Naruszenia bezpieczeństwa danych osobowych przez firmy kurierskie

Decyzja Prezesa Urzędu Ochrony Danych Osobowych
z dnia 22 kwietnia 2021 r., DKN.5130.3114.2020

W ocenie Prezesa UODO, Spółka w sposób niewystarczający dokonywała oceny skuteczności środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania danych osobowych znajdujących się na dokumentach dostarczanych klientom Spółki za pośrednictwem podmiotu świadczącego usługi kurierskie, co stanowi naruszenie art. 24 ust. 1 oraz art. 32 ust. 1 i 2 rozporządzenia 2016/679. (…) Spółka pomimo wdrożenia polityki oraz procedur ochrony danych osobowych związanych ze zgłaszaniem naruszeń, a także zawarcia umowy powierzenia przetwarzania danych osobowych z podmiotem przetwarzającym, nie wypracowała odpowiednich mechanizmów mających na celu kontrolę realizacji przez podmiot przetwarzający swoich zobowiązań.

Paweł Litwiński
Uniwersytet SWPS
litwinski@bartalitwinski.pl
ORCID: 0000-0002-4293-1917

https://doi.org/10.26881/gsp.2021.4.12

Decyzją z dnia 22 kwietnia 2021 r. (Decyzja) Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) stwierdził naruszenie przez Cyfrowy Polsat S.A. z siedzibą w Warszawie (Spółka) art. 24 ust. 1 i art. 32 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE[1] (ogólne rozporządzenie o ochronie danych) (RODO) i nałożył na Spółkę administracyjną karę pieniężną w wysokości 1.136.975 zł.

[1] Dz. Urz. UE L 119 z 2016 r., s. 1, Dz. Urz. UE L 127 z 2018 r., s. 2 oraz Dz. Urz. UE L 74 z 2021 r., s. 35.

Stan faktyczny sprawy

Decyzja została wydana w stosunkowo prostym stanie faktycznym, który jednak – jak się wydaje – ustalony został przez Prezesa UODO w sposób wybiórczy, z pominięciem istotnych okoliczności, o czym dalej. Otóż Spółka korzysta z usług podmiotu świadczącego usługi kurierskie, który w tym zakresie pełni rolę podmiotu przetwarzającego dane osobowe (tak jest traktowany przez Spółkę, a ta kwalifikacja nie została w żaden sposób zakwestionowana przez Prezesa UODO). W toku świadczonych usług kurierskich dochodziło do naruszeń bezpieczeństwa danych osobowych, polegających na „utracie przez kurierów dokumentów zawierających dane osobowe klientów lub na wydaniu przez kurierów niewłaściwej osobie dokumentów zawierających dane osobowe w postaci: imienia i nazwiska, adresu zamieszkania lub pobytu, numeru PESEL, adresu e-mail, serii i numeru dowodu osobistego bądź innego dokumentu tożsamości, numeru telefonu oraz danych dotyczących łączących strony umów"[2]. W stosunku do tych naruszeń Spółka wykonywała obowiązki zgłaszania naruszeń oraz zawiadamiania o naruszeniach osób, których dane dotyczą. Analiza informacji zawartych w zgłoszeniach oraz materiału dowodowego zebranego w postępowaniu pozwoliła Prezesowi UODO na przyjęcie, że „Spółka w sposób niewystarczający dokonywała oceny skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych znajdujących się na dokumentach dostarczanych klientom Spółki za pośrednictwem podmiotu świadczącego usługi kurierskie, co stanowi naruszenie art. 24 ust. 1 oraz art. 32 ust. 1 i 2 [RODO]"[3]. Innymi słowy, zdaniem Prezesa UODO, choć naruszeń dopuszczała się firma kurierska, to na Spółce ciążył prawny obowiązek zapewnienia bezpieczeństwa danych osobowych przetwarzanych w imieniu Spółki przez firmę kurierską.

Status firmy kurierskiej w świetle przepisów o ochronie danych osobowych

Analizę Decyzji wypada rozpocząć od najistotniejszego problemu, tj. od prawidłowej kwalifikacji prawnej firmy kurierskiej z perspektywy przepisów o ochronie danych osobowych. Istnieją w tym zakresie dwie możliwości: uznanie firmy kurierskiej za administratora danych osobowych albo za podmiot przetwarzający dane osobowe. Kwalifikacji tej trzeba przy tym dokonać oddzielnie w stosunku do trzech grup danych osobowych: danych osobowych nadawcy, danych osobowych odbiorcy oraz danych osobowych, które mogą być zawarte w przemieszczanej przesyłce.

[2] Decyzja, s. 2.
[3] *Ibidem*, s. 11.

Do rozstrzygnięcia sformułowanego wyżej problemu kluczowy wydaje się status firmy kurierskiej z perspektywy przepisów ustawy – Prawo pocztowe[4]. Otóż firmy kurierskie, którym przysługuje status operatora pocztowego w rozumieniu art. 3 pkt 12 u.p.p., dysponują ustawowym, bo wynikającym z art. 42 tejże ustawy, tytułem prawnym do przetwarzania danych osobowych przekazywanych w przesyłkach pocztowych, a także danych osobowych nadawcy i odbiorcy przesyłki. W tym zakresie nie działają więc w imieniu nadawcy przesyłki, a w imieniu własnym[5], nie sposób więc przyznać im statusu podmiotu przetwarzającego dane osobowe. Oznacza to, że podmioty świadczące usługi kurierskie powinny zostać uznane za administratorów danych osobowych, z pewnością w zakresie danych osobowych nadawców i odbiorców przesyłek – o czym w dalszej części glosy.

