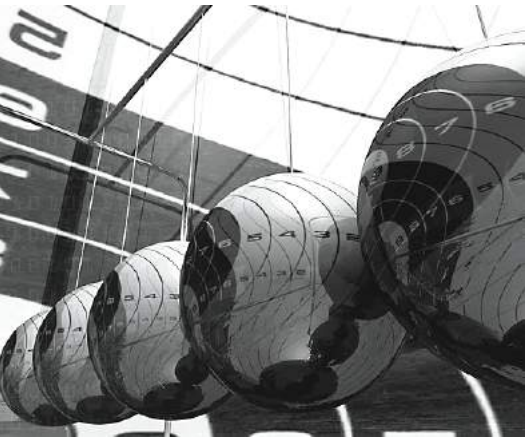


· RODO ·

PORADNIK DLA SEKTORA FINTECH

Ministerstwo Cyfryzacji

Wstęp

• Pytanie 1.

RODO[1] przewiduje, że administrator może przetwarzać bez zgody osoby, której dane dotyczą – na podstawie przesłanki tzw. uzasadnionych interesów – dane osobowe celem wysyłania drogą elektroniczną informacji handlowych. Z kolei ustawa o świadczeniu usług drogą elektroniczną (dalej „UŚUDE") wymaga zgody na przesyłanie informacji handlowych drogą elektroniczną.

1) Czy w związku z tym, z punktu widzenia RODO marketing w takich przypadkach odbywa się na podstawie uzasadnionych interesów i nie wymaga zgody, ale konieczne jest odebranie zgody wynikającej z UŚUDE?

Odpowiedź: Przesyłanie informacji handlowych jest dopuszczalne w oparciu o zgodę odebraną na podstawie przepisów UŚUDE. Przetwarzanie danych osobowych w tym celu będzie miało za podstawę uzasadniony interes administratora. Zgoda na przesyłanie informacji handlowych na gruncie UŚUDE stanowi łącznik między udzielającym zgodę a administratorem, o którym mowa w motywie 47 RODO. Fakt wyrażenia zgody na przesyłanie informacji handlowych na gruncie UŚUDE sprawia, że osoba wyrażająca taką zgodę ma rozsądne przesłanki, by spodziewać się, że może nastąpić przetwarzanie danych w tym celu. W obecnym stanie prawnym zgoda powinna spełniać warunki określone w UŚUDE. Warto jednak podkreślić, że projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 zakłada zmianę UŚUDE w ten sposób, że przesądzi o stosowaniu RODO do oceny skuteczności zgody.

[1] 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)

2) Czy konieczne jest odebranie odrębnej zgody na podstawie przepisów prawa telekomunikacyjnego na otrzymywanie informacji handlowych drogą telefoniczną?

Odpowiedź: W takim przypadku nie zachodzi potrzeba odbierania odrębnych zgód z art. 10 UŚUDE oraz art. 172 ust. 1 Prawa telekomunikacyjnego (Pt), jeżeli obie zgody miałyby dotyczyć tego samego zakresu czynności, np. wysyłki reklamowych wiadomości SMS lub MMS.

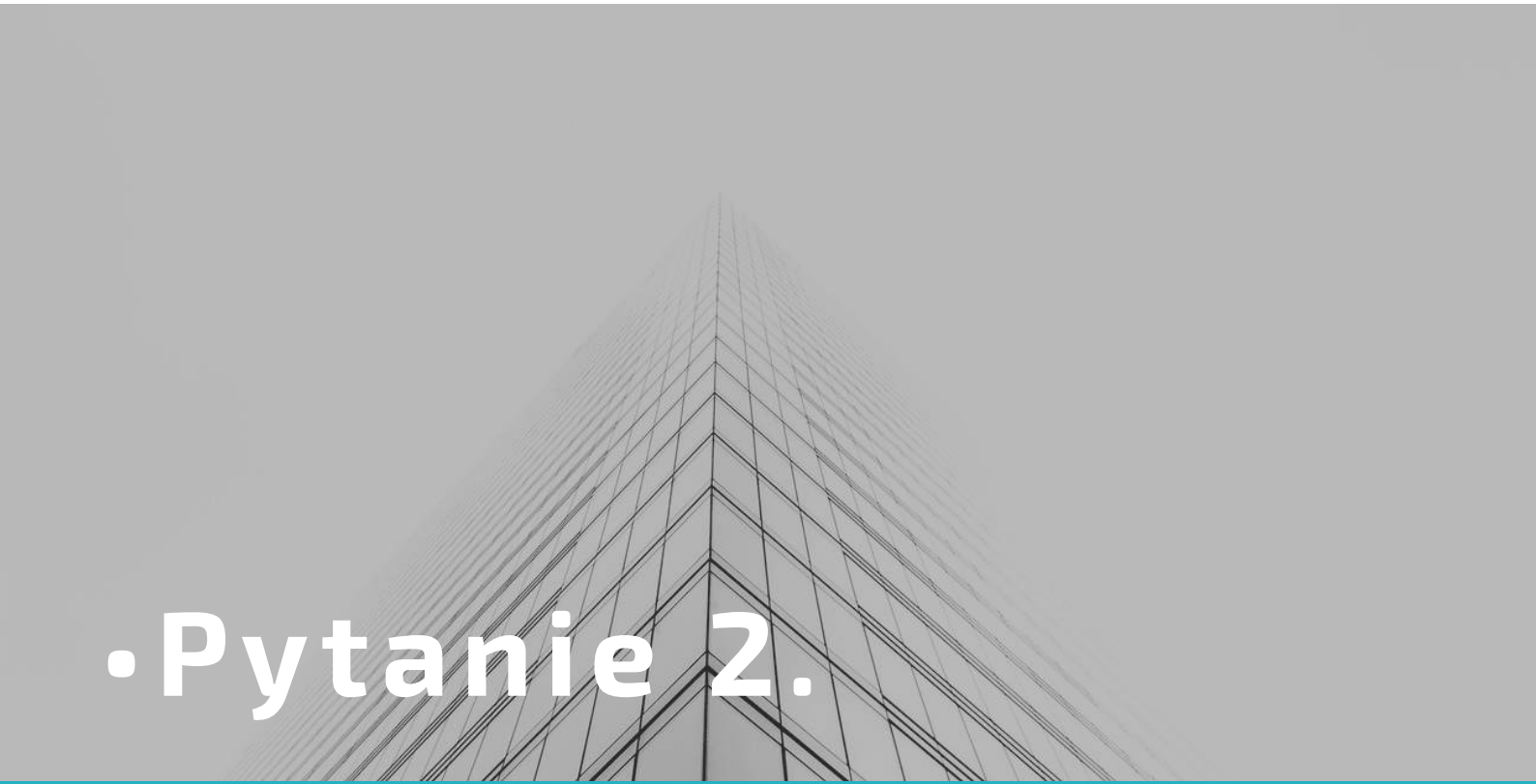
Uzasadnienie: Przetwarzanie danych osobowych w celach marketingowych zasadniczo nie wymaga odbierania zgody i może odbywać się na podstawie przesłanki prawnie uzasadnionych interesów przedsiębiorcy. Sprawę tę rozstrzyga wprost motyw (47) RODO, zgodnie z którym: „Za działanie wykonywane w prawnie uzasadnionym interesie można uznać przetwarzanie danych osobowych do celów marketingu bezpośredniego". Prawa odbiorcy zabezpiecza w tym wypadku możliwość złożenia bezwarunkowego sprzeciwu na przetwarzanie jego danych w celach marketingowych Zgodnie z art. 10 ust. 1 ustawy o świadczeniu usług drogą elektroniczną (UŚUDE), prowadzenie marketingu bezpośredniego poprzez wysyłkę wiadomości e-mail, SMS lub MMS wymaga zgody odbiorcy tylko w sytuacji wysyłania informacji „niezamówionych". Zgodnie z art. 10 ust. 2 UŚUDE informację handlową uważa się za zamówioną, jeżeli odbiorca wyraził zgodę na otrzymywanie takiej informacji, w szczególności udostępnił w tym celu identyfikujący go adres elektroniczny. Formalna zgoda nie jest zatem niezbędna, wystarczy, że odbiorca poda swój adres e-mail lub numer telefonu np. w polu formularza internetowego opisanego słowami „podaj swój adres e-mail, jeżeli chcesz otrzymywać od nas informacje o…" lub w rubryce opisanej w podobny sposób w pisemnej umowie. Także wszelkie internetowe formularze kontaktowe, w ramach których odbiorca prosi o udzielenie mu odpowiedzi na zadane pytanie lub przekazanie informacji o świadczonych usługach, stanowią formę „zamówienia" informacji handlowej, w związku z czym odpowiedzi na takie pytania można udzielić bez odbierania dodatkowych zgód. Ocena, czy zgoda została skutecznie udzielona powinna być dokonana w oparciu o warunki ustalone w UŚUDE, która w sposób autonomiczny określa warunki skutecznego udzielenia zgody.

W przypadku wykorzystywania telefonu do tego typu marketingu nie zachodzi potrzeba odbierania odrębnych zgód z art. 10 UŚUDE oraz art. 172 ust. 1 Prawa telekomunikacyjnego (Pt), jeżeli obie zgody miałyby dotyczyć tego samego zakresu czynności, np. wysyłki reklamowych wiadomości SMS lub MMS. Nie dochodzi w tym przypadku do naruszenia zasady dobrowolności zgody poprzez połączenie w jednym oświadczeniu kilku celów, gdyż zgoda wyrażana jest na jeden cel (wysyłka informacji handlowej z wykorzystaniem telekomunikacyjnego urządzenia końcowego), z tym że zastosowanie do niego znajdują dwie odrębne normy prawne. Brak jest również przeszkód prawnych ku temu, aby jedną zgodą objąć cel prowadzenia marketingu bezpośredniego z wykorzystaniem łączności elektronicznej, co obejmowałoby rozmowy telefoniczne oraz wysyłkę informacji pisemnych w formie poczty elektronicznej. Zasady nieobejmowania jedną formułą zgody kilku celów nie powinno się bowiem odczytywać jako nakaz odrębnego pytania o zgodę na każdy rodzaj czynności mogących się składać na realizację tego celu.

Do zgody wymaganej przez art. 172 Pt znajdują ponadto zastosowanie rozważania dotyczące art. 10 UŚUDE w zakresie formy tej zgody (art. 174 pkt 1). Prawo telekomunikacyjne nie stoi na przeszkodzie temu, aby oświadczenie o wyrażeniu zgody przybrało postać „jednoznacznej czynności potwierdzającej", np. poprzez podanie numeru telefonu w rubryce opisanej „podaj swój numer telefonu, jeżeli chcesz…". Wynika to z faktu, że zgodnie z art. 60 Kodeksu cywilnego oświadczeniem woli jest każda czynność osoby, która wyraża jej wolę w sposób dostateczny. Powyższa interpretacja stanie się tym bardziej uprawniona po wejściu w życie projektowanej ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679, której założeniem będzie zmiana dotychczasowej treści art. 174 Pt poprzez odesłanie do wymogów zgody określonych w RODO. Rozporządzenie unijne (RODO) wskazuje natomiast wprost, że zgoda może przybrać formę „wyraźnego działania potwierdzającego" (art. 4 pkt 11 RODO), a nie tylko formalnego oświadczenia.

Obowiązek informacyjny – ubezpieczyciele, banki

RODO nie nakłada na administratorów danych osobowych obowiązku ponownego lub uzupełniającego poinformowania podmiotów danych o przetwarzaniu ich danych (tak zwanego obowiązku informacyjnego), stosownie do art. 13 lub 14 RODO. Dotyczy to podmiotów danych, których dane zostały zebrane przed 25 maja 2018 r., o ile cele przetwarzania nie zostały rozszerzone. W zgodzie z zasadą transparentności administrator powinien udostępnić informacje o przetwarzaniu danych osobowych, w zakresie określonym w art. 13 i 14 RODO, w sposób umożliwiający podmiotom danych zapoznanie się z tymi informacjami, np. poprzez zamieszczenie polityki prywatności na stronie internetowej lub udostępnienie jej do wglądu w swojej siedzibie oraz miejscach, w których obsługiwani są klienci.



Pytanie 2.

Art. 13 i 14 RODO nakładają na administratora obowiązek podania osobie, której dane dotyczą, określonych w tych przepisach informacji zarówno w przypadku, gdy dane osobowe zbierane są od tej osoby (art. 13), jak i wtedy, gdy pochodzą z innego źródła(art. 14). Istotnym zagadnieniem na tle przywołanych przepisów jest kwestia, czy na administratorze danych ciąży obowiązek informacyjny względem osób, których dane zostały zebrane przed dniem rozpoczęcia stosowania RODO, tj. przed dniem 25 maja 2018 r.

O braku obowiązku ponownego lub uzupełniającego poinformowania o przetwarzaniu danych osobowych przesądza brzmienie art. 13 i 14 RODO. Zgodnie z nimi poinformowanie o fakcie przetwarzania danych powinno nastąpić „podczas pozyskiwania danych osobowych" (gdy dane zbierane są od osoby, której dane dotyczą - art. 13) lub co do zasady „w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca" (gdy danych nie pozyskano od tej osoby – art. 14). Normy przepisów art. 13 i 14 aktualizują się zatem tylko w sytuacji gdy dane są pozyskiwane i nie ma powodów, a przede wszystkim prawnych podstaw do tego, aby rozszerzać zakres stosowania tych przepisów na dane zebrane przed rozpoczęciem stosowania RODO. Rozporządzenie nie zawiera przepisów wskazujących terminy ewentualnego ponownego spełniania obowiązku informacyjnego względem osób, których dane zostały zebrane przed 25 maja 2018 r. Należy więc uznać, że prawodawca europejski nie zakładał w ogóle konieczności ponownego spełnienia obowiązku informacyjnego.

W omawianym kontekście istotne znaczenie ma także wyrok Naczelnego Sądu Administracyjnego w Warszawie z dnia 11 kwietnia 2003 r., sygn. akt II SA 1578/02, dotyczący realizacji obowiązku informacyjnego wynikającego z art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych w odniesieniu do danych zebranych przed wejściem w życie tej ustawy. NSA uznał (podtrzymując stanowisko wyrażone wcześniej w decyzji GIODO), iż art. 24 ustawy wyraźnie ustanawia ten obowiązek "w przypadku zbierania danych osobowych od osoby, której one dotyczą". Nie odnosi się więc do każdej formy przetwarzania danych, lecz tylko do ich zbierania.
W momencie zbierania danych przez bank nie obowiązywała jeszcze przedmiotowa ustawa, w tym jej art. 24 ust. 1. Bank nie miał więc obowiązku informowania skarżącego o zbieraniu jego danych.

Zgodnie z motywem 171 RODO przetwarzanie, które w dniu rozpoczęcia stosowania rozporządzenia (25 maja 2018 r.) już się toczy, powinno w terminie dwóch lat od wejścia rozporządzenia w życie zostać dostosowane do jego przepisów. Na gruncie tego motywu w wytycznych Grupy Roboczej Artykułu 29 w sprawie przejrzystości na mocy rozporządzenia 2016/679, WP260 rew.01, stwierdzono, iż oznacza to, że przed 25 maja 2018 r. administratorzy danych powinni zrewidować wszystkie informacje przekazywane osobom, których dane dotyczą, odnoszące się do przetwarzania ich danych osobowych (na przykład oświadczeń/ informacji dotyczących prywatności, etc.) w celu zapewnienia, że przestrzegają wymogów w odniesieniu do przejrzystości, które są omawiane w tych wytycznych.

W wytycznych wskazano również, że w wypadku zmiany lub rozszerzenia informacji administrator powinien wyjaśnić osobie, której dane dotyczą, że zmiany te zostały uczynione w celu zapewnienia zgodności z RODO. Grupa Robocza art. 29 rekomenduje, aby takie zmiany czy rozszerzenia zostały aktywnie dostarczone osobie, której dane dotyczą, ale jako minimum administrator powinien te informacje uczynić publicznie dostępnymi (np. na stronie internetowej). Jeśli zmiany są znaczące lub kluczowe powinny one zostać aktywnie dostarczone osobie, której dane dotyczą. Na gruncie powyższych wytycznych należy zatem uznać, że na administratorze ciąży ponowny obowiązek informacyjny względem osoby, której dane przetwarza, tylko w wypadku zmiany lub uzupełnienia takich informacji (where changes or additions are made to such information) i tylko wtedy, jeżeli zmiany te są istotne (if the changes or additions are material or substantive).

Należy podkreślić, że w wytycznych Grupy Roboczej art. 29 nie zawarto stanowiska, zgodnie z którym należałoby ponownie spełniać obowiązek informacyjny w sposób indywidualny (zwłaszcza poprzez masową jednorazową akcję wysyłkową). W wytycznych znajduje się jedynie stwierdzenie, że przed 25 maja 2018 r. administrator danych powinien dokonać rewizji stosowanych klauzul informacyjnych, tak aby były one zgodne z RODO, a w przypadku konieczności ich uzupełnienia celem zapewnienia transparentności może to zrobić poprzez publikację na stronie internetowej. Na administratorze ciąży przede wszystkim obowiązek wdrożenia mechanizmów zapewniających rzetelne i transparentne informowanie osoby, której dane dotyczą („rzetelny administrator"), a zatem powinien on zadbać raczej o możliwość poinformowania (ewentualnie doinformowania) w sposób możliwie przejrzysty i czytelny dla osoby, której dane dotyczą, o zasadach przetwarzania jej danych. Można to jednak uczynić „przy okazji" komunikacji z tą osobą, w rozsądnych terminach, lub informując o tym publiczne: udostępnienie informacji publicznie może nastąpić w dowolnej formie, jednak ze względu na potrzebę jak najszerszego ich rozpowszechnienia powinno nastąpić przede wszystkim w formie elektronicznej w sieci Internet (tak w komentarzu Edyta Bielak – Jomaa).

Gdyby Grupa Robocza art. 29 uznała za konieczne ponowne spełnienie obowiązku informacyjnego w każdym przypadku przetwarzania danych osobowych, zawarłaby takie stwierdzenie w wytycznych dotyczących przejrzystości.

Gdyby Grupa Robocza art. 29 uznała za konieczne ponowne spełnienie obowiązku informacyjnego w każdym przypadku przetwarzania danych osobowych, zawarłaby takie stwierdzenie w wytycznych dotyczących przejrzystości.

Z powyższego wynika, że jeżeli dane osoby zostały zebrane przed rozpoczęciem stosowania RODO, a wobec tej osoby prawidłowo spełniono obowiązek informacyjny na podstawie obowiązujących wówczas przepisów ustawy o ochronie danych osobowych, to administrator nie ma obowiązku ponownego spełnienia tego obowiązku, podając informacje wynikające z art. 13 i 14 RODO.

2) "Warstwowy" sposób realizowania obowiązku informacyjnego

Zgodnie ze stanowiskiem Grupy Roboczej Art. 29 zawartym w "Wytycznych w sprawie przejrzystości na mocy rozporządzenia 2016/679" dopuszczalne jest stosowanie przez administratora "warstwowych" procedur w celu spełnienia obowiązku informacyjnego. Warstwowe można rozumieć jako podzielone na etapy.

Grupa Robocza Art. 29 zaleca, aby pierwsza warstwa/procedura zawierała szczegóły dotyczące celów przetwarzania, tożsamość administratora oraz informację o prawach osoby, której dane dotyczą. Ważność podania tej informacji wynika bezpośrednio, w szczególności, z motywu 39 RODO.
Warstwowe podejście do realizacji obowiązku informacyjnego można również wdrożyć w kontekście pozasieciowym/niecyfrowym (tj. środowisku rzeczywistym, takim jak relacja pomiędzy osobami lub komunikacja telefoniczna), w którym administratorzy mogą wdrożyć procedury ułatwiające udzielenie informacji.

Mając na względzie zapewnienie zasady przejrzystości wynikającej z RODO, dopuszczalne będzie stosowanie przez administratora warstwowego procesu informowania osób o ich prawach wynikających z art. 13 i 14 RODO poprzez:

1) wskazanie informacji dotyczących celów przetwarzania i tożsamości administratora oraz informacji o miejscu, w którym możliwe jest zapoznanie się z zasadami przetwarzania i przysługującymi osobom fizycznym prawami.Przy czym treść komunikatu pierwszej warstwy powinna wprost wskazywać, że we wskazanym miejscu, np. polityce prywatności, podmiot danych może uzyskać informację o przysługujących mu prawach oraz dalszych informacji o przetwarzaniu danych osobowych przez administratora.

2) przekazanie osobie dalszych szczegółowych informacji przez odesłanie na adres strony internetowej administratora lub informację o możliwości uzyskania pełnej informacji po wybraniu odpowiedniej opcji.

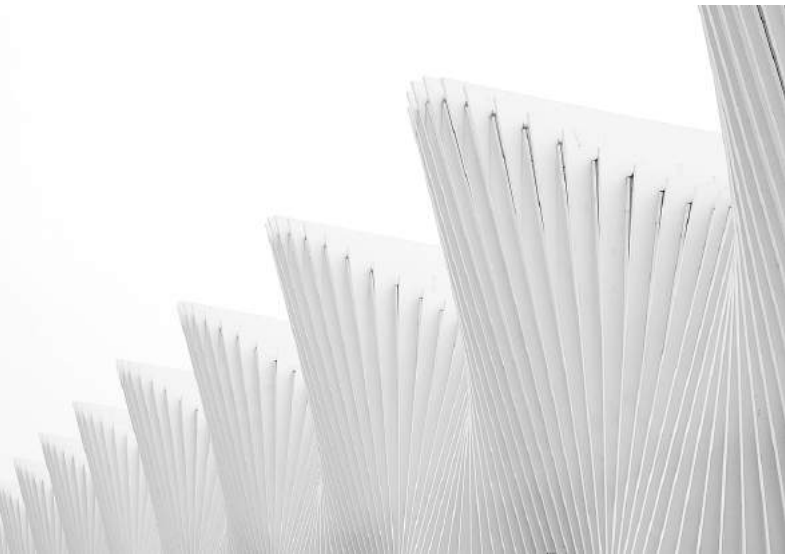
•Pytanie 3.

Czy przedsiębiorcy zajmujący się świadczeniem usług związanych z zarządzaniem wierzytelnościami i windykacją roszczeń w imieniu i na rachunek wierzyciela, w świetle przepisów RODO, powinni być traktowani jako odrębny administrator takich danych, udostępnionych mu w celu świadczenia usługi, czy też jako podmiot przetwarzający dane osobowe powierzone przez wierzyciela?

Odpowiedź:
Status przedsiębiorców świadczących usługi zarządzania wierzytelnościami i windykacji roszczeń uzależniony jest od tego, kto i w jakim zakresie określa cele i sposoby przetwarzania danych osobowych. Praktyka rynku usług windykacyjnych w Polsce wskazuje na możliwość przyjęcia dwóch koncepcji, w zależności od faktycznie pełnionej roli:

1) Przedsiębiorcy, będący firmami windykacyjnymi, którzy kompleksowo zarządzają wierzytelnościami, a tym samym samodzielenie określają cele, sposoby, zasady i szczegółowe operacje przetwarzania mają status odrębnego do wierzyciela administratora danych.

2) Przedsiębiorcy, będący firmami windykacyjnymi, mają status podmiotu przetwarzającego dane, jeżeli cele, sposoby i zasady przetwarzania danych osobowych określa wierzyciel, precyzując je w umowie powierzenia przetwarzania danych, w której określa przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także swoje prawa i obowiązki, które następnie realizuje zgodnie z brzmieniem zawartej umowy w tym zakresie.



Uzasadnienie

Zgodnie z art. 4 pkt 7 RODO status administratora posiada podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Zgodnie natomiast z art. 4 pkt 8 RODO status podmiotu przetwarzającego ma podmiot, który przetwarza dane osobowe w imieniu administratora. Status przedsiębiorców świadczących usługi zarządzania wierzytelnościami i windykacji roszczeń uzależniony jest więc od tego, kto określa cele i sposoby przetwarzania udostępnionych danych osobowych.

Granicą podziału między rolą administratora i podmiotu przetwarzającego jest więc to, jaką usługę świadczy dana firma, jak dalece jest ona związana umownymi instrukcjami wierzyciela i czy posiada uprawnienie do decydowania o celu przetwarzania. Decydujące znaczenie przy ocenie statusu firmy windykacyjnej powinno mieć więc kryterium funkcjonalne i faktyczna rola w procesach przetwarzania danych osobowych, a nie formalne zapisy umów.

Firmy windykacyjne, które kompleksowo zarządzają wierzytelnościami, samodzielnie określając przy tym zakres, charakter i cel operacji na danych osobowych, mają status odrębnego administatora danych przy spełnieniu warunków, które określają rolę administratora. Wewnętrzne procedury i polityki przewidują wówczas swobodę firmy windykacyjnej w zarządzaniu procesem i narzędziami wykorzystywanymi w celu optymalizacji procesów zmierzających do odzyskania długu.

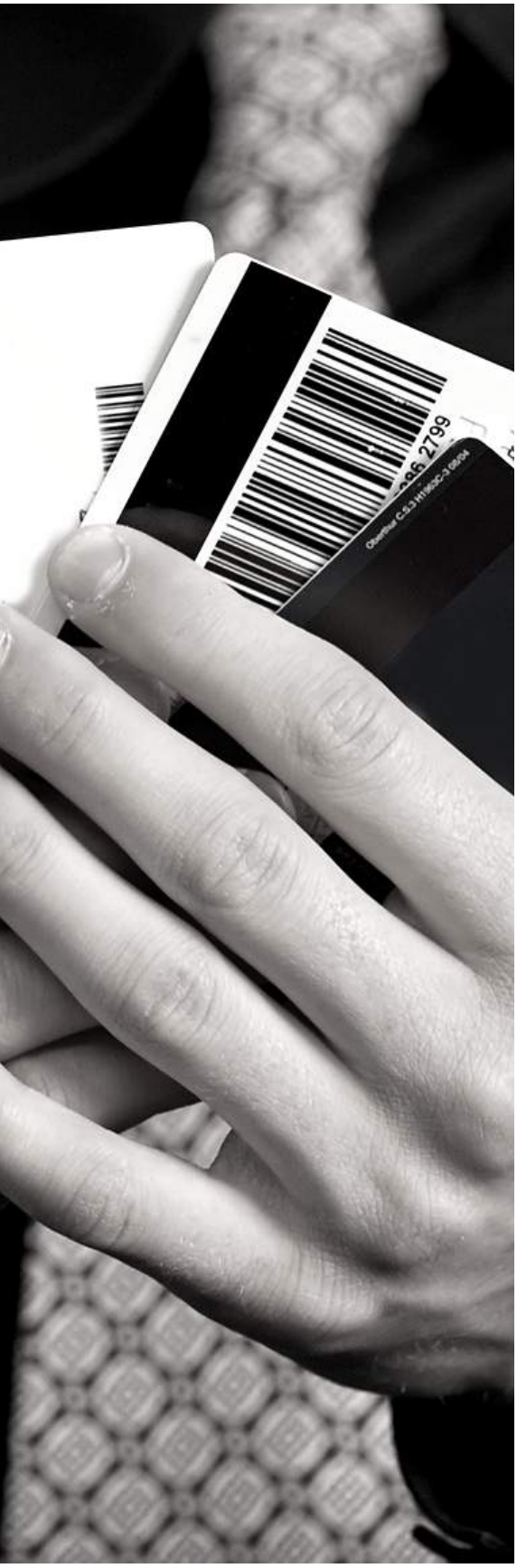
Wybór konkretnych metod windykacyjnych oznacza jednocześnie prowadzenie istotnych operacji przetwarzania danych osobowych, w tym poprzez ich poszukiwanie, wzbogacanie, uzupełnianie, modyfikowanie i aktualizowanie, czy udostępnianie podmiotom wspierającym proces odzyskania należności. Procesy te powodują modyfikację istniejących zbiorów danych w ramach realizacji świadczenia usług windykacyjnych

Zaznaczyć przy tym należy, że zakres, charakter i cel realizowany jest przez firmę windykacyjną nie dla celów własnych, lecz dla celów realizowanych przez wierzyciela – zleceniodawcę. W tej sytuacji, firma windykacyjna, prowadząc istotne operacje przetwarzania danych osobowych (jak wskazane wyżej), działa na zlecenie administratora, którego zakres jest wskazany w umowie.

Aby uznać przedsiębiorcę windykacyjnego za administratora danych niezbędne jest stwierdzenie, iż w ramach dochodzenia wierzytelności może samodzielnie ustalać konkretne cele i sposoby przetwarzania danych, a operacje przetwarzania danych osobowych w ramach realizowanych strategii windykacyjnych nie są określone lub uzgodnione z wierzycielem i nie podlegają nadzorowi i kontroli z jego strony. Firma windykacyjna, jako odrębny administrator danych, ponosi wówczas samodzielną i niezależną od wierzyciela odpowiedzialność za naruszenie przepisów dotyczących ochrony danych osobowych.

Jeżeli natomiast cele, sposoby i zasady przetwarzania danych osobowych określa sam wierzyciel, precyzując je w umowie powierzenia przetwarzania danych, a także wykonuje rzeczywisty nadzór nad określonymi przez siebie sposobami i zasadami przetwarzania danych, firma windykacyjna ma status podmiotu przetwarzającego dane. Wierzyciel powierzający dane osobowe, na gruncie art. 28 RODO, sprawuje wówczas nadzór i kontrolę nad przetwarzaniem danych i może ponosić współodpowiedzialność za niezgodne z prawem przetwarzanie danych przez przedsiębiorcę windykacyjnego.

W tej sytuacji firma windykacyjna przetwarza dane osobowe na polecenie administratora i w zakresie przez niego określonym w umowie, w której określony jest przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora. Przedsiębiorca windykacyjny samodzielnie nie określa celów przetwarzania, bazując w tym zakresie na sprecyzowanych poleceniach wierzyciela.



W takim przypadku wierzyciel, jako administrator danych osobowych swoich dłużników, powierza ich przetwarzanie przedsiębiorcy windykacyjnemu jako podmiotowi przetwarzającemu. Ten ostatni ma obowiązek działania w granicach określonych przez przepisy prawa i regulacje konkretnych umów powierzenia, zgodnie z art. 28 RODO gwarantujących, że:

- dane osobowe są przetwarzane na polecenie administratora i w zakresie określonym przez administratora w umowie powierzenia przetwarzania;
- umowa powierzenia przetwarzania określa przedmiot i czas trwania powierzenia oraz obowiązek zwrotu lub usunięcia danych po zakończeniu powierzenia;
- umowa powierzenia przetwarzania określa charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane będą przetwarzane;
- umowa powierzenia określa szczegółowo prawa i obowiązki administratora i procesora, przewidując także regulacje umożliwiające kontrolę nad podmiotem przetwarzającym;
- administrator danych osobowych sprawuje realny nadzór nad przetwarzaniem powierzonych danych przez podmiot przetwarzający;
- dalsze powierzenie przetwarzania danych osobowych („podpowierzenie") przez podmiot przetwarzający wymaga uzyskania zgody administratora danych osobowych.

Sytuację, w której przedsiębiorca windykacyjny, działając jako podmiot przetwarzający, przekracza rolę wyznaczoną procesorowi, reguluje art. 28 ust. 10 RODO. W zakresie w jakim podmiot przetwarzający wykracza poza cele i sposoby przetwarzania danych określone przez administratora, uznaje się go za odrębnego administratora danych w odniesieniu do takiego przetwarzania. Artykuł 28 ust. 10 RODO wyznacza więc granicę dla procesora, po przekroczeniu której automatycznie zostaje on zakwalifikowany jako odrębny administrator.

Praktyka rynku usług windykacyjnych w Polsce wskazuje, że przedsiębiorcy windykacyjni świadczą swoje usługi w oparciu o własne procesy windykacji i wewnętrzne polityki, co powoduje, że w znaczącej ilości przypadków wykonują istotne operacje na danych osobowych.

•Pytanie 4.

Czy administrator ma obowiązek usunięcia danych, w tym danych wrażliwych (art. 9 RODO) oraz danych dotyczących skazań (art. 10 RODO) w przypadku, gdy dane te zostały przekazane administratorowi z własnej inicjatywy podmiotu danych, tj. bez uprzedniej wiedzy oraz sygnalizowanej przez administratora potrzeby przekazania takich danych?

Odpowiedź:

