Realizacja obowiązków administratora danych w związku z powierzeniem przetwarzania danych osobowych, odpowiedzialność podmiotu przetwarzającego oraz model współpracy między tymi podmiotami

Decyzja Prezesa Urzędu Ochrony Danych Osobowych
z dnia 11 lutego 2021 r., DKN.5130.2024.2020

1. **Obowiązkiem administratora (…) przy dokonywaniu oceny proporcjonalności zabezpieczeń jest branie pod uwagę czynników i okoliczności dotyczących przetwarzania (np. rodzaj, sposób przetwarzania danych) i ryzyka, jakie się z nim wiąże. Jakiekolwiek zmiany w procesie przetwarzania danych osobowych są okolicznością szczególnie obarczającą administratora odpowiedzialnością za zmaterializowanie się zagrożeń związanych z niedopełnieniem powyższych obowiązków. Zapewnienie odpowiedniego bezpieczeństwa danym osobowym, na każdym etapie przetwarzania, powinno być przedmiotem szczególnej troski administratora.**
2. **(...) Koniecznością staje się możliwość udowodnienia przed organem nadzorczym, że wprowadzone rozwiązania, mające na celu zapewnienie bezpieczeństwa danych osobowych, są adekwatne do poziomu ryzyka, jak również uwzględniają charakter danej organizacji oraz wykorzystywanych mechanizmów przetwarzania danych osobowych. Administrator samodzielnie ma przeprowadzić szczegółową analizę prowadzonych procesów przetwarzania danych i dokonać oceny ryzyka, a następnie zastosować takie środki i procedury, które będą adekwatne do oszacowanego ryzyka.**

Edyta Bielak-Jomaa
Uniwersytet Łódzki
ejomaa@wpia.uni.lodz.pl
ORCID: 0000-0002-9217-7959

https://doi.org/10.26881/gsp.2021.4.11

1. Uwagi wstępne

Komentowana decyzja odnosi się do bardzo istotnego – z praktycznego punktu widzenia – zagadnienia, jakim jest prawidłowa realizacja ciążących na administratorze danych obowiązków w związku z powierzeniem przetwarzania danych osobowych, odpowiedzialności podmiotu przetwarzającego oraz modelu współpracy między tymi podmiotami. Glosowane rozstrzygnięcie porusza także inną ważną i w praktyce trudną kwestię – przeprowadzenie przez administratora oceny ryzyka, ale ta pozostaje nieco na uboczu rozważań prowadzonych w niniejszym opracowaniu.

Tytułem wprowadzenia godzi się przypomnieć najbardziej istotne aspekty analizowanego rozstrzygnięcia organu nadzorczego. W dniu 11 lutego 2021 r. Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO), wydał decyzję, mocą której ukarał Krajową Szkołę Sądownictwa i Prokuratury – administratora danych osobowych, karą 100 tys. zł za brak realizacji ciążących na niej obowiązków administratora, czego skutkiem było naruszenie ochrony danych osobowych dotyczące ponad 50 tys. osób, m.in. sędziów, prokuratorów, asesorów prokuratury, referendarzy sądowych, kuratorów, polegające na nieuprawnionym dostępie do bazy danych Krajowej Szkoły Sądownictwa i Prokuratury (KSSiP)[1]. Kategorie danych, których dotyczyło naruszenie obejmowały: imiona i nazwiska, adresy e-mail, numery telefonów, adresy zamieszkania, miejsca pracy oraz ich adresy, adresy IP, daty pierwszego i ostatniego logowania, hasła i numery różnego rodzaju komunikatorów, numery PESEL. Naruszenie spowodowało, w ocenie Prezesa UODO, wysokie ryzyko wystąpienia negatywnych skutków w przyszłości, wynikających z charakteru danych, dużej liczby podmiotów danych, prawdopodobnie złej woli osoby, która w sposób nieuprawniony uzyskała do nich dostęp.

Krajowa Szkoła Sądownictwa i Prokuratury zgłosiła Prezesowi UODO naruszenie ochrony danych osobowych, w którym wskazano, że administrator został powiadomiony przez Komendę Główną Policji o pojawieniu się w internecie danych osobowych związanych z domeną kssip.gov.pl. Tego samego dnia administrator stwierdził naruszenie ochrony danych osobowych. Po zapoznaniu się z rodzajem danych ustalił, że są to dane z bazy danych witryny szkolenia.kssip.gov.pl powstałe w trakcie testowej migracji do nowej platformy szkoleniowej ekssip.kssip.gov.pl. W celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków wobec osób, których dane dotyczą, administrator wysłał zgłoszenie do administracji forum publikującego odnośnik do bazy danych z żądaniem zablokowania informacji oraz do administracji portalu udostępniającego plik z danymi – o zablokowanie możliwości pobierania. Ponadto, usunął wszystkie hasła na nowej platformie i umieścił informację o konieczności zmiany hasła przy logowaniu do nowej platformy. Stwierdzając wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, rozpoczął informowanie wszystkich osób, których naruszenie dotyczy, o zaistniałej sytuacji.