Mimo tego, że stwierdzenie takie nie pada wprost, a może być wyprowadzane jedynie z czynionych przez organ nadzorczy rozważań dotyczących podstawy przetwarzania danych osobowych, status administratora danych osobowych operatora pocztowego w stosunku do danych osobowych odbiorcy przesyłki został potwierdzony przez Generalnego Inspektora Ochrony Danych Osobowych (GIODO) w decyzji z dnia 2 lipca 2013 r.[6] Odpowiadając natomiast na pytanie[7] dotyczące zadań Inspektora Ochrony Danych Osobowych (IODO), Prezes UODO stwierdził wprost, że „Poczta Polska i inni operatorzy pocztowi w związku z wykonywaniem usług pocztowych są administratorami danych osobowych nadawców i adresatów przesyłek". W tym samym wpisie uznano jednak, że przekazanie do odkażania (fumigacji) pudeł zawierających dokumenty w sytuacji, gdy pudła są zamknięte, zapieczętowane i nie są na żadnym etapie odkażania otwierane przez pracowników zleceniobiorcy, należy uznać za przypadek powierzenia przetwarzania danych, co wydaje się stanowiskiem co najmniej kontrowersyjnym, jako że w takiej sytuacji ma się do czynienia wyłącznie z operacją wykonywaną na rzeczy (pudło), bez dostępu do danych osobowych i bez operacji wykonywanych na tychże danych. Z innego założenia, jak się wydaje, wyszedł w tym zakresie bawarski organ nadzorczy, który uznał, że czyszczenie strojów roboczych, mających plakietkę z nazwiskiem, nie stanowi operacji powierzenia przetwarzania danych osobowych zawartych na tejże plakietce[8].

---

[4] Ustawa z dnia 23 listopada 2012 r. – Prawo pocztowe (tekst jedn.: Dz. U. z 2020 r., poz. 1041 ze zm.; dalej: u.p.p.).

[5] Działanie w imieniu administratora danych jest istotną cechą podmiotu przetwarzającego – dokonuje on czynności przetwarzania „w imieniu administratora", a więc sam nie decyduje o celu i sposobach przetwarzania, lecz realizuje cele wyznaczone przez administratora (zob. P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 124).

[6] DOLiS/DEC-708/13/41776; interesujące jest przy tym, że podstawą przetwarzania danych osobowych nadawcy i odbiorcy przesyłki przez operatora pocztowego jest w ocenie organu nadzorczego realizacja przez operatora pocztowego własnego prawnie uzasadnionego interesu związanego z doręczaniem przesyłek.

[7] Wpis na stronie https://uodo.gov.pl/pl/225/1467 z dnia 24 marca 2020 r. [dostęp: 22.11.2021].

[8] Bayerisches Landesamt für Datenschutzaufsicht, *FAQ zur DS-GVO*, https://www.lda.bayern.de [dostęp: 22.11.2021].

Jednocześnie jednak można odnaleźć i takie decyzje organu nadzorczego, w których firma kurierska uznana została za przetwarzającego dane osobowe na zlecenie nadawcy, który uznany został za administratora danych. W szczególności w decyzji z 21 września 2011 r.[9] stwierdzono wprost, że „spółka miała prawo do powierzenia w drodze umowy, na podstawie art. 31 ustawy [o ochronie danych osobowych z 1997 r.], dane osobowe do przetwarzania firmie kurierskiej w celu wykonywania usług miejskich i krajowych w zakresie przewożenia przesyłek". Status firm kurierskich w kontekście przetwarzania przez nie danych osobowych na potrzeby świadczenia usług kurierskich jest więc w świetle Decyzji i stanowisk organu nadzorczego wyjątkowo niejasny, a znajdujące się w obrocie prawnym rozstrzygnięcia są ze sobą sprzeczne. Co dodatkowo ważne, można sformułować istotne wątpliwości co do tego, czy przemieszczenie przesyłki zawierającej dane osobowe z punktu A do punktu B, w zamkniętej kopercie, co do której istnieje obowiązek zachowania tajemnicy korespondencji i tajemnicy pocztowej, stanowi w ogóle przetwarzanie danych osobowych zawartych w tejże przesyłce. Przetwarzaniem danych osobowych są bowiem operacje wykonywane na danych osobowych, a nie na nośnikach tychże danych. Jeżeli więc usługa polega na przemieszczeniu nośnika danych osobowych, a w świetle art. 42 u.p.p. operator pocztowy nie może się zapoznać z treścią tychże danych osobowych[10], wówczas nie sposób przyjąć, że dochodzi do przetwarzania przez niego danych osobowych. Zakaz zapoznawania się przez operatora pocztowego z danymi osobowymi zawartymi w przesyłce powoduje także, że można argumentować, iż w świetle wyroku TSUE z dnia 19 października 2016 r., C-582/14, ws. *Patrick Breyer przeciwko Bundesrepublik Deutschland*, te informacje dla operatora pocztowego nie mogą być w ogóle uznane za informacje o charakterze danych osobowych. Trybunał przyjął bowiem, że informacja nie ma charakteru danych osobowych m.in. wtedy, gdy identyfikacja osoby fizycznej jest „zakazana prawem"[11], a z taką właśnie sytuacją ma się do czynienia na gruncie działalności operatorów pocztowych.

O ile więc usługa świadczona przez firmę kurierską polegała wyłącznie na doręczeniu przesyłki do adresata, a firmie tej przysługiwał status operatora pocztowego, o tyle to ona pełniła rolę administratora danych osobowych w stosunku do danych nadawcy i odbiorcy, nie zaś ukarana Spółka. W stosunku do danych osobowych przekazywanych w przesyłkach pocztowych firma ta powinna zostać także uznana za administratora danych, albo wręcz należałoby przyjąć, że nie przetwarza ona tych danych – z pewnością jednak nie dochodziłoby w ten sposób do powierzenia

[9] DOLiS/DEC-819/11.

[10] W literaturze podnosi się, że przypadki kontroli i zatrzymywania korespondencji, a więc zapoznania się z treścią korespondencji, są określone każdorazowo we właściwych przepisach ustawowych jako przepisy odrębne pozwalające na przetwarzanie danych lub przepisów stanowiących tajemnicę pocztową – zob. M. Gaj, T. Laprus-Bałuka, A. Zaborowska, *Prawo pocztowe. Komentarz*, Warszawa 2017, s. 153.

[11] Pkt 46 uzasadnienia wyroku ws. C-582/14; zob. szerzej na ten temat P. Litwiński, *Pojęcie danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych – glosa do wyroku Trybunału Sprawiedliwości z 19.10.2016 r. w sprawie C-582/14 Patrick Breyer*, EPS 2017, nr 5.

przetwarzania danych osobowych[12]. Nie wiadomo jednak, czy na gruncie Decyzji tak właśnie przedstawiał się stan faktyczny, ponieważ brak w niej jakichkolwiek informacji na ten temat, a pojęcie „operatora pocztowego" pojawia się w Decyzji jeden raz, w następującym kontekście: „Nawiasem mówiąc, przypadki zgłaszanych naruszeń ochrony danych osobowych związanych z nieprawidłowościami po stronie operatorów pocztowych nie należą do wyjątkowych w praktyce UODO, do wyjątków należą jednak sytuacje, w których administrator nie podejmuje natychmiastowych działań związanych z zaginięciem bądź nieprawidłowym doręczeniem nadanych przez siebie przesyłek zawierających dane osobowe klientów"[13]. Mogłoby to wskazywać na traktowanie firmy kurierskiej przez Prezesa UODO jako operatora pocztowego, jednakże zamiast tego Prezes UODO przyjmuje – w ślad za stroną – że firmie kurierskiej przysługuje status podmiotu przetwarzającego dane osobowe na zlecenie Spółki. Ważne przy tym jest przywołane już wcześniej stwierdzenie zawarte w uzasadnieniu Decyzji, że naruszenia bezpieczeństwa danych osobowych polegały na utracie przez kurierów „dokumentów zawierających dane osobowe klientów" oraz na „wydaniu przez kurierów niewłaściwej osobie dokumentów zawierających dane osobowe". Jak się więc wydaje, naruszenia te dotyczyły danych osobowych zawartych w przesyłkach.

Praktyka rynkowa wskazuje na to, że istnieją przypadki, w których firma kurierska będzie świadczyła usługę przetwarzania danych osobowych na zlecenie nadawcy. Będą to usługi związane z dostarczaniem umów i innych dokumentów od nadawcy do adresata, a polegające w szczególności na weryfikacji tożsamości adresata, który w obecności kuriera podpisuje np. umowę z nadawcą, czy na uzupełnieniu niektórych danych osobowych adresata na dokumentach, które następnie są zwracane do nadawcy. Co więcej, jak wskazuje się w literaturze, część firm kurierskich zastrzega w umowach z klientami, że przejmując od nich przesyłki, działa jako administrator danych, inne firmy z kolei – że jako podmiot przetwarzający[14]. Tymczasem, na gruncie Decyzji brak jest jakichkolwiek rozważań na ten temat, a zamiast tego w sposób automatyczny przyjęto, że firma kurierska działa jako przetwarzający dane osobowe na zlecenie ukaranej Spółki, nie uzasadniając tego w żaden sposób, w szczególności nie odnosząc się do tego, jakie usługi świadczone są przez firmę kurierską. Jednocześnie status podmiotów uczestniczących w procesie przetwarzania danych osobowych jest kluczowy z punktu widzenia zakresu ciążących na nich obowiązków, a także – a może przede wszystkim – z perspektywy nałożenia kary za naruszenie tychże. Dość powiedzieć, że jeżeli na gruncie omawianej decyzji status administratora danych przysługiwał firmie kurierskiej, wówczas nałożenie kary pieniężnej na ukaraną Spółkę pozbawione byłoby jakichkolwiek podstaw prawnych – nie można jednak tej tezy zweryfikować ze względu na bardzo istotne braki w zakresie uzasadnienia Decyzji, które wynikają, jak się wydaje, z błędów poczynionych na gruncie postępowania dowodowego w sprawie.

[12] Podobnie Bayerisches Landesamt für Datenschutzaufsicht, FAQ zur DS-GVO, https://www.lda.bayern.de [dostęp: 22.11.2021].

[13] Decyzja, s. 23.

[14] J. Styczyński, *Nierejestrowane przesyłki kontrowersyjne w świetle RODO*, „Dziennik Gazeta Prawna" z dnia 2 lipca 2019 r.

Nie można także tej informacji zweryfikować, korzystając z powszechnie dostępnego rejestru operatorów pocztowych, prowadzonego przez Prezesa Urzędu Komunikacji Elektronicznej[15], ponieważ w Decyzji nie pada nazwa firmy kurierskiej, która świadczyła usługi na rzecz ukaranej Spółki. Jest to o tyle niezrozumiałe, że Prezes UODO takimi informacjami dysponował, jako że w aktach sprawy, jak wynika z uzasadnienia Decyzji, znajduje się umowa zawarta przez Spółkę z firmą kurierską[16].

Ryzyko i jego analiza

Istotne fragmenty uzasadnienia Decyzji poświęcone są temu, jakie ryzyko dla praw i wolności osób, których dane dotyczą, powstało w wyniku naruszeń bezpieczeństwa danych osobowych zaistniałych w wyniku działań firmy kurierskiej. Sprowadzić je można do następującego fragmentu pochodzącego z uzasadnienia: „Prezes UODO uznał, że naruszenie poufności danych, w szczególności danych dotyczących łącznie imienia i nazwiska, adresu zamieszkania lub pobytu, numeru PESEL, serii i numeru dowodu osobistego bądź innego dokumentu tożsamości, numeru telefonu oraz innych kategorii danych dotyczących łączących strony umów (np. ID kontraktu, numer umowy, numer dokumentu, numer sprzętowy, numer i kwota faktury VAT, numer konta do wpłat), powoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w związku z czym konieczne jest zawiadomienie osoby, której dane dotyczą, o naruszeniu jej danych osobowych”[17]. Takie stanowisko wpisuje się w linię orzeczniczą Prezesa UODO, w której zakłada się konsekwentne uznawanie numeru PESEL za daną osobową o „szczególnym charakterze”[18], co przekłada się na przyjmowanie, że naruszenie poufności danych osobowych obejmujące numer PESEL powoduje powstanie wysokiego ryzyka dla praw i wolności osób, których dane dotyczą. Jako przykład tego rodzaju praktyki można wskazać wcześniejszą decyzję Prezesa UODO o nałożeniu na Towarzystwo Ubezpieczeń i Reasekuracji Warta S.A. administracyjnej kary pieniężnej[19] w wysokości 85.588 zł w związku z obowiązkami dotyczącymi zgłaszania naruszeń bezpieczeństw danych osobowych, w której przyjęto, że „(…) z uwagi na to, że wskazane naruszenie poufności danych dotyczy numerów PESEL wraz z imionami i nazwiskami, adresami zamieszkania, numerami telefonów oraz adresami poczty elektronicznej, to należy uznać, że może ono wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych”.

Poświęcenie tej kwestii kilku stron uzasadnienia decyzji wydaje się co najmniej niecelowe, jako że ukarana Spółka tak właśnie przyjmowała, dokonując zgłoszeń naruszeń

[15] Rejestr dostępny: https://bip.uke.gov.pl/rop/rejestr-operatorow-pocztowych [dostęp: 22.11.2021].
[16] Decyzja, s. 6.
[17] *Ibidem*, s. 15.
[18] Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2019, s. 165, uodo.gov.pl [dostęp: 22.11.2021].
[19] Decyzja z dnia 9 grudnia 2020 r., DKN.5131.5.2020.

bezpieczeństwa danych osobowych, co wprost przyznaje Prezes UODO w uzasadnieniu decyzji, stwierdzając, iż „Spółka wyjaśniła, że mimo to, że uzyskany wynik analizy naruszeń pozwolił określić poziom dotkliwości naruszenia ochrony danych dla osób, których dane dotyczą, jako „niski", Spółka notyfikowała jednak naruszenia, ze względu na wytyczne Prezesa Urzędu Ochrony Danych Osobowych przekazane Spółce w wystąpieniu z dnia (…) września 2018 r. (…), wskazujące na konieczność notyfikowania zdarzeń, które obejmowały nr PESEL, określając ryzyko jako „wysokie"[20]. Co jednak najistotniejsze, ani na gruncie analizowanej decyzji, ani też w treści wcześniejszych dokumentów, Prezes UODO w żaden sposób nie uzasadnia swojego stanowiska o „szczególnym charakterze" numeru PESEL i o wysokim ryzyku, jakie generują naruszenia bezpieczeństwa danych osobowych obejmujące ten numer.

Kluczowe z punktu widzenia postępowania po stwierdzeniu naruszenia bezpieczeństwa danych osobowych jest określenie poziomu ryzyka naruszenia praw i wolności osób fizycznych w wyniku incydentu. Istnieje wiele sposobów postępowania w celu ustalenia poziomu tego ryzyka. W każdym przypadku jednak, zgodnie z zaleceniami zawartymi w motywach 75 i 76 preambuły do RODO, podczas oceny ryzyka zasadniczo należy wziąć pod uwagę zarówno prawdopodobieństwo, jak i powagę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, a ryzyko naruszenia należy oszacować na podstawie obiektywnej oceny. Badając naruszenie, rozpatruje się więc w ujęciu ogólnym prawdopodobieństwo materializacji zagrożenia oraz szkody dla osób, których dane dotyczą, jakie mogą z niego wyniknąć[21]. W tym kontekście stanowisko zajęte przez Prezesa UODO w glosowanej decyzji, zgodnie z którym „dla oceny wysokiego ryzyka naruszenia praw lub wolności osób fizycznych związanego z naruszeniem ochrony danych osobowych nie ma znaczenia, czy to ryzyko się zmaterializuje, a fakt istnienia ryzyka"[22], wymaga pewnego komentarza. Otóż bowiem fakt nieziszczenia się ryzyka w istocie nie ma znaczenia dla oceny jego poziomu w kontekście naruszenia bezpieczeństwa danych osobowych – przedmiotem badania przez administratora powinien być stopień prawdopodobieństwa wystąpienia skutku w postaci ryzyka naruszenia praw i wolności osoby, której dane dotyczą[23]. Jednocześnie jednak nie można zgodzić się z twierdzeniem, że dla oceny wysokiego ryzyka naruszenia praw lub wolności osób fizycznych związanego z naruszeniem ochrony danych osobowych wyłączne znaczenie ma fakt istnienia ryzyka – ponieważ w ten sposób pomija się drugi, poza powagą ryzyka, element istotny przy ocenie poziomu ryzyka, mianowicie prawdopodobieństwo wystąpienia zdarzenia, które skutkuje ryzykiem.

---

[20] Decyzja, s. 12.

[21] Obowiązki administratorów związane z naruszeniami ochrony danych osobowych, wersja 1.0, czerwiec 2019, s. 13, uodo.gov.pl [dostęp: 22.11.2021].

[22] Decyzja, s. 14.

[23] P. Barta, M. Kawecki, P. Litwiński [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021, s. 352; podobnie W. Chomiczewski [w:] E. Bielak-Jomaa, D. Lubasz, *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 711.

Tak jak konsekwentnie Prezes UODO łączy naruszenia bezpieczeństwa danych osobowych obejmujące numer PESEL z wysokim ryzykiem dla praw i wolności osób, których dane dotyczą, tak samo konsekwentnie organ nadzorczy nie uzasadnia swojego stanowiska. Zamiast tego przytaczane są wyłącznie potencjalne konsekwencje, jakie mogą się wiązać z takim naruszeniem – wskazuje się następujące, typowe zagrożenia dla praw i wolności osób, których dane dotyczą:

- uzyskanie przez osoby trzecie kredytów w instytucjach pozabankowych, na szkodę osoby, której dane dotyczą;
- uzyskanie dostępu do danych o stanie zdrowia osoby, której dane dotyczą w przypadku przełamania zabezpieczeń do systemu świadczeń opieki zdrowotnej lub korzystania ze świadczeń opieki zdrowotnej przysługujących tej osobie;
- korzystanie z praw obywatelskich osoby, której dane naruszono, np. wykorzystanie danych do oddania głosu w głosowaniu nad środkami budżetu obywatelskiego;
- zarejestrowanie przedpłaconej karty telefonicznej (pre-paid), która może posłużyć do celów przestępczych;
- wyłudzenie ubezpieczenia lub środków z ubezpieczenia;
- zawarcie umów cywilnoprawnych, np. najmu nieruchomości;
- posłużenie się fałszywymi danymi, np. przy otrzymywaniu mandatu[24].

Wszystkie te przypadki można określić zbiorczo mianem przypadków kradzieży tożsamości, a więc przestępstwa, które polega na wykorzystaniu danych osobowych innej osoby, podszywającej się pod tę osobę poprzez posłużenie się nimi[25].

Zjawisko braku uzasadnienia tezy o wysokim poziomie ryzyka dla praw i wolności osób, których dane dotyczą, jakie powstaje na skutek naruszeń bezpieczeństwa danych osobowych obejmujących numer PESEL, na gruncie glosowanej decyzji[26] przybiera postać oznajmującego stwierdzenia „Prezes UODO uznał". Tymczasem w literaturze dostępne są już analizy tego problemu, które wskazują na zgoła odmienne wnioski w zakresie poziomu ryzyka. W szczególności podnosi się, że prawdopodobieństwo popełnienia przestępstwa kradzieży tożsamości w wyniku naruszenia bezpieczeństwa danych osobowych obejmującego numer PESEL wynosi nie więcej, niż 0,17% i jest to z założenia wartość zawyżona przez brak możliwości oszacowania wpływu na nią takich czynników, jak choćby masowa publiczna dostępność numerów PESEL np. w Krajowym Rejestrze Sądowym[27]. Oczywiście na gruncie analizowanej decyzji istotne znaczenie dla oceny prawdopodobieństwa ziszczenia się ryzyka dla praw i wolności osób, których dane dotyczą, ma także zakres danych osobowych, które były przedmiotem

[24] Obowiązki administratorów związane z naruszeniami ochrony danych osobowych…, s. 17.

[25] J. Grabowska, A. Kaczmarczyk, *Kradzież tożsamości z art. 190a § 1 K.K. obowiązującego kodeksu karnego*, „Kortowski Przegląd Prawniczy" 2016 nr 4, s. 86.

[26] Co nie przeszkadza Prezesowi UODO czynić zarzutu pod adresem ukaranej spółki, jakoby ta „w swych wyjaśnieniach podkreślała jedynie, że dokonała oceny zgodnie z metodą ENISA, nie wskazując jednocześnie dodatkowego uzasadnienia przyjętych przez siebie kryteriów oceny ryzyka" (Decyzja, s. 15).

[27] P. Litwiński, *PESEL, wyciek danych i ryzyko*, „Rzeczpospolita" z dnia 25 maja 2021 r.; szczegółowe rozważania na ten temat wraz z opisem zastosowanej metody badawczej i jej wyników zostaną opublikowane przez autora w czasopiśmie „ABI Expert" 2021, nr 3 (tekst złożony do druku).

naruszenia. Słusznie więc zwraca uwagę Prezes UODO, że „metoda ENISA (metoda używana do szacowania poziomu ryzyka związanego z naruszeniem) wskazuje, że ostateczna wartość punktowa dla kontekstu przetwarzania (KPD) (obrazująca poziom ryzyka) może być zwiększana bądź zmniejszana w zależności od wystąpienia różnych czynników, m.in. szerokiego zakresu danych dla jednej osoby, charakteru danych czy możliwych negatywnych skutków dla podmiotu danych oraz skali naruszonych danych (dla tej samej osoby)"[28]. Poza tak ogólnym – i przez to prawdziwym – stwierdzeniem, w decyzji brak jest jednak jakiegokolwiek konkretu obrazującego, czy tok rozumowania Prezesa UODO, prowadzący do kategorycznego wniosku przytoczonego wyżej, czy w szczególności uzasadniającego przyjęcie w tym konkretnym przypadku, że taki a nie inny zakres danych spowodował powstanie wysokiego ryzyka dla praw i wolności osób dotkniętych naruszeniem.

Obowiązek sporządzenia uzasadnienia decyzji administracyjnej nakazuje sporządzać to uzasadnienie w taki sposób, aby strony znały argumenty i przesłanki podejmowania decyzji[29]. Tymczasem, w niniejszej sprawie jest dokładnie odwrotnie – teza organu nadzorczego w zakresie poziomu ryzyka jest znana, zaś argumenty ją potwierdzające – nie.

Administrator i przetwarzający w kontekście naruszeń bezpieczeństwa danych osobowych

Zakładając, że w glosowanej decyzji prawidłowo został ustalony stan faktyczny, wypada przejść do tego, co może stanowić jej największą wartość, mianowicie do problemu współpracy pomiędzy administratorem danych a przetwarzającym, w kontekście naruszeń bezpieczeństwa danych osobowych.

Obowiązki związane z naruszeniami bezpieczeństwa danych, o których mowa w art. 33 i 34 RODO, są obowiązkami administratora danych[30]. W przypadku powierzenia przetwarzania danych osobowych, jeżeli do naruszenia bezpieczeństwa doszło w organizacji podmiotu przetwarzającego, administrator danych może wykonać swoje obowiązki o tyle tylko, o ile otrzyma stosowną informację od przetwarzającego. Ten aspekt współpracy pomiędzy administratorem a przetwarzającym znalazł wyraz w art. 28 ust. 3 lit. e RODO, zgodnie z którym przetwarzający powinien pomagać administratorowi wywiązać się m.in. z obowiązku zgłaszania naruszenia ochrony danych osobowych (art. 33 RODO) oraz z obowiązku zawiadamiania osób, których dane dotyczą, o naruszeniu ochrony danych (art. 34 RODO). Wykonując ten obowiązek,

[28] Decyzja, s. 15.

[29] J. Zimmermann, *Glosa do wyroku NSA z 19 czerwca 1997 r., V SA 1512/96*, OSP 1998, z. 2, poz. 29.

[30] W literaturze określa się administratora danych mianem „głównego adresata" tych obowiązków, jednocześnie przyjmując, że obowiązki przetwarzającego ograniczają się do zgłoszenia naruszenia administratorowi danych – zob. K. Wygoda [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, s. 364.

przetwarzający powinien uwzględniać nie tylko charakter przetwarzania, ale również dostępne mu informacje, tj. informacje, w których jest posiadaniu, lub które, ze względu na zakres wykonywanych czynności przetwarzania, może uzyskać[31]. Ponieważ obowiązek pomagania administratorowi jest własnym obowiązkiem przetwarzającego, który wynika wprost z przepisów RODO, umowa powierzenia nie powinna powielać przepisów RODO, ale powinna zawierać szczegółową informację, jak procesor powinien pomagać administratorowi w spełnieniu wskazanych tam obowiązków[32].

Naruszenie bezpieczeństwa danych osobowych należy zgłosić Prezesowi UODO niezwłocznie, nie później jednak, niż w ciągu 72 godzin po jego stwierdzeniu przez administratora danych (art. 33 ust. 1 RODO). W decyzji zawarto szczegółowe informacje na temat statystyk terminowości zgłaszania naruszeń przez ukaraną Spółkę. I tak wskazuje się, że spośród zgłoszeń dokonanych w czerwcu 2020 r., „60% ogólnej liczby naruszeń (…) zostało zidentyfikowanych przez Spółkę powyżej 60 dni od daty zdarzenia powodującego naruszenie, zaś ponad 33% ogólnej liczby zgłoszeń stanowiły zdarzenia zidentyfikowane przez Spółkę powyżej 90 dni od daty zdarzenia". Z kolei spośród zgłoszeń dokonanych w lipcu 2020 r., „ponad 44% ogólnej liczby zgłoszeń stanowią naruszenia zidentyfikowane powyżej 60 dni od daty zdarzenia powodującego naruszenie, zaś 15% ogólnej liczby zgłoszeń stanowiły zdarzenia zidentyfikowane przez Spółkę powyżej 90 dni od daty zdarzenia powodującego naruszenie"[33]. Przyjęto również, że takie terminy dokonywania zgłoszeń wynikają z terminów przekazywania stosownych informacji przez firmę kurierską, które zostały wydłużone w ocenie ukaranej Spółki przez trwającą pandemię koronawirusa[34]. Natomiast Prezes UODO nie dał wiary wyjaśnieniom Spółki dotyczącym wpływu pandemii koronawirusa na terminowość wykonywania obowiązków związanych ze zgłaszaniem naruszeń bezpieczeństwa danych osobowych: „Zgromadzony materiał dowodowy nie mógł potwierdzić również dodatkowych wyjaśnień Spółki, że »istotny wpływ na terminowość zgłoszeń naruszeń danych osobowych dotyczących niniejszego postępowania Urzędu, dotyczących weryfikacji poprawności obsługi procesu dokumentów zwrotnych, miał okres trwającej pandemii«, ponieważ 60% ogólnej liczby naruszeń ochrony danych osobowych zgłoszonych w czerwcu 2020 r. zostało zidentyfikowanych przez Spółkę powyżej 60 dni od daty zdarzenia powodującego naruszenie, zaś ponad 33% ogólnej liczby zgłoszeń stanowiły zdarzenia zidentyfikowane przez Spółkę powyżej 90 dni od daty zdarzenia, tj. zdarzenia sprzed ogłoszenia stanu pandemii"[35]. Nie oceniając prawidłowości takiej a nie innej oceny dowodów w realiach tej sprawy, podkreślić jednak należy, że stan trwającej pandemii miał bez wątpienia wpływ na wykonywanie obowiązków związanych z naruszeniami bezpieczeństwa danych osobowych. Według danych pozyskanych przez autora w trybie dostępu do informacji publicznej, w I kwartale 2020 r.,

[31] P. Barta, M. Kawecki, P. Litwiński [w:] *Ogólne rozporządzenie o ochronie danych*…, s. 324.
[32] Wytyczne Europejskiej Rady Ochrony Danych 7/2020 w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO, s. 37, https://uodo.gov.pl/pl/414/1714 [dostęp: 22.11.2021].
[33] Decyzja, s. 20.
[34] *Ibidem*, s. 4.
[35] *Ibidem*, s. 5.

a więc w okresie poprzedzającym gwałtowny rozwój w Polsce pandemii, Prezesowi UODO zgłoszono 2016 przypadków naruszeń, podczas gdy w II kwartale 2020 r., czyli w czasie tzw. lockdownu, masowej pracy zdalnej[36] i skokowego wzrostu popularności usług kurierskich[37], tych naruszeń zgłoszono 1656. Jak się wydaje, tak istotny spadek liczby zgłaszanych naruszeń nie wiąże się ze wzrostem bezpieczeństwa przetwarzanych danych w czasie pandemii, a wręcz odwrotnie, ze spadkiem tegoż, na skutek masowego przechodzenia na pracę zdalną, do której organizacje nie były przygotowane, co mogło skutkować utratą kontroli nad procesami przetwarzania danych osobowych.

W opinii Grupy Roboczej Art. 29 (przejętej przez Europejską Radę Ochrony Danych), przyjmuje się, że administrator „stwierdził" wystąpienie naruszenia w momencie, w którym uzyskał wystarczającą dozę pewności co do tego, że doszło do wystąpienia incydentu bezpieczeństwa, który doprowadził do ujawnienia danych osobowych[38]. Skoro więc ukarana Spółka nie wiedziała o naruszeniu, nie mogła dokonać jego zgłoszenia – słusznie więc na gruncie niniejszej sprawy nie zarzucono Spółce dokonywania zgłoszeń z naruszeniem terminów wskazanych w RODO. Jednocześnie jednak przyjęto, że „brak szybkiej reakcji ze strony podmiotu przetwarzającego nie zdejmuje jednak z administratora odpowiedzialności za stwierdzenie naruszenia ochrony danych osobowych, bowiem zdolność do m.in. wykrywania naruszeń powinna być postrzegana jako kluczowy element środków technicznych i organizacyjnych, w tym każdej polityki w zakresie bezpieczeństwa danych"[39]. O ile bowiem w przypadku, gdy do naruszenia dochodzi w organizacji podmiotu przetwarzającego, administrator danych nie ma faktycznej możliwości dowiedzenia się o naruszeniu bez współpracy ze strony przetwarzającego, o tyle jednak to na administratorze ciążą takie obowiązki, jak:

- obowiązek korzystania 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 (art. 28 ust. 1 RODO);
- obowiązek dokonywania zgłoszeń naruszeń w terminie wynikającym z przepisów RODO.

Zwłaszcza ten pierwszy obowiązek ma kluczowe znaczenie dla prawidłowego funkcjonowania relacji pomiędzy administratorem danych a przetwarzającym. Jego treścią jest nakaz skierowany do administratora danych, aby korzystał z usług wyłącznie takich przetwarzających, którzy zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków

[36] W końcu czerwca 2020 r. udział osób, które pracowały zdalnie w związku z sytuacją epidemiczną w ogólnej liczbie pracujących objętych badaniem „Popyt na pracę", wyniósł 10,2%, a w województwie mazowieckim sięgnął niemal 25% – dane za opracowaniem Głównego Urzędu Statystycznego: Wpływ epidemii COVID-19 na wybrane elementy 10.09.2020 r. rynku pracy w Polsce w II kwartale 2020 r., stat.gov.pl [dostęp: 22.11.2021].

[37] W 2020 r. liczba przesłanych paczek wzrosła o 34,8%, a rynek usług kurierskich wzrósł o 22% w porównaniu do 2019 r., https://trans.info/pl/rynek-kurierski-w-polsce-rosnie-dwucyfrowo-wzrost-jeszcze-przyspieszy-227511 [dostęp: 22.11.2021].

[38] Wytyczne WP 250 rev. 01, s. 12, https://www.uodo.gov.pl/pl/3/1345 [dostęp: 22.11.2021].

[39] Decyzja, s. 18.

technicznych i organizacyjnych odpowiadających wymogom RODO, w tym wymogom bezpieczeństwa przetwarzania (zob. motyw 81 preambuły do RODO).

Jak wskazała Europejska Rada Ochrony Danych, obowiązek korzystania wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków, ma charakter obowiązku stałego, trwającego przez cały czas przetwarzania danych przez przetwarzającego w imieniu administratora[40]. W konsekwencji, administrator danych powinien weryfikować w odpowiednich odstępach czasu, czy przetwarzający daje takowe gwarancje, w tym poprzez przeprowadzanie audytów i inspekcji. I jeżeli administrator danych uzyska informacje o tym, że po stronie przetwarzającego dochodzi do naruszeń bezpieczeństwa danych osobowych, zwłaszcza o charakterze powtarzającym się, wówczas powinien podjąć działania zmierzające do weryfikacji, czy powierzenie przetwarzania danych temu konkretnemu podmiotowi w dalszym ciągu spełnia wymagania z art. 28 ust. 1 RODO, a więc czy przetwarzający w dalszym ciągu zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą (zakładając oczywiście, że takie gwarancje dawał z chwilą nawiązywania stosunku powierzenia). Jak się wydaje, nie można w tym kontekście mówić o „nadzorze" administratora danych osobowych nad przetwarzaniem danych w jego imieniu przez przetwarzającego, jak czyni to Prezes UODO[41], jako że nadzór oznacza – prócz uprawnień kontrolnych – także możliwość wywierania wpływu na działalność podmiotu nadzorowanego[42]. Jest tak dlatego, ponieważ w art. 28 ust. 3 lit. a RODO przyjęto, że przetwarzający może przetwarzać dane osobowe wyłącznie na udokumentowane polecenie administratora – przetwarzać, a więc wykonywać operacje na danych osobowych, które wykonuje w imieniu administratora danych. Tymczasem zastosowanie konkretnych środków zabezpieczenia danych osobowych nie jest jako takie operacją przetwarzania i nie może być objęte poleceniem administratora, o którym mowa w art. 28 ust. 3 lit. a RODO[43]. Co więcej, obowiązek stosowania przez przetwarzającego odpowiednich środków zabezpieczenia danych osobowych jest jego własnym obowiązkiem, na co wprost wskazuje art. 28 ust. 3 lit. c RODO. Z pewnością natomiast należy wymagać reakcji ze strony administratora danych na informacje o naruszeniach bezpieczeństwa danych osobowych, do których dochodzi po stronie przetwarzającego i podjęcia działań zmierzających do sprawdzenia, czy przetwarzający należycie chroni powierzone dane osobowe.

---

[40] Wytyczne Europejskiej Rady Ochrony Danych 7/2020 w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO, s. 30.

[41] Decyzja, s. 22.

[42] Zob. np. definicja nadzoru autorstwa W. Dawidowicza, zgodnie z którą nadzór to "właściwość organu nadrzędnego do wywierania wpływu na działalność organu podporządkowanego" (W. Dawidowicz, *Zagadnienia ustroju administracji państwowej w Polsce*, Warszawa 1970, s. 34).

[43] Zobowiązanie do stosowania przez przetwarzającego środków zabezpieczenia danych osobowych wskazywanych przez administratora danych może wynikać z umowy łączącej strony, jednakże wtedy inna będzie jego natura (cywilnoprawna, nie zaś publicznoprawna), a stosowanie tego rodzaju rozwiązania w praktyce kontraktowej nie jest zjawiskiem powszechnym i zależy od wielu czynników, w szczególności od ew. przewagi kontaktowej administratora danych.

Niewątpliwie jedną z form sprawdzenia będzie audyt przeprowadzony przez administratora danych w organizacji podmiotu przetwarzającego[44].

Jeżeli administrator danych, w wyniku podjętych czynności uzna, że naruszenia bezpieczeństwa danych osobowych, do których dochodzi w organizacji podmiotu przetwarzającego, można wyeliminować, wówczas winien podjąć odpowiednie działania, które do tego doprowadzą: przewidziane umową lub dążąc do zmiany umowy. Jeżeli natomiast administrator danych uzna, że przetwarzający nie zapewnia już gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą, w szczególności gdy ten odmawia podjęcia działań naprawczych lub zmiany umowy, jeżeli zachodzi taka konieczność, wówczas winien zakończyć korzystanie z jego usług, jako że takie przetwarzanie przestałoby spełniać warunek, o którym mowa w art. 28 ust. 1 RODO.

Co tak naprawdę wynika z decyzji ws. Cyfrowego Polsatu?

Pomijając wskazane wyżej naruszenia przepisów o postępowaniu, które w ocenie autora miały bardzo istotny wpływ na treść rozstrzygnięcia, wnioski, do których – na gruncie przepisów prawa materialnego – dochodzi Prezes UODO w glosowanej decyzji, zasługują na aprobatę. Wnioski te można w istocie sprowadzić do jednego, choć długiego, stwierdzenia, a mianowicie, że korzystanie przez administratora danych z usług podmiotu przetwarzającego, także będącego wysokiej klasy profesjonalistą, nie zwalnia tegoż administratora z ciągłego monitorowania przestrzegania przez przetwarzającego przepisów o ochronie danych osobowych i reagowania na stwierdzone nieprawidłowości, z zakończeniem stosunku powierzenia włącznie, jeżeli administrator uzna, że przetwarzający zaprzestał zapewniania gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Jeżeli administrator danych tego obowiązku nie wypełnia, wówczas narusza ciążący na nim prawny obowiązek zapewnienia bezpieczeństwa danych osobowych przetwarzanych w jego imieniu przez przetwarzającego. Takie spojrzenie na obowiązki administratora danych stanowi konsekwencję postrzegania ochrony danych osobowych jako procesu o charakterze ciągłym, którego nie można sprowadzić do jednorazowej czynności, czyli – do wyboru przetwarzającego i zawarcia z nim odpowiedniej umowy. Jednocześnie nie sposób nie zauważyć, że niewyjaśnienie statusu firmy kurierskiej z perspektywy przepisów o ochronie danych osobowych stanowi największą wadę glosowanej decyzji – jest to

[44] Prezes UODO w uzasadnieniu decyzji z 17 grudnia 2020 r., DKN.5130.1354.202, o nałożeniu kary na ID Finance Poland Sp. z o.o. uznał, że m.in. audyt RODO przeprowadzony w tej spółce będącej przetwarzającym dowodził braku naruszenia przez administratora art. 28 ust. 1 RODO – zob. P. Barta, M. Kawecki, P. Litwiński [w:] *Ogólne rozporządzenie o ochronie danych*…, s. 314.

stracona szansa na wyjaśnienie wątpliwości z tym związanych, zwłaszcza że w przeszłości zdarzały się sprzeczne ze sobą rozstrzygnięcia, które przytoczono wyżej.

Literatura

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

Dawidowicz W., *Zagadnienia ustroju administracji państwowej w Polsce*, Warszawa 1970.

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

Gaj M., Laprus-Bałuka T., Zaborowska A., *Prawo pocztowe. Komentarz*, Warszawa 2017.

Grabowska J., Kaczmarczyk A., *Kradzież tożsamości z art. 190a § 1 K.K. obowiązującego kodeksu karnego*, „Kortowski Przegląd Prawniczy" 2016, nr 4, s. 86.

Litwiński P., *PESEL, wyciek danych i ryzyko*, „Rzeczpospolita" z dnia 25 maja 2021 r.

Litwiński P., *Pojęcie danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych – glosa do wyroku Trybunału Sprawiedliwości z 19.10.2016 r. w sprawie C-582/14 Patrick Breyer*, EPS 2017, nr 5.

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

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

Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2019, uodo.gov.pl [dostęp: 22.11.2021].

Styczyński J., *Nierejestrowane przesyłki kontrowersyjne w świetle RODO*, „Dziennik Gazeta Prawna" z dnia 2 lipca 2019 r.

Zimmermann J., *Glosa do wyroku NSA z 19 czerwca 1997 r., V SA 1512/96*, OSP 1998, z. 2, poz. 29.

Streszczenie

Paweł Litwiński

Naruszenia bezpieczeństwa danych osobowych przez firmy kurierskie

Decyzja Prezesa UODO z 22 kwietnia 2021 r. dotyczy naruszeń bezpieczeństwa danych osobowych, do których dochodziło w związku z korzystaniem z usług firm kurierskich. Sedno decyzji można sprowadzić do stwierdzenia, że korzystanie przez administratora danych z usług podmiotu przetwarzającego nie zwalnia tego administratora z konieczności ciągłego monitorowania przestrzegania przez przetwarzającego przepisów o ochronie danych osobowych i reagowania na stwierdzone nieprawidłowości. To reagowanie w skrajnych przypadkach może przybrać postać zakończenia stosunku powierzenia, jeżeli administrator uzna, że przetwarzający zaprzestał zapewniania gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Jeżeli administrator danych tego obowiązku nie wypełnia, wówczas narusza ciążący na nim obowiązek zapewnienia bezpieczeństwa danych osobowych przetwarzanych w jego imieniu przez przetwarzającego.

Słowa kluczowe: ochrona danych osobowych, RODO; administrator; przetwarzający; administracyjna kara finansowa, kurier, naruszenie danych.

Summary

Paweł Litwiński

Personal Data Breaches by Courier Companies

The decision of the President of the Personal Data Protection Office of April 22, 2021 concerns breaches of the security of personal data that occurred in connection with the use of courier services. The essence of the decision can be boiled down to the statement that that the use of the processor's services by the data controller does not release the controller from the necessity to constantly monitor the processor's compliance with the provisions on the personal data protection law and to react to identified violations. If the controller finds that the processor has ceased to provide guarantees for the implementation of appropriate technical and organizational measures so that the processing complies with the requirements of the GDPR, processing by the processor shall be terminated. If the data controller does not fulfill this obligation, then he breaches his obligation to ensure the security of personal data processed by the processor on his behalf.

Keywords: personal data protection; GDPR; controller; processor; administrative fine; courier; data breach.