityki;
- uzupełnić rejestry czynności przetwarzania;
- zawrzeć umowy powierzenia przetwarzania danych osobowych;
- dokonać inwentaryzacji zasobów;
- zawrzeć umowy dotyczące zapewnienia infrastruktury informatycznej wykorzystywanej strony internetowej w postaci Biuletynu Informacji Publicznej;
- faktycznie zaprzestać przetwarzania danych, które staje się nieuzasadnione w związku z upływem czasu.

Owe administracyjne czynności administratora tylko pośrednio wpływają na treść, postać i zakres danych osobowych ujawnianych w ramach dostępu do informacji publicznej, do czego wprost odnosi się art. 86 RODO, stanowiąc, że dane osobowe zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub podmiot prywatny, w celu wykonania zadania realizowanego w interesie publicznym, mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem UE lub prawem państwa członkowskiego, któremu podlegają ten organ lub podmiot, dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych na mocy tego rozporządzenia.

Jednakże, biorąc pod uwagę zakres regulacji RODO oraz przewidzianych w nim procedur przetwarzania danych osobowych, można uznać, że ów obszar godzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych, dookreślonym w RODO nie tylko w aspekcie dopuszczalności przetwarzania,

ale i środków bezpieczeństwa o charakterze technicznym i organizacyjnym odpowiadającym charakterowi, zakresowi, kontekstowi i celom przetwarzania oraz ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, powinien rozciągać się także na te ostatnie – „wykonawcze" („administracyjne") uwarunkowania. Ochrona danych osobowych bowiem to zespół procedur postępowania z danymi osobowymi pozwalających ustalić, kiedy i na jakich warunkach korzystanie z nich jest legalne, oraz jakie prawa przysługują osobie fizycznej, w związku z przetwarzaniem jej danych osobowych. To procedury, które w praktyce chronią obydwie strony stosunku informacyjnego – i osobę, której dane dotyczą, i podmiot, który je przetwarza poprzez wyznaczenie wyraźnych reguł jego działania, a także poprzez wprowadzenie gwarancji o charakterze instytucjonalnym na czele z niezależnym organem nadzorczym wyposażonym w odpowiednie w tym względzie kompetencje. Ujęcie to odpowiada przybliżonej wcześniej konstrukcji współstosowania przepisów o ochronie danych osobowych oraz o dostępie do informacji publicznej, gdzie dostęp do informacji ma być realizowany przy jednoczesnym uwzględnieniu zasad ochrony danych, w tym wskazanych w art. 5 RODO, z którymi korespondują inne przepisy RODO i wynikające z nich obowiązki, czego wyraz odnaleźć można w sposobie formułowania zarzutów przez organ nadzorczy, który wskazując na naruszenia przepisów RODO, zwykle w pierwszej kolejności przytacza stosowną jednostkę redakcyjną art. 5 RODO, łącząc jej regulację z bardziej szczegółowym („merytorycznym") przepisem tego aktu.

Zgodzić się jednocześnie należy z WSA w Warszawie, że zasady wskazane w art. 5 RODO mają charakter samoistny i są wiążącymi normami prawnymi, określającymi konkretne normy postępowania w przedmiotowym zakresie. Mogą pełnić rolę subsydiarną w stosunku do innych przepisów, zwłaszcza przy ich interpretacji i stosowaniu norm prawnych dotyczących ochrony danych osobowych, jednak równie istotna jest ich funkcja jako norm nadrzędnych nad innymi przepisami. Prawodawca podkreśla ich szczególne znaczenie, określając je mianem „zasad"[24], przy czym tak administrator, jak i organ nadzorczy są zobowiązani do przestrzegania zawartych w tym przepisie zasad, a wszelkie wyłączenia mają charakter absolutnie wyjątkowy. Sąd słusznie podkreśla przy tym, że przy stosowaniu art. 5 ust. 1 RODO administrator ma znaczną swobodę w zakresie stosowanych rozwiązań, ale jednocześnie jednak ponosi odpowiedzialność za naruszenie przepisów o ochronie danych osobowych i – jak wynika z art. 5 ust. 2 RODO – to administrator danych powinien wykazać, a zatem udowodnić, że

[24] Na temat „zasady prawa" szerzej zob. R. Dworkin, *The model of rules*, „The University of Chicago Law Review" 1967, no. 1, s. 14 i n; R. Alexy, *A Theory o f Constitutional Rights*, przekł. J. Rivers, Oxford 2002; *idem*, *On the structure of legal principles*, „Ratio Juris" 2000, nr 3, s. 290 i n.; M. Kordela, *Możliwość konstruowania ogólnej teorii zasad prawa. Uwagi do koncepcji Roberta Alexy'ego*, RPEiS 2007, z. 2, s. 11 i n.; G. Maroń, *Formuła ważenia zasad prawa jako mechanizm usuwania ich kolizji na przykładzie koncepcji Roberta Alexy'ego*, „Zeszyty Naukowe Uniwersytetu Rzeszowskiego" 2009, nr 7, s. 86 i n.; E.G. Nalbandian, *Notes on Roland Dworkin's theory of law*, „Mizan Law Review" 2009, vol. 3, no. 2, s 370 i n., file:///C:/Users/msako/AppData/Local/Temp/145475-Article%20Text-384713-1-10-20161008.pdf [dostęp: 22.06.2021]; L. Leszczyński, G. Maroń, *Zasady prawa. Ujęcie dogmatyczno-porównawcze*, „Studia Iuridica Lublinensia" 2016, vol. 25, s. 317 i n.

przestrzega przepisów określonych w art. 5 ust. 1 RODO, czego w analizowanej sprawie nie dokonał Burmistrz Aleksandrowa Kujawskiego.

Analizowany wyrok WSA w Warszawie oraz poprzedzająca go decyzja Prezesa UODO potwierdzają zatem tezę, że zastosowanie RODO przy realizacji prawa dostępu do informacji publicznej odnosi się nie tylko do swoistego jądra tej relacji, gdzie dostęp do informacji publicznej krzyżuje się z prawem do ochrony danych osobowych, ale również do uwarunkowań proceduralnych, które określone zostały w RODO i które pozostają współstosowane z tymi przepisami u.d.i.p., które określają tryby i formy realizacji dostępu do informacji publicznej.

Powierzenie przetwarzania danych osobowych w związku z prowadzeniem BIP

W analizowanym wyroku, WSA w Warszawie podzielił zapatrywanie Prezesa UODO, że naruszeniem art. 5 ust. 1 lit. a oraz lit. f w zw. z art. 5 ust. 2 RODO jest udostępnianie danych osobowych zewnętrznym podmiotom w związku z prowadzeniem strony internetowej BIP Urzędu Miejskiego w Aleksandrowie Kujawskim bez uprzedniego zawarcia z tymi podmiotami umów powierzenia danych osobowych, w rozumieniu art. 28 ust. 3 RODO, kwalifikując to udostępnienie jako dokonane bez podstawy prawnej. Ze stanowiskiem tym należy się zgodzić, co więcej – korzystanie z zewnętrznego podmiotu dostarczającego rozwiązań technicznych do prowadzenia BIP jest jednym z bardziej powszechnych przykładów powierzenia przetwarzania danych osobowych w sektorze publicznym[25].

Powierzenie przetwarzania danych osobowych to stan faktyczny, jaki istnieje w konkretnych okolicznościach relacji pomiędzy administratorem a podmiotem przetwarzającym, czy też niekiedy pomiotami przetwarzającymi, jak ma to miejsce w analizowanej sytuacji, z którym to stanem faktycznym RODO wiąże określone obowiązki prawne każdego z podmiotów pozostających w tej relacji. Istotą powierzenia przetwarzania danych osobowych jest zlecenie na zewnątrz czynności przetwarzania danych osobowych – usługi wymagającej przetwarzania danych, w ramach której, przetwarzanie to jest elementem podstawowym lub co najmniej niezbędnym[26]. Tak jest właśnie w przypadku przetwarzania danych osobowych w ramach BIP, przy czym nie ma znaczenia, że informacje udostępniane w tym urzędowym publikatorze z zasady są jawne i powszechnie dostępne. Pamiętać trzeba bowiem, że zasady ochrony danych

[25] Zob. M. Sakowska-Baryła, *Powierzenie przetwarzania danych osobowych w sektorze publicznym* [w:] *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, red. M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda, Wrocław 2017, s. 13.

[26] Zob. M. Sakowska-Baryła, *Powierzenie przetwarzania w administracji publicznej* [w:] M. Jabłoński, M. Sakowska-Baryła, K. Wygoda, *Czy jesteśmy gotowi na stosowanie RODO? Wybrane zagadnienia z zakresu funkcjonowania administracji publicznej*, Wrocław 2018, s.108–110.

osobowych odnoszą się do każdej kategorii danych osobowych – także tych, które z założenia mają być powszechnie dostępne i z którymi łatwo się zapoznać.

Biorąc pod uwagę treść art. 28 RODO, nie sposób zatem kwestionować, że w przypadku powierzenia zewnętrznemu podmiotowi lub podmiotom prowadzenia BIP przez Burmistrza, to on właśnie jako administrator powinien zadbać o to, aby to powierzenie spełniało wymogi wynikające z przepisów prawa. Chodzi tu przede wszystkim o zawarcie pisemnej umowy powierzenia przetwarzania danych osobowych (art. 28 ust. 9 RODO), o treści odpowiadającej wymaganiom określonym w art. 28 ust. 3 RODO, a także o to, aby być w stanie wykazać dokonanie weryfikacji podmiotu przetwarzającego, co zakłada się w art. 28 ust. 1 RODO.

Choć powyższe ustalenia należy uznać za oczywiste, to jednak warte uwagi są okoliczności, w jakich do rzeczonego powierzenia prowadzenia BIP na zewnątrz doszło w analizowanej sprawie. W uzasadnieniu decyzji Prezesa UODO wskazuje się bowiem, że w trakcie kontroli ustalono, że ów BIP Urzędu Miejskiego w Aleksandrowie Kujawskim był prowadzony w formule dość często spotykanej w praktyce, gdzie dostarczanie takiej usługi zapewniane jest przez zewnętrzny podmiot, w ramach realizacji pewnego szerszego zamysłu organizacyjnego i finansowego, gdzie faktycznie bywa, iż umowa dotycząca realizacji tej usługi zawierana jest przez podmiot, który finansuje przedsięwzięcie, zaś poszczególni – pomniejsi – administratorzy wielokrotnie nie zawierają ani umów dotyczących ogólnie świadczenia usług, ani powierzenia przetwarzania. Jak czytamy w decyzji Prezesa UODO, w toku jego kontroli ustalono, że w związku z dostarczeniem oprogramowania dotyczącego utworzenia regionalnego biuletynu informacji publicznej, zawarta została umowa pomiędzy Województwem Kujawsko-Pomorskim a konsorcjum podmiotów, w której nie zostały ujęte postanowienia dotyczące ochrony danych osobowych ani nie została zawarta umowa o powierzeniu przetwarzania danych osobowych związana ze świadczeniem usług serwisowych na rzecz Urzędu Miejskiego w Aleksandrowie Kujawskim. Siłą rzeczy zatem w toku kontroli nie przedstawiono umowy pomiędzy Województwem Kujawsko-Pomorskim a Burmistrzem Miasta Aleksandrowa Kujawskiego, ani nie wykazano innego instrumentu prawnego, z którego wynikałoby, że udostępnienie serwera oraz dostarczenie oprogramowania służącego do utworzenia regionalnego biuletynu informacji publicznej realizowane jest przez Województwo Kujawsko-Pomorskie na rzecz Urzędu Miejskiego w Aleksandrowie Kujawskim. Szersze analizy tak zarysowanego stanu faktycznego znacząco wychodziłyby poza zakres prowadzonych tu rozważań, niemniej problem braku umów powierzenia w sytuacjach, gdy mamy do czynienia z relacją na swój sposób kaskadową – kiedy kto inny przedsięwzięcie finansuje, a kto inny z niego korzysta, bądź też gdy np. województwo, gmina, czy powiat nabywają usługę dla jednostek organizacyjnych powiązanych ze sobą na różne sposoby (wspólnym budżetem, relacjami organizacyjnymi, uczestnictwem we wspólnym projekcie unijnym), w praktyce okazuje się kwestią nieincydentalną. W tym stanie rzeczy konieczne wydaje się zalecać staranne przygotowanie takich przedsięwzięć, także w obszarze ochrony danych osobowych oraz umowne potwierdzenie relacji w odniesieniu do wszystkich pozostających w niej administratorów.

Naruszenie zasady ograniczenia czasowego przetwarzania danych osobowych

W analizowanym wyroku, WSA w Warszawie z aprobatą odniósł się do ustaleń Prezesa UODO, co do naruszenia przez Burmistrza art. 5 ust. 1 lit. e w zw. z art. 5 ust. 2, tj. zasady ograniczenia przechowywania, oraz art. 24 RODO poprzez brak odpowiednich polityk dotyczących przetwarzania danych osobowych w BIP Urzędu Miejskiego w Aleksandrowie Kujawskim pod kątem ich aktualności i celowości publikacji oraz określających terminy usunięcia danych osobowych. W wyniku oględzin strony BIP Urzędu Miejskiego w Aleksandrowie Kujawskim ustalono bowiem, że wśród zamieszczonych tam informacji pozostawały dokumenty zawierające dane osobowe, tj. oświadczenia majątkowe oraz informacje o wynikach naborów na wolne stanowiska, gdzie najstarsze informacje dotyczyły naborów przeprowadzonych w 2012 r. i zawierały informacje o wybranych kandydatach w zakresie: imię i nazwisko oraz miejsce zamieszkania w rozumieniu przepisów kodeksu cywilnego[27], zaś najstarsze zamieszczone na archiwalnej stronie BIP tego urzędu oświadczenia majątkowe dotyczyły 2010 r., co spowodowało stwierdzenie przez organ nadzorczy naruszenie przepisów RODO.

Powyższe zagadnienie wydaje się szczególnie kontrowersyjne z tej racji, że w przepisach u.d.i.p., ani też w innych przepisach przewidujących umieszczanie informacji w BIP zwykle nie wskazuje się, po jakim czasie informacje te mają być z tego publikatora usunięte. Zgodnie z argumentacją Prezesa UODO, podzielaną przez WSA w Warszawie, ów brak określonych przepisami prawa okresów przetwarzania udostępnionych informacji (zawierających dane osobowe) nie powoduje jednak, że informacje takie można przetwarzać bezterminowo. Wobec powyższego, administrator, zgodnie z zasadą ograniczonego przechowywania (art. 5 ust. 1 lit. e RODO), powinien w tym zakresie kierować się przepisami z innych aktów prawa, z których wynika czas, przez jaki może przetwarzać dane osobowe, a w przypadkach, w których prawo nie reguluje okresu retencji danych, po przeprowadzeniu analiz powinien określić ten okres tak, aby przetwarzanie danych było zgodne z celami, dla których realizacji je pozyskano.

Nie jest to zresztą jedyny wyrok odnoszący się do tego zagadnienia. Zasada ograniczenia czasowego wynikająca z art. 5 ust. 1 lit. e RODO była przedmiotem analiz WSA w Warszawie w sprawie II SA/Wa 1810/19, która dotyczyła kwestii nadmiernego czasowo udostępniania w BIP danych osobowych osoby, która ubiegała się o stanowisko sędziego. Dokonując oceny stanu faktycznego, WSA argumentował, że cel, jakim było udostępnienie informacji o wynikach konkursu na stanowisko sędziego, został już osiągnięty z uwagi na upływ prawie siedmiu lat od przyjęcia opublikowanej w BIP uchwały[28].

Należy podzielić zdanie WSA w Warszawie wyrażone w obydwu sprawach, że cel przetwarzania nie może funkcjonować i być oceniany w oderwaniu od okoliczności przetwarzania, a ustalając ten cel, należy odwołać się do okoliczności konkretnej

[27] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (tekst jedn.: Dz. U. z 2020 r., poz. 1740 ze zm.).
[28] Zob. wyrok WSA w Warszawie z dnia 29 stycznia 2020 r., II SA/Wa 1810/19, LEX nr 3041123.

sprawy, aby właściwie określić upływ spodziewanego terminu użyteczności danych. Tyle tylko, że kwestia przynajmniej przybliżonego określenia terminu usunięcia danych z BIP oraz wyraźne wskazanie, że tego typu usunięcie w ogóle jest możliwe, powinna być przesądzona wprost w przepisach prawa. Zważyć bowiem należy, że określanie celu przetwarzania danych osobowych przez administratora także w kontekście realizacji dostępu do informacji publicznej może następować inaczej w zależności od tego, jakie przesłanki w tej mierze będą brane pod uwagę przez administratora. Tymczasem, zważywszy na to, że dostęp ten jest realizowany przez kategorie podmiotów zobowiązanych, określonych w art. 4 u.d.i.p., które z założenia są do siebie podobne i realizują podobne cele, czas przetwarzania przez nie danych osobowych także powinien być podobny, a przy samodzielnie dokonywanych ustaleniach nie jest. Co więcej, obawa przed administracyjną karą pieniężną w związku ze zbyt długim przetwarzaniem danych w BIP może prowadzić z kolei do zdewaluowania założenia wynikającego z u.d.i.p., że to właśnie bezwnioskowe udostępnianie informacji w BIP jest podstawową formą zapewniania dostępu do informacji publicznej. W literaturze wskazuje się nawet na zasadę pierwszeństwa bezwnioskowego uzyskiwania informacji publicznej[29].

Wojewódzki Sąd Administracyjny w Warszawie w analizowanym tu wyroku potwierdził zatem słuszność sformułowanego przez Prezesa UODO zarzutu naruszenia art. 24 RODO poprzez brak odpowiednich polityk dotyczących przetwarzania danych osobowych w BIP Urzędu Miejskiego w Aleksandrowie Kujawskim pod kątem ich aktualności i celowości publikacji oraz określających terminy usunięcia danych osobowych, a w konsekwencji także słuszność nakazania przez Prezesa UODO dostosowania operacji przetwarzania danych osobowych do RODO, poprzez wdrożenie polityk określających okresy przetwarzania danych w BIP zgodne z przepisami prawa lub niezbędne do realizacji celów, w których dane są przetwarzane, zapewniających przestrzeganie terminów usuwania danych.

Na tle tychże ustaleń uzasadnione wydaje się poczynienie także pewnej krytycznej uwagi odnoszącej się do dokumentacyjnego aspektu przestrzegania zasad ochrony danych osobowych w sektorze publicznym. Odnotować trzeba bowiem, że w analizowanej sprawie doszło do sformułowania wobec Burmistrza zarzutu braku rzeczonej polityki, co poczytane zostało jako naruszenie RODO, a w konsekwencji wpłynęło na sformułowanie nakazu wdrożenia takiego dokumentu. Problem jednak w tym, że z żadnego z przepisów RODO nie sposób wyprowadzić wniosku, że posiadanie nominalnie takiej właśnie polityki jest obowiązkiem administratora. W zastrzeżeniu tym nie chodzi o to, aby kwestionować przyjęty w RODO otwarty sposób sformułowania wymogów w zakresie wprowadzanych rozwiązań technicznych i organizacyjnych, ponieważ ma on swoje istotne walory. Niemniej jednak brak bliższego skategoryzowania obowiązków technicznych i organizacyjnych w przypadku administratorów z sektora publicznego prowadzi do tego, że niemożliwe jest ustalenie katalogu obowiązków z zakresu ochrony danych osobowych, ciążących na administratorze, co jednak powinno być

[29] Zob. M. Bernaczyk, *Obowiązek bezwnioskowego udostępniania informacji publicznej*, Warszawa 2008, s. 150–156.

standardem w przypadku administratorów z sektora publicznego. Jeśli bowiem do kategorii administratorów zalicza się organy władzy publicznej i podmioty publiczne, to podstawową zasadą ich funkcjonowania jest działanie na podstawie i w granicach prawa. Tym samym, powinno być dla nich przewidywalne, jakie konkretnie obowiązki na nich ciążą, jakich dokładnie procedur mają przestrzegać i jakie polityki mają stworzyć. Tymczasem zakres koniecznych rozwiązań w postaci środków technicznych i organizacyjnych składających się na system ochrony danych osobowych, w RODO określa się w sposób otwarty, a o tym, czego na podstawie RODO można wymagać od będących administratorami organów lub podmiotów publicznych, wielokrotnie dowiedzieć się można dopiero z treści uzasadnień decyzji organu nadzorczego, bądź też jego stanowisk publikowanych na stronie internetowej. To źródła wiedzy przydatne w praktyce, ale niemające cech prawa powszechnie obowiązującego. W tym stanie rzeczy nie można poczynić wyczerpujących ustaleń, czy organ władzy publicznej lub inny podmiot publiczny zrealizował ciążące na nim obowiązki. W analizowanej sprawie Prezes UODO stwierdził m.in. brak u Burmistrza – publicznego administratora – „procedur wewnętrznych dotyczących przeglądu zasobów opublikowanych w BIP pod kątem zapewnienia przetwarzania danych, zgodnie z zasadą ograniczonego przechowywania, w wyniku czego na stronie BIP Urzędu Miejskiego w Aleksandrowie Kujawskim publikowane są dokumenty zawierające dane osobowe przez okres dłuższy niż wynika to z przepisów prawa", a z brakiem tym powiązał zastosowanie środków naprawczych z art. 58 ust. 2 RODO. Trzeba jednak wskazać, że przepisy RODO oraz przepisy prawa krajowego nie przewidują wprost posiadania tego rodzaju procedury przez wójta, burmistrza czy prezydenta miasta. Zarzut naruszenia przepisów RODO w tym względzie i okoliczność wydania ostatecznej decyzji administracyjnej wskazującej na naruszenia prawa i nakładającej administracyjną karę pieniężną siłą rzeczy przekładają się ustalenia dotyczące wypełnienia swoich obowiązków przez osoby fizyczne i ich odpowiedzialność. To niezwykle istotne w sektorze publicznym choćby z uwagi na zasady odpowiedzialności karnej funkcjonariuszy publicznych za niedopełnienie obowiązków, bądź też zasady odpowiedzialności za naruszenie dyscypliny finansów publicznych[30].

Brak wdrożenia odpowiednich środków technicznych i organizacyjnych oraz brak analizy ryzyka

Zarówno WSA w Warszawie, jak i Prezes UODO w analizowanej sprawie odnotowali naruszenia w postaci niewdrożenia odpowiednich środków technicznych i organizacyjnych mających na celu ochronę praw lub wolności osób fizycznych w związku z przechowywaniem nagrania sesji wyłącznie na serwerach YouTube, bez wykonywania kopii nagrań sesji Rady Miejskiej Aleksandrowa Kujawskiego, znajdujących się we własnych

[30] Zob. M. Sakowska-Baryła, *Specyfika stosowania RODO przez organy i podmioty publiczne* [w:] *Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych 2020*, red. G. Sibiga, M. Praw. 2020, nr 23 – dodatek, s. 33.

zasobach Urzędu Miejskiego. Taki stan rzeczy w ocenie sądu i organu nadzorczego uzasadniał postawienie skarżącemu Burmistrzowi zarzutu naruszenia art. 5 ust. 1 lit. f, w związku z art. 5 ust. 2 RODO, a więc zasady integralności i poufności, oraz art. 32 RODO poprzez niewdrożenie odpowiednich środków technicznych i organizacyjnych, mających na celu zabezpieczenie danych osób fizycznych w związku z przechowywaniem nagrań sesji Rady Miasta wyłącznie na serwerach YouTube, bez wykonywania i przechowywania kopii zapasowych tych nagrań w zasobach własnych Urzędu Miejskiego. W ocenie sądu, przekazanie danych osobowych podmiotowi zewnętrznemu, który transmituje posiedzenia organów w ogólnodostępnej sieci jaką jest internet, gdzie przetwarzane są dane osobowe, spowodowało naruszenie przepisów o ochronie danych osobowych, a środki, które należało podjąć, winny być proporcjonalne do wskazanego wysokiego ryzyka. Sąd podniósł, że z chwilą zakończenia nagrania było ono zapisane jedynie na stronie YouTube, a u skarżącego nie pozostawała żadna kopia zapasowa, co – zdaniem Sądu – naruszało w sposób jednoznaczny i ewidentny przepisy art. 32 ust. 1 lit. b i lit. c RODO. Przy tym sąd zaakcentował, że ewentualna awaria techniczna serwisu internetowego, może spowodować utratę nagrania i uniemożliwić administratorowi danych osobowych przywrócenie ich dostępności, w efekcie podmiot zobowiązany nie będzie mógł zapewnić poufności, integralności, dostępności i odporności systemów i usług przetwarzania. Dlatego w ocenie sądu, organ w sposób prawidłowy i zgodny z obowiązującymi przepisami wykazał naruszenie przez skarżącego przepisów RODO.

Trudno nie przyznać racji temu wywodowi, aczkolwiek argumentacja ta nie jest zupełna, a przy tym, wziąwszy pod uwagę to, że w przypadku zlecania na zewnątrz usługi utrzymania BIP, zarówno organ nadzorczy, jak i sąd dobitnie akcentowali brak legalizacji takiego udostępniania danych, dziwić może, że w przypadku przekazywania danych do YouTube nie pogłębiono już argumentacji. Ani WSA w Warszawie, ani Prezes UODO nie dokonali analizy roli, w jakiej występuje podmiot będący właścicielem tego serwisu. Jak słusznie wskazują Jan Byrski i Henryk Hoser, trudno przyjąć, że jest on wyłącznie podmiotem przetwarzającym (skoro może np. potencjalnie samodzielnie usuwać opublikowane nagrania), stąd należałoby co najmniej rozważyć, czy nie powinien on występować w roli współadministratora (wspólnie z podmiotem prowadzącym kanał) – zarówno w odniesieniu do danych osób, które znajdują się na nagraniach, jak również osób, które odtwarzają nagrania zamieszczone na zewnętrznym serwisie. Zastrzeżenia i niedosyt wywołuje to, że ani Prezes UODO, ani sąd w ogóle nie przeanalizowali tej istotnej kwestii, choć ma ona niepoślednie znaczenie dla określenia obowiązków spoczywających na Burmistrzu (podmiot prowadzący kanał), jak również na podmiocie odpowiedzialnym za serwis YouTube[31].

[31] Zob. J. Byrski, H. Hoser, *Pierwsza administracyjna kara pieniężna Prezesa UODO nałożona na podmiot publiczny*, „Informacja w Administracji Publicznej" 2020, nr 1, s. 14–15.

Brak analizy ryzyka w związku z korzystaniem z kanału YouTube

Jak argumentował WSA, przepis art. 32 RODO nie wymaga od administratora wdrożenia jakichkolwiek środków technicznych i organizacyjnych, które mają stanowić środki ochrony danych osobowych, ale wymaga wdrożenia środków adekwatnych, a taką adekwatność oceniać należy pod kątem sposobu i celu, w jakim dane osobowe są przetwarzane, ale też należy brać pod uwagę ryzyko związane z przetwarzaniem tych danych osobowych, które to ryzyko charakteryzować się może różną wysokością. Przyjęte środki mają mieć charakter skuteczny, w konkretnych przypadkach niektóre środki będą musiały być środkami o charakterze niwelującym niskie ryzyko, inne zaś – muszą niwelować ryzyko wysokie, ważne jednak jest, aby wszystkie środki (a także każdy z osobna) były adekwatne i proporcjonalne do stopnia ryzyka.

Na tym tle wydaje się zasadne stawianie Burmistrzowi zarzutu nieprzeprowadzenia analizy ryzyka w związku z korzystaniem z kanału YouTube w celu realizacji obowiązku prawnego wynikającego z art. 8 ust. 2 u.d.i.p., a więc naruszenia prawa materialnego, tj. art. 5 ust. 1 lit. f w zw. z art. 5 ust. 2 i art. 24 RODO. W tym przypadku sąd nie miał wątpliwości, że wdrożone przez Burmistrza procedury nie zapewniły w pełni bezpieczeństwa danych osobowych. W ocenie sądu, wdrożenie takiej analizy zminimalizowałoby ryzyko powstania uchybień w procesie przetwarzania danych osobowych, stąd pod tym właśnie kątem należy rozpatrywać ewentualną konieczność tworzenia odpowiedniej procedury systemu bezpieczeństwa i ochrony danych osobowych. Wskazanie na konieczność wprowadzenia takiej właśnie procedury nie powinno dziwić, ani być kwestionowane ze względu na niewątpliwą spójność analizy ryzyka, czy też innych procedur z tego zakresu z ogólnym zamysłem związanym ze stosowaniem przepisów RODO, jakim jest proaktywna postawa administratora i wdrażania środków techniczno-organizacyjnych, adekwatnych do tego ryzyka . Odnotować jednak należy, że zarówno Prezes UODO, jak i WSA odnoszą się do analizy ryzyka w zakresie korzystania z kanału YouTube, uznając najpewniej, że korzystanie przez administratora z zasobów i narzędzi oferowanych przez podmioty zewnętrzne może wiązać się z – jak to określił organ nadzorczy, a później WSA – „wyższym ryzykiem naruszenia ochrony danych osobowych" ze względu na fakt, że środki organizacyjne i techniczne wykorzystywane do ochrony danych osobowych opublikowanych na YouTube zostały określone i wdrożone przez Google LLC (z siedzibą w USA), właściciela YouTube. Dla porządku podnieść wypada, że w art. 24, art. 25, art. 32 oraz w art. 3 RODO jest mowa o „ryzyku naruszenia praw lub wolności osób fizycznych", nie zaś o „ryzyku ochrony danych osobowych", jakim to terminem posłużył się sąd i organ nadzorczy. Ponadto, w ich orzeczeniach brak głębszej refleksji, z jakich powodów korzystanie przez administratora z zasobów i narzędzi oferowanych przez podmioty zewnętrzne, w tym przypadku przez podmiot prowadzący kanał YouTube, może wiązać się z wyższym ryzykiem nie tyle naruszenia ochrony danych osobowych, co naruszenia praw lub wolności osób fizycznych. Określenie „wyższe ryzyko" jest przy tym wątpliwe o tyle, że na gruncie RODO gradacja ryzyka nie obejmuje takiego poziomu jak owo „wyższe ryzyko". Właściwie z treści RODO

wyprowadzać można wniosek, że doniosłe przy stosowaniu tego aktu są trzy stany: brak ryzyka, ryzyko i wysokie ryzyko[32]. Czy zatem „wyższe ryzyko", jest „ryzykiem wysokim" nie można się dowiedzieć ani z wyroku WSA w Warszawie, ani z decyzji Prezesa UODO, a przesądzenie tego byłoby wskazane, zwłaszcza że zgodnie z art. 35 RODO, z wysokim ryzykiem wiąże się obowiązek przeprowadzenia i udokumentowania oceny skutków dla ochrony danych osobowych.

Braki w rejestrze czynności przetwarzania

Trudno podawać w wątpliwość stwierdzenie przez organ nadzorczy naruszenia przez Burmistrza art. 5 ust. 2 RODO w związku z art. 30 ust. 1 lit. d oraz lit. f RODO poprzez niewskazanie w rejestrze czynności przetwarzania danych osobowych dla czynności związanych z publikacją informacji na stronie BIP Urzędu Miasta w Aleksandrowie Kujawskim, wszystkich odbiorców danych oraz niewskazanie dla tych czynności przetwarzania planowanego terminu usunięcia danych w sposób zapewniający przetwarzanie danych, zgodnie z zasadą ograniczonego przechowywania. Stwierdzenie tego naruszenia odzwierciedla to, że organ nadzorczy przedmiotem swoich ustaleń czyni skrupulatność prowadzenia tego rejestru oraz wskazuje, że adnotacje w nim sporządzane powinny być możliwie konkretne i wyczerpujące. Sąd wskazał przy tym, że administrator, który nie wykaże w rejestrze czynności kategorii odbiorców, którym dane osobowe zostały lub zostaną ujawnione, oraz nie wskaże planowego terminu usunięcia poszczególnych kategorii danej (pod warunkiem, że jest to możliwe – a w niniejszej sprawie taka możliwość istniała), narusza bezpośrednio przepisy dotyczące ochrony danych osobowych, za których przestrzeganie jest odpowiedzialny. Sąd wyprowadza z tego słuszny wniosek, że każdy z obowiązków wynikających z art. 30 ust. 1 RODO musi zostać zrealizowany: naruszeniem przepisu jest niewykonanie choćby jednego z obowiązków wskazanego przy prowadzeniu rejestru czynności przetwarzania danych osobowych.

Administracyjna kara pieniężna

Ponieważ za naruszenie przepisów art. 5 ust. 1 lit. a, e oraz lit. f, art. 5 ust. 2, art. 28, art. 30 ust. 1 lit. d i lit. f oraz art. 32 RODO Prezes UODO nałożył na Burmistrza Aleksandrowa Kujawskiego karę pieniężną w kwocie 40 tys. zł, WSA w Warszawie ocenił, mając na uwadze charakter dokonanych naruszeń oraz ilość przepisów prawa materialnego w zakresie ochrony danych osobowych, których naruszenia dopuścił się skarżący, że owa kara pieniężna jest karą adekwatną, proporcjonalną i nałożona została w sposób

[32] Zob. A. Mednis, *Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych*, M. Praw. 2016, nr 20 – dodatek, s. 29.

prawidłowy. Organ należycie uzasadnił wymiar kary, biorąc pod uwagę bardzo długi czas trwania naruszeń, umyślny ich charakter, wysoki stopień odpowiedzialności administratora oraz brak jego współpracy z organem po wszczęciu postępowania. Maksymalna kara za stwierdzone naruszenia wynosi 100 tys. zł, na skarżącego nałożono tylko 40% możliwej kary, co pozwala ocenić ją jako skuteczną, proporcjonalną i odstraszającą.

Rzecz jasna, zarówno z podstawami do nałożenia administracyjnej kary pieniężnej w tym przypadku, jak i z jej wysokością można polemizować. Istotne wątpliwości budzi choćby to, czy rzeczona kara rzeczywiście jest proporcjonalna do „przewinienia" skarżącego. Można uznać także, że kwota kary jest nader wysoka, zważywszy na treść i charakter danych, dotkniętych naruszeniem RODO. Dane te bowiem w znaczącej części stanowiły informacje powszechnie dostępne, z mocy prawa podlegające udostępnieniu, choć rzeczywiście dyskusyjną kwestią pozostaje ich przechowywanie wyłącznie w zasobach YouTube, czy też poniechanie zawarcia umowy powierzenia przetwarzania danych, podczas gdy obowiązek taki istniał również pod rządami poprzednio obowiązujących przepisów prawa. Wydaje się jednak, że najistotniejszym czynnikiem, przemawiającym za jej wymierzeniem była prewencja zarówno indywidualna, jak i generalna. Jak bowiem argumentował w zaskarżonej decyzji organ nadzorczy, „odstraszający charakter kary pieniężnej wiąże się z zapobieganiem naruszeniom w przyszłości oraz przykładanie większej wagi do realizacji zadań administratora. Kara ma odstraszać zarówno administratora, przed ponownym naruszeniem, jak i inne podmioty. Nakładając decyzją administracyjną karę pieniężną za naruszenie przepisów o ochronie danych osobowych Prezes Urzędu Ochrony Danych Osobowych wziął pod uwagę oba aspekty: po pierwsze – charakter represyjny, Burmistrz naruszył przepisy ogólnego rozporządzenia o ochronie danych, po drugie – charakter prewencyjny, zarówno Burmistrz, jak i inni administratorzy, będą skutecznie zniechęceni do naruszania w przyszłości prawa ochrony danych osobowych, jednocześnie dokładając większej staranności przy realizacji swoich obowiązków wynikających z ogólnego rozporządzenia o ochronie danych".

Przytoczona argumentacja organu nadzorczego wydaje się równocześnie dobrym podsumowaniem prowadzonych tu rozważań. Z jednej strony bowiem, analizowane orzeczenia mają wymiar indywidualny dla ukaranego administratora, z drugiej zaś – orzeczenia te niewątpliwe kierują uwagę na zwiększenie staranności przy wykonywaniu wynikających z RODO obowiązków ciążących na publicznych administratorach.

Literatura

Barta P., Litwiński P., *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, Warszawa 2021.

Bernaczyk M., *Obowiązek bezwnioskowego udostępniania informacji publicznej*, Warszawa 2008.

Byrski J., Hoser H., *Pierwsza administracyjna kara pieniężna Prezesa UODO nałożona na podmiot publiczny*, „Informacja w Administracji Publicznej" 2020, nr 1.

Czerniawski M., *Ochrona danych osobowych w prawie międzynarodowym* [w:] *Ochrona danych osobowych*, red. D. Lubasz, Warszawa 2020.

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

Jabłoński M., *Rola i znaczenie RODO w procesie definiowania gwarancji niezależności i spójności krajowego systemu ochrony danych osobowych* [w:] M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda, *Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym*, Wrocław 2017.

Mednis A., Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych, M. Praw. 2016, nr 20 – dodatek.

Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.

Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, red. M. Sakowska-Baryła, Warszawa 2018.

Sakowska-Baryła M., *Dostęp do informacji publicznej a ochrona danych osobowych*, Wrocław 2014.

Sakowska-Baryła M., *Powierzenie przetwarzania danych osobowych w sektorze publicznym* [w:] *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, red. M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda, Wrocław 2017.

Sakowska-Baryła M., *Problem współstosowania ustawy o dostępie do informacji publicznej i ustawy o ochronie danych osobowych* [w:] *Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość*, red. A. Mednis, Warszawa 2016.

Sakowska-Baryła M., *Specyfika stosowania RODO przez organy i podmioty publiczne* [w:] *Ocena i przegląd RODO po dwóch latach obowiązywania. Aktualne problemy prawnej ochrony danych osobowych 2020*, red. G. Sibiga, M. Praw. 2020, nr 23 – dodatek.

Sibiga G., *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych osobowych – wybrane zagadnienia*, [w:] *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych*, red. *idem*, „Biblioteka Monitora Prawniczego" 2016.

Sibiga G., Małobęcka-Szwast I., *Relacje prawa do informacji publicznej oraz prawa do ochrony danych osobowych w świetle ogólnego rozporządzenia o ochronie danych (RODO)* [w:] *Polskie przepisy o ochronie danych osobowych. Aktualne problemy prawnej ochrony danych 2019*, red. *idem*, M. Praw. 2019, nr 22 – dodatek.

Wilbrandt-Gotowicz M., *Prywatność osoby fizycznej jako ograniczenie jawności informacji publicznych (w świetle orzecznictwa sądów administracyjnych)* [w:] *Jawność i jej ograniczenia*, red. G. Szpor, t. 4, *Znaczenie orzecznictwa*, red. M. Jaśkowska, Warszawa 2014.

Streszczenie

Marlena Sakowska-Baryła

Pierwsza administracyjna kara pieniężna nałożona na podmiot z sektora publicznego

Glosa poświęcona została omówieniu wyroku WSA w Warszawie, a także poprzedzającej go decyzji Prezesa Urzędu Ochrony Danych Osobowych w sprawie na styku ochrony danych osobowych oraz dostępu do informacji publicznej. Orzeczenia te można uznać za doniosłe o tyle, że

dotyczą udostępniania danych osobowych w Biuletynie Informacji Publicznej, kwestii retencji danych osobowych leżącej w gestii podmiotu publicznego w przypadku, gdy przepisy nie precyzują czasu upubliczniania danych w tymże publikatorze, zabezpieczenia danych, w tym wdrożenia procedur, których prowadzenie nie zostało wprost przewidziane w ustawie, powierzenia przetwarzania danych osobowych w warunkach działalności podmiotów publicznych, a wreszcie dość newralgicznego zagadnienia, jakim jest zastosowanie RODO do przetwarzania danych osobowych w związku z realizacją dostępu do informacji publicznej. Na kanwie tych orzeczeń możliwe jest prześledzenie istotnych kwestii współstosowania przepisów RODO z przepisami regulującymi zagadnienia dostępu do informacji publicznej na wielu płaszczyznach – zarówno w obszarze dopuszczalności przetwarzania danych osobowych oraz zasad rozliczalności, jak i w obszarze techniczno-organizacyjnym.

Słowa kluczowe: informacja publiczna; administracyjna kara pieniężna; sektor publiczny; RODO; Biuletyn Informacji Publicznej; bezpieczeństwo danych, oświadczenia majątkowe.

Summary

Marlena Sakowska-Baryła

First Administrative Fine Imposed on a Public Sector Entity

The text discusses the judgement of the Voivodeship Administrative Court in Warsaw and the preceding decision of the President of the Personal Data Protection Office concerning the issue of personal data protection and access to public information. These rulings can be considered important as they concern the access to personal data in the Public Information Bulletin, the issue of retention of personal data which are within the competence of a public entity when the regulations do not specify the time of making the data public in that publication, data security, including the implementation of procedures, the performance of which is not directly provided by the law, entrusting the processing of personal data in the conditions of activity of public entities, and finally quite a sensitive issue which is the application of GDPR to the processing of personal data in relation to the exercise of access to public information. On the basis of these rulings, it is possible to trace significant issues of co-application of the provisions of GDPR with the provisions regulating the issues of access to public information at many levels – both in the area of admissibility of personal data processing and the principles of accountability, as well as in the technical and organisational.

Keywords: public information; administrative fine; public sector; GDPR; Public Information Bulletin; data security, assets declaration.