[1] Zob. glosowana decyzja DKN.5130.2024.2020, https://www.uodo.gov.pl/decyzje/DKN.5130.2024.2020 [dostęp: 20.11.2021].

Zdaniem Prezesa UODO, KSSiP naruszyła szereg przepisów RODO[2]: art. 5 ust. 1 lit. f, art. 25 ust. 1, art. 28 ust. 3, art. 32 ust. 1 i 2, poprzez:

a) niezastosowanie odpowiednich środków technicznych i organizacyjnych mających zapewnić zdolność do ciągłego zapewnienia poufności usług przetwarzania;
b) brak testowania i oceny skuteczności środków technicznych i organizacyjnych, mających na celu zapewnienie bezpieczeństwa danych osobowych znajdujących się w kopii bazy danych platformy szkoleniowej Krajowej Szkoły Sądownictwa i Prokuratury;
c) niewłaściwe uwzględnienie ryzyka związanego ze zmianami w procesie przetwarzania;
d) powierzenie przetwarzania danych osobowych z naruszeniem art. 28 ust. 3 RODO:
   – bez umownego zobowiązania podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora;
   – bez określenia w umowie powierzenia przetwarzania danych osobowych kategorii osób;
   – bez doprecyzowania rodzaju danych osobowych przez wskazanie ich kategorii.

Administrator, bez względu na to, czy jest jedynym podmiotem przetwarzającym dane osobowe, czy tez powierza dane, albo ich część do przetwarzania innemu podmiotowi, ponosi odpowiedzialność za ich bezpieczeństwo. Przepisy rozporządzenia 2016/679 zobowiązują więc zarówno administratorów, jak i podmioty przetwarzające do przyjęcia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych. W analizowanym rozstrzygnięciu, Prezes UODO uznał, że administrator – KSSIP nie zapewnił bezpieczeństwa danych (poprzez niezastosowanie odpowiednich środków technicznych i organizacyjnych służących poufności przetwarzania, brak testowania i oceny skuteczności tych środków oraz niewłaściwe uwzględnienie ryzyka związanego ze zmianami w procesie przetwarzania danych), co było spowodowane niezgodnością z przepisami RODO zawartej umowy powierzenia oraz zakresem odpowiedzialności stron tej umowy.

2. Obowiązki administratora

W przywołanej decyzji Prezes UODO kilkukrotnie wskazał na obowiązki administratora w przetwarzaniu danych osobowych, przede wszystkim w kontekście stosowania środków technicznych i organizacyjnych, o których mowa w art. 24, art. 25 i art. 32 RODO. Zgodnie z art. 24 ust. 1 RODO, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym

[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; dalej: RODO; rozporządzenie 2016/679).

prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem, i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

W świetle glosowanej decyzji, oznacza to, że KSSiP, przy dokonywaniu oceny proporcjonalności zabezpieczeń powinna uwzględnić czynniki i okoliczności dotyczące przetwarzania (np. rodzaj danych osobowych, sposób przetwarzania danych) i ryzyko, jakie się z nim wiąże. Słusznie podkreślił Prezes UODO, że wdrożenie odpowiednich zabezpieczeń stanowi obowiązek będący przejawem realizacji ogólnej, określonej w art. 5 ust. 1 lit. f RODO, zasady integralności i poufności, zgodnie z którą dane osobowe powinny być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. Środki te powinny być zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą. Powinny one zatem uwzględniać, zgodnie z art. 25 ust. 1 rozporządzenia 2016/679, stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania.

Administrator zobowiązany jest ponadto do zastosowania środków technicznych i organizacyjnych odpowiadających ryzyku (adekwatnych do tego ryzyka) naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia (art. 32 ust. 1 RODO). Oznacza to, że odpowiedzialny administrator powinien wpierw określić poziom ryzyka, jakie wiąże się z przetwarzaniem danych osobowych, by móc następnie zdecydować, jakie odpowiadające temu ryzyku (minimalizujące je), środki techniczne i organizacyjne zastosować. Znajduje to potwierdzenie w wyroku wojewódzkiego sądu administracyjnego z dnia 3 września 2020 r.[3] Sąd orzekł w nim, że administrator samodzielnie ma przeprowadzić szczegółową analizę prowadzonych procesów przetwarzania danych i dokonać oceny ryzyka, a następnie zastosować takie środki i procedury, które będą adekwatne do oszacowanego ryzyka. Uwzględnić, przy tym powinien 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. W innym orzeczeniu sąd orzekł, że w art. 32 rozporządzenia 2016/679 nie wymaga się od administratora danych wdrożenia jakichkolwiek środków technicznych i organizacyjnych, które mają stanowić środki ochrony danych osobowych, ale wymaga wdrożenia środków adekwatnych. Taką adekwatność oceniać należy pod kątem sposobu i celu, w jakim dane osobowe są przetwarzane, ale też należy brać pod uwagę ryzyko związane

[3] Wyrok WSA w Warszawie z dnia 3 września 2020 r., II SA/Wa 2559/19, LEX nr 3077973.

z przetwarzaniem tych danych osobowych, które to ryzyko charakteryzować się może różnym poziomem[4].

Analiza ryzyka powinna mieć także znaczenie przy wyborze podmiotu przetwarzającego oraz przy określeniu warunków umowy powierzenia. Zgodnie z art. 28 ust. 1 rozporządzenia 2016/679, administrator powinien korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą[5]. Realnemu zapewnieniu tego wymogu służy uprawnienie administratora do uzyskania od podmiotu przetwarzającego wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 RODO oraz uprawnienie do przeprowadzania audytów, w tym inspekcji. Jak wskazuje się w motywie 81 RODO, aby zapewnić przestrzeganie wymogów niniejszego rozporządzenia w przypadku przetwarzania, którego w imieniu administratora ma dokonać podmiot przetwarzający, administrator powinien, powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania. Administrator musi więc nie tylko sprawdzić prawidłowość i adekwatność środków bezpieczeństwa zastosowanych przez podmiot przetwarzający, ale także móc wykazać, że weryfikacji takiej dokonał, np. poprzez dokonanie audytu albo żądanie od podmiotu przetwarzającego dowodu, że taki audyt się odbył, i raportu z jego przeprowadzenia[6]. Tymczasem, w prezentowanej sprawie, administrator nie mógł wykazać się ani posiadaniem odpowiedniej dokumentacji potwierdzającej przyjęcie i wdrożenie środków zabezpieczenia technicznego i organizacyjnego, zgodnie z przepisami RODO, co świadczy o naruszeniu przepisów i skutkuje brakiem kontroli administratora nad przetwarzaniem danych osobowych, ani także – co jest kluczowe z punktu widzenia analizowanego rozstrzygnięcia – wskazaniem przesłanek weryfikacji podmiotu przetwarzającego. Warte podkreślenia jest stanowisko Prezesa UODO, który uznał, że wybór nawet profesjonalnego hostingodawcy posiadającego niezbędne certyfikaty przy określonych zabezpieczeniach dostępu do systemu oraz przy ograniczeniu kontaktu między pracownikami administratora i podmiotu przetwarzającego nie jest gwarancją minimalizowania ryzyka ewentualnego naruszenia bezpieczeństwa danych, na co wskazywał administrator. Słusznie zauważył też, że nie wyczerpuje to w żaden sposób obowiązku przeprowadzenia analizy ryzyka, która w tym przypadku jest nieadekwatna zarówno w odniesieniu do charakteru podejmowanych czynności w związku z migracją, jak i charakteru zawartej umowy usługi hostingu.

---

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

5 Wyrok WSA w Warszawie z dnia 27 października 2020 r., II SA/Wa 2559/19, LEX nr 3100511.

6 M. Krzysztofek, *Warunki dopuszczalności powierzenia – lista kontrolna*, ABI Ekspert 2017, nr 4, s. 19.

Prezes UODO zarzucił KSSiP, że brak angażowania podmiotu przetwarzającego w proces migracji oraz nieudzielenie pełnych informacji o podejmowanych czynnościach i oczekiwanych rezultatach, spowodowało, że administrator nie miał wiedzy, czy przetwarzane dane osobowe są odpowiednio zabezpieczone. Prowadzi to do stwierdzenia, że KSSiP nie podjęła wystarczających działań mających na celu zweryfikowanie bezpieczeństwa środowiska przetwarzania zarówno przed rozpoczęciem działań migracyjnych, jak i po ich zakończeniu, a w szczególności nie zweryfikowała lokalizacji kopii bazy danych.

3. Umowa powierzenia

W opisywanym przypadku dużą rolę odgrywa też zakres i poziom usług wynikający z umowy hostingowej. Kwestię tę podkreślono w uzasadnieniu decyzji o nałożeniu na administratora kary. Jak wynika z treści, podmiot przetwarzający jako wykonawca usługi hostingowej, został wyłoniony w postępowaniu o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego[7]. Prezes UODO, powołując się na treść art. 28 ust. 3 RODO, wskazał, że umowa ma na celu zapewnienie precyzyjnego ustalenia granic działania podmiotu przetwarzającego, powinna zatem kompleksowo regulować, co jest podstawą umowy powierzenia ze względu na związanie podmiotu przetwarzającego z celem ustalonym przez administratora, oraz wskazywać treść. Artykuł 28 ust. 3 RODO, w sposób rozbudowany determinuje treść umowy, która musi zawierać przedmiot i czas trwania przetwarzania; charakter i cel przetwarzania; rodzaj danych osobowych; kategorie osób, których dane dotyczą; obowiązki i prawa administratora. W literaturze podkreśla się, że określenie celu i charakteru przetwarzania oraz rodzaju danych osobowych sprowadzać się powinno do doprecyzowania, jakie kategorie danych i po co zostały powierzone do przetwarzania, a także w jaki sposób mają być przetwarzane. Precyzyjna regulacja w tym zakresie konieczna jest ze względu na związanie podmiotu przetwarzającego ustalonym przez administratora celem[8].

W glosowanej decyzji w sposób niewystarczający określono zakres powierzanych danych. Wskazano bowiem, że „podmiot przetwarzający w ramach świadczenia usługi hostingowej przetwarzał będzie powierzone dane osobowe zwykłe obejmujące zbiory danych osobowych niezbędne do wykonywania prac w systemie informatycznym na rzecz administratora". Krajowa Szkoła Sądownictwa i Prokuratury, powierzając przetwarzanie danych osobowych, nie wskazała w umowie powierzenia kategorii osób oraz nie doprecyzowała rodzaju danych osobowych przez podanie ich kategorii. Opisując przetwarzanie danych, umowa powinna bowiem również odwoływać się do kategorii danych osobowych, jeśli można je doprecyzować. O ile w przypadku przetwarzania danych związanych np. z usługą poczty elektronicznej, trudno jest jednoznacznie taki

[7] Ustawa z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 1843).

[8] K. Witkowska-Nowakowska, *Komentarz do art. 28 RODO* [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 639.

zakres wskazać, o tyle w przypadku przetwarzania danych w celach związanych z funkcjonowaniem platformy szkoleniowej KSSiP, informacje takie, jako możliwe do określenia, powinny być w niej zawarte.

Ponadto, jak wskazano w decyzji, administrator nie zawarł w umowie zobowiązania podmiotu przetwarzającego do przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora, co stanowi wymóg wynikający z art. 28 ust. 3 pkt a rozporządzenia 2016/679. Trudno nie podzielić stanowiska Prezesa Urzędu, że określenie sposobu zgłaszania (pisemnie, faksem, pocztą elektroniczną) usterek związanych z usługami hostingowymi, w tym ich niedostępność, nie jest wystarczające do uznania tego postanowienia za udokumentowane polecenie administratora. Udokumentowane polecenie administratora oznacza bowiem możliwość przetwarzania danych na podstawie udokumentowanych instrukcji i wskazówek administratora. Co prawda prawodawca unijny, wprowadzając obowiązek dokumentowania wszystkich wskazówek, nie przesądził, jaką ma mieć ono formę, to jednak warto zauważyć, że zastrzeżenie możliwości działania podmiotu przetwarzającego wyłącznie na udokumentowane polecenie administratora może zostać implementowane do umowy na etapie jej tworzenia. Skoro w art. 28 ust. 3 lit. a RODO wymaga się, by sama umowa powierzenia miała formę pisemną, w tym elektroniczną, to należy przyjąć, że w jej ramach ustanowiony powinien zostać generalny obowiązek działania na udokumentowane polecenie administratora, natomiast dopuszczalne wydaje się przyjęcie, że same wskazówki kształtowane być mogą na późniejszym etapie w formie ustalonej przez strony stosunku powierzenia. Istotne jest natomiast, by wszelkie polecenia administratora były konsekwentnie dokumentowane[9]. Takich działań nie wykonał administrator, bowiem ani umowa nie zawierała ogólnego polecenia, ani na późniejszym etapie jej realizacji administrator nie przekazał żadnych wskazówek procesorowi, które to polecenie by dokumentowały.

4. Model współpracy administratora z podmiotem przetwarzającym

Konsekwencją zawarcia umowy powierzenia jest zbudowanie prawidłowego modelu współpracy między stronami umowy. W komentowanej decyzji, Prezes UODO poświęcił uwagę ocenie współpracy między KSSIP a podmiotem przetwarzającym. Zasady i zakres współpracy wynikać powinny z treści umowy powierzenia, winny być bowiem one efektem wzajemnych relacji, obowiązków i odpowiedzialności stron umowy powierzenia. Dla prawidłowej realizacji umowy kapitalne znaczenie ma dodatkowo określenie kanałów komunikacyjnych między administratorem i podmiotem przetwarzającym. W analizowanym rozstrzygnięciu model współpracy administratora z procesorem był nieskuteczny. Brak zrozumienia przez administratora roli, jaką on pełni w relacji z podmiotem przetwarzającym, doprowadziły do naruszenia ochrony danych osobowych. Krajowa Szkoła Sądownictwa i Prokuratury zarówno przed naruszeniem

[9] *Ibidem*, s. 640.

ochrony danych, jak i po jego stwierdzeniu nie miała pełnej świadomości, jak kształtują się prawa i obowiązki pomiędzy nią a podmiotem przetwarzającym.

Podmiot przetwarzający wskazywał, że kilkukrotnie strony prowadziły korespondencję mającą na celu jasne wskazanie kwestii działań podmiotu przetwarzającego nad systemem hostującym, a obszarem danych i aplikacji klienta, którym podmiot przetwarzający się nie zajmował, i do którego wglądu nie posiadał. Z okoliczności sprawy wynikało, że pracownicy KSSiP zarówno przed naruszeniem ochrony danych, jak i po jego stwierdzeniu, nie mieli pełnej świadomości, jak kształtują się prawa i obowiązki pomiędzy administratorem a podmiotem przetwarzającym. Administrator wielokrotnie oczekiwał wykonywania zadań wykraczających poza zakres tej umowy. Podmiot przetwarzający nie znał struktury i konfiguracji autorskich aplikacji instalowanych przez administratora na tych zasobach, w tym nie miał obowiązku, bez wiedzy administratora i na udokumentowane jego polecenie, prowadzenia czynności konfiguracyjnych w zakresie dostępu do katalogów czy baz danych, z których aplikacje te korzystają. Zgodnie z istotą świadczonej usługi, administrator dysponuje pełną wiedzą o tym, jakie dane osobowe przetwarza, w jaki sposób, w jakiej lokalizacji (w ramach udostępnionych zasobów) i za pomocą jakich narzędzi. Jedynie na udokumentowane polecenie administratora podmiot przetwarzający może dokonywać ingerencji w zakresie wynikającym z charakteru świadczonych usług i zawartej umowy.

Kolejnym zagadnieniem, na jakie zwrócił uwagę Prezes UODO, jest język komunikacji między stronami umowy powierzenia. Administrator posługiwał się określoną nomenklaturą i oznaczeniami (np. baza danych PROD PS, „stara" platforma szkoleniowa, platforma e-learning, baza szkoleniowa), która dla dostawcy usług hostingowych, z uwagi na charakter świadczonej usługi, w opinii procesora, była nieprawidłowa i niezrozumiała. Rodziło to problemy interpretacyjne i oznaczało oczekiwanie administratora do wykonywania przez podmiot przetwarzający czynności poza określone w umowie. Przepisy rozporządzenia 2016/679, jak wskazano w komentowanej decyzji, dają pewną swobodę w zakresie kształtowania relacji między administratorem a podmiotem przetwarzającym. Należy więc oczekiwać, że administrator wypracuje model współpracy z podmiotem przetwarzającym, który będzie zapewniał przetwarzanie zgodne z przepisami o ochronie danych osobowych, a w szczególności będzie umożliwiał realizację zasady rozliczalności wyrażoną w art. 5 ust. 2 RODO. O ile zatem strony umowy ustaliły kanały komunikacji oraz wyznaczyły osoby wykonujące czynności związane z realizacją umowy, o tyle osoby wskazane przez KSSiP nadal nie miały świadomości, jak kształtują się prawa i obowiązki pomiędzy administratorem a podmiotem przetwarzającym. Uprawniona jest więc konstatacja, że osoby wyznaczone do kontaktu z podmiotem przetwarzającym, powinny zostać uprzednio poinformowane o zakresie usług świadczonych przez podmiot przetwarzający i o obowiązkach leżących po stronie administratora. Treść porozumienia natomiast nie powinna budzić wątpliwości, a zatem strony powinny używać i posługiwać się pojęciami zrozumiałymi dla obu stron, co może skutecznie minimalizować ryzyko naruszenia ochrony danych osobowych.

Brak współpracy na poziomie poprawnej komunikacji, błędne polecenia wydawane podmiotowi przetwarzającemu, fałszywa ocena ról, zadań i zakresu obowiązków określonych w umowie powierzenia prowadzą w konsekwencji do braku właściwej, odpowiedzialnej weryfikacji tego, czy zlecona czynność została wykonana, i czy została wykonana prawidłowo. Trzeba zaznaczyć, że administrator jest inicjatorem podejmowanych działań jako podmiot decydujący o celach i sposobach przetwarzania. Zgodnie z umową o świadczenie usług, to jemu zostało udostępnione środowisko, w którym tego przetwarzania dokonuje, i to administrator w pierwszej kolejności odpowiada za bezpieczeństwo przetwarzanych danych, a jak wynika z umowy, w razie konieczności korzysta z pomocy podmiotu przetwarzającego.

5. Odpowiedzialność podmiotu przetwarzającego

Całościowa ocena stanu faktycznego analizowanej sprawy wymaga zrecenzowania działań podmiotu przetwarzającego, w kontekście ich wpływu na naruszenie ochrony danych osobowych. W glosowanej decyzji, zdaniem organu nadzorczego, podmiot przetwarzający wypełniał obowiązki wynikające z umowy powierzenia i umowy głównej, a także stosował przyjęte przez siebie środki organizacyjne, mające na celu zapewnienie bezpieczeństwo systemów informatycznych. To administrator nie podjął się analizy, czy wskazując podmiotowi przetwarzającemu miejsce do wykonania kopii zapasowej bazy danych, nie naraża danych osobowych w niej zawartych na naruszenie ich poufności; nie poinformował podmiotu przetwarzającego o istotności podejmowanych działań pod kątem ochrony danych osobowych.

Prezes UODO uznał, że co prawda z art. 28 ust. 3 lit. f RODO wynika obowiązek podmiotu przetwarzającego wspierania administratora w wywiązywaniu się z obowiązków określonych w art. 32–36 tego rozporządzenia, jednak opatrzony jest on warunkami, które należy za każdym razem uwzględnić, tj. charakter przetwarzania oraz dostępne podmiotowi przetwarzającemu informacje. W umowie powierzenia określono, że podmiot przetwarzający pomaga w tym zakresie „w miarę możliwości". Krajowa Szkoła Sądownictwa i Prokuratury jednak w zleceniach nie zwróciła się z prośbą o uprzednie zweryfikowanie bezpieczeństwa wskazanej lokalizacji oraz nie poinformowała podmiotu przetwarzającego o okolicznościach prowadzonych czynności, tj. prowadzonej migracji, której przedmiotem są dane osobowe, oraz że proces ten musi zapewniać ich odpowiednie bezpieczeństwo. Podmiot przetwarzający, nie dysponując takimi informacjami, nie może za każdym razem domyślać się charakteru wykonywanej czynności i każdą operację wykonywać, uprzednio weryfikując, czy ma do czynienia z danymi osobowymi, oraz czy środowisko i zasoby, udostępnione zgodnie z umową administratorowi, są prawidłowo i bezpiecznie skonfigurowane. Kontekst prowadzonych działań był znany wyłącznie administratorowi, i to na nim spoczywa bezwzględny obowiązek upewnienia się, czy prowadzone czynności nie będą narażały osób, których przetwarzanie danych dotyczy, na naruszenie ich praw lub wolności.

Prezes UODO uznał, że za całość operacji związanych z wykonaniem kopii bazy danych i przekazaniem jej do serwera docelowego, odpowiedzialny był KSSiP, podmiot przetwarzający nie był angażowany ani informowany o charakterze podejmowanych czynności, i realizował zadania wynikające z umowy o świadczenie usług, np. czynności w ramach wsparcia technicznego. Nie dopatrzył się również okoliczności, które pozwoliłyby stwierdzić, że procesor nie zapewniał wystarczających gwarancji dla bezpieczeństwa danych osobowych oraz nie udostępniał administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 rozporządzenia 2016/679 bądź uniemożliwiał administratorowi przeprowadzanie audytów, w tym inspekcji. W konsekwencji, Prezes UODO umorzył postępowanie administracyjne wobec podmiotu przetwarzającego.

Uważam, że kwestia umorzenia postępowania wobec podmiotu przetwarzającego powinna być jednak skomentowana. W ocenie Prezesa UODO, procesor wypełniał obowiązki wynikające z umowy powierzenia i umowy głównej, a także stosował przyjęte przez siebie środki organizacyjne mające na celu zapewnienie bezpieczeństwa systemów informatycznych. Zdaniem Prezesa UODO, to administrator nie podjął się analizy, czy wskazując podmiotowi przetwarzającemu miejsce do wykonania kopii zapasowej bazy danych, nie naraża danych osobowych w niej zawartych na naruszenie ich poufności. Warto jednak zwrócić uwagę, że podmiot przetwarzający powinien pomagać administratorowi także w realizacji obowiązków wynikających z art. 32–36 RODO, a odnoszących się do: bezpieczeństwa przetwarzania, zgłaszania naruszeń ochrony danych organowi nadzorczemu, zawiadamiania osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, oceny skutków dla ochrony danych oraz uprzednich konsultacji. Jak wskazuje się w literaturze, ustalenie zasad partycypacji podmiotu przetwarzającego w realizacji tych zadań ma szczególnie istotne znaczenie z perspektywy administratora, rozliczanego przez organ nadzorczy z ich realizacji. Słusznie podkreśla się, że ze zobowiązaniem podmiotu przetwarzającego do wsparcia w wykonywaniu wskazanych powyżej obowiązków współgrają normy adresowane bezpośrednio do tego podmiotu, mieszczące się w art. 32–36 RODO. W konsekwencji, poza nałożeniem na podmiot przetwarzający obowiązku zastosowania odpowiednich środków bezpieczeństwa wynikającego z art. 32 RODO, wskazać należy w tym aspekcie na zobowiązanie podmiotu przetwarzającego do obowiązków implikujących konieczność przeprowadzenia kompleksowej, rzetelnej i wyczerpującej analizy procesów przetwarzania i całego kontekstu, w jakim to przetwarzanie się odbywa. Do takiego całościowego zbadania danego przetwarzania niezbędne jest uzyskanie przez administratora szeregu informacji, w tym m.in. w zakresie stosowanych środków bezpieczeństwa, certyfikacji w określonych obszarach, zidentyfikowanych po stronie podmiotu przetwarzającego zagrożeń i ryzyk związanych z przetwarzaniem[10]. O ile zatem należy zgodzić się ze stanowiskiem Prezesa UODO, że odpowiedzialność za wyciek

[10] K. Witkowska-Nowakowska, *Komentarz do art. 28 RODO*…, s. 642–643, M. Sakowska-Baryła, komentarz do art. 28 [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. *eadem*, Warszawa 2018, s. 327–328.

ponosi uczelnia, trudno podzielać opinię, że procesor, który zarządzał zasobami serwerowymi, nie ponosi żadnej winy, a więc także odpowiedzialności za wyciek danych. W przedstawionej sprawie działania podmiotu przetwarzającego określić można jako bierne zachowanie. Wykonywał on działania ograniczone do poleceń administratora, odmawiając wykonania polecenia lub żądając jego doprecyzowania, w sytuacji gdy były one niejasne albo nieprecyzyjne. W mojej ocenie, takie zaangażowanie podmiotu przetwarzającego, w tej konkretnie sprawie, nie spełniało obowiązku udzielania pomocy, do którego zobowiązany jest podmiot przetwarzający na mocy art. 28 ust. 3 lit. f RODO. W doktrynie wskazuje się, że naruszenie obowiązku pomocy administratorowi nie musi prowadzić do naruszenia obowiązku realizacji praw podmiotów danych przez administratora, ale wówczas, gdy administrator będzie mógł zrealizować te obowiązki nawet przy braku pomocy procesora[11]. W tym określonym przypadku działanie administratora doprowadziło jednak do naruszenia bezpieczeństwa danych osobowych, należałoby zatem podjąć próbę odpowiedzi na pytanie, czy do naruszenia doszłoby, gdyby procesor w sposób bardziej aktywny udzielał pomocy administratorowi oraz czy nie wpływało to na rozmiar i skalę naruszenia. Jednak, trzeba przypomnieć, że administrator dokonał wyboru profesjonalnego podmiotu (z zachowaniem formalnych wymogów), miał więc słusznie prawo oczekiwać od niego wsparcia na wysokim poziomie fachowości. Warto również zwrócić uwagę na to, że przepis ten (art. 28 ust. 3 lit. f RODO) uzależnia pomoc udzielną administratorowi od charakteru przetwarzania i dostępnych informacji, jakie posiada procesor. Prawodawca europejski nie ogranicza zakresu pomocy do informacji uzyskanych od administratora. Gdyby jednak nawet rozumienie „dostępnych informacji" zawęzić tylko do tych otrzymywanych od administratora, to uważam, że w tej sprawie należy przyjąć, że podmiot przetwarzający na podstawie nieprecyzyjnych komunikatów, jakie otrzymywał od pracowników administratora miał podstawę do uznania, że po stronie administratora występują problemy ze zrozumieniem jego roli, uprawnień i możliwości działania. To już powinno uruchomić po stronie procesora decyzję o wsparciu KSSiP w zakresie zapewnienia bezpieczeństwa danych osobowych przetwarzanych w ramach usługi hostingowej. Dodatkowo, umorzenie postępowania wobec podmiotu przetwarzającego może być niezrozumiałe również z tego powodu, że pracownik tego podmiotu otrzymał zarzuty karne związane z nielegalnym udostępnieniem danych osobowych z bazy danych KSSiP. Moim zdaniem, w tych warunkach nie sposób uznać, że procesor, przetwarzając dane z upoważnienia KSSiP, nie naruszył obowiązków podmiotu przetwarzającego, do jakich obowiązany jest mocą przepisów RODO[12].

[11] M. Gumularz, P. Kozik, *Odpowiedzialność administracyjna przy powierzaniu*, ABI Ekspert 2017, nr 4, s. 11.

[12] Poza zakresem rozważań pozostaje oczywiście problematyka ewentualnej odpowiedzialności cywilnej procesora wobec administratora danych.

6. Uwagi końcowe

Na koniec warto zaznaczyć, że analizowana decyzja jest kolejną świadczącą o tym, że przyczyn nałożenia przez organ nadzorczy administracyjnej kary finansowej, jest zwykle co najmniej kilka. Administrator w tej sprawie popełnił szereg błędów: nie uwzględnił zasady *privacy by design* – poprzez brak odpowiedniego zabezpieczenia danych osobowych już w fazie projektowania, przyjął nieprawidłową metodę współpracy z podmiotem przetwarzającym, nie wdrożył prawidłowych technicznych środków zabezpieczeń i nie uwzględnił ryzyka. Szczególną uwagę należy także zwrócić na niezrealizowanie przez administratora obowiązku kontroli procesu przetwarzania danych w całym ich cyklu. Obowiązków tych nie można sprowadzać wyłącznie do formalnego wypełniania zadań wynikających z przepisów, przygotowania dokumentacji, zawarcia umowy powierzenia, udostępnienia danych czy wprowadzenie systemów i certyfikowanych rozwiązań technicznych. Administrator musi wziąć odpowiedzialność za proces przetwarzania danych, oceniając konkretną sytuację z uwzględnieniem wszystkich okoliczności i relacji zachodzących między wszystkimi uczestnikami przetwarzania. Oczywiście nie każda, nawet błędna decyzja administratora musi prowadzić do naruszenia bezpieczeństwa danych i powodować odpowiedzialność administratora, jednak w rezultacie na poziom bezpieczeństwa danych osobowych zawsze w efekcie największy wpływ mają decyzje administratora. Dlatego Prezes Urzędu Ochrony Danych Osobowych w swoich rozstrzygnięciach wspomina nie tylko o konieczności posiadania procedur, ale też potrzebie rzeczywistego testowania i weryfikacji bezpieczeństwa, bo jest to niezbędne z punktu widzenia realizacji zasady rozliczalności.

Literatura

Gumularz M., Kozik P., *Odpowiedzialność administracyjna przy powierzaniu*, ABI Ekspert 2017, nr 4, s. 11.

Krzysztofek M., *Warunki dopuszczalności powierzenia – lista kontrolna*, ABI Ekspert 2017, nr 4, s. 19.

Sakowska-Baryła M., komentarz do art. 28 [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. *eadem*, Warszawa 2018.

Witkowska-Nowakowska K., *Komentarz do art. 28 RODO* [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018.

Streszczenie

Edyta Bielak-Jomaa

Realizacja obowiązków administratora danych w związku z powierzeniem przetwarzania danych osobowych, odpowiedzialność podmiotu przetwarzającego oraz model współpracy między tymi podmiotami

Przedstawiona glosa dotyczy decyzji Prezesa Urzędu Ochrony Danych Osobowych nakładającej karę finansową na administratora – Krajową Szkołę Sądownictwa i Prokuratury. Administrator ukarany został za nieprawidłową realizację ciążących na nim obowiązków związanych z powierzeniem przetwarzania danych osobowych, odpowiedzialności podmiotu przetwarzającego oraz modelu współpracy między administratorem a podmiotem przetwarzającym. Odpowiedzialny administrator powinien określić poziom ryzyka, jakie wiąże się z przetwarzaniem danych osobowych, aby zastosować środki organizacyjne i techniczne adekwatne do tego ryzyka. Analiza ryzyka powinna mieć miejsce także przy wyborze podmiotu przetwarzającego, oraz określaniu warunków umowy powierzenia. Z jej treści powinny wynikać także zasady i zakres współpracy, która ma określać wzajemne relacje, obowiązki i odpowiedzialność stron umowy powierzenia. Dla prawidłowej realizacji umowy znaczenie ma dodatkowo określenie kanałów komunikacyjnych między administratorem i podmiotem przetwarzającym.

Słowa kluczowe: administracyjna kara finansowa; administrator; przetwarzający; przetwarzanie danych osobowych; analiza ryzyka; umowa powierzenia przetwarzania; RODO.

Summary

Edyta Bielak-Jomaa

Fulfillment of the Obligations of Data Controller in Connection with the Entrustment of Personal Data Processing, the Responsibility of the Processor and the Model of Cooperation Between These Entities Decision of the President of the Personal Data Protection Office of 11 February 2021, DKN.5130.2024.2020

This commentary concerns the decision of the President of the Personal Data Protection Office imposing a financial penalty on the controller – the National School of Judiciary and Public Prosecution. The controller was fined for incorrect performance of its duties related to the outsourcing of personal data processing, the responsibility of the processor and the model of cooperation between the controller and the processor. The controller in charge should determine the level of risk involved in processing of personal data in order to apply organisational and technical measures appropriate to those risks. The risk analysis should also take place when choosing the processor and defining the conditions of the entrustment agreement. The content of the agreement should also determine the principles and scope of cooperation i.e. mutual relations, duties and responsibilities of the parties to the entrustment agreement. For the proper implementation of the agreement it is also important to determine the communication channels between the controller and the processor.

Keywords: administrative fine; controller; processor; personal data processing; risk analysis; controller-processor agreement; GDPR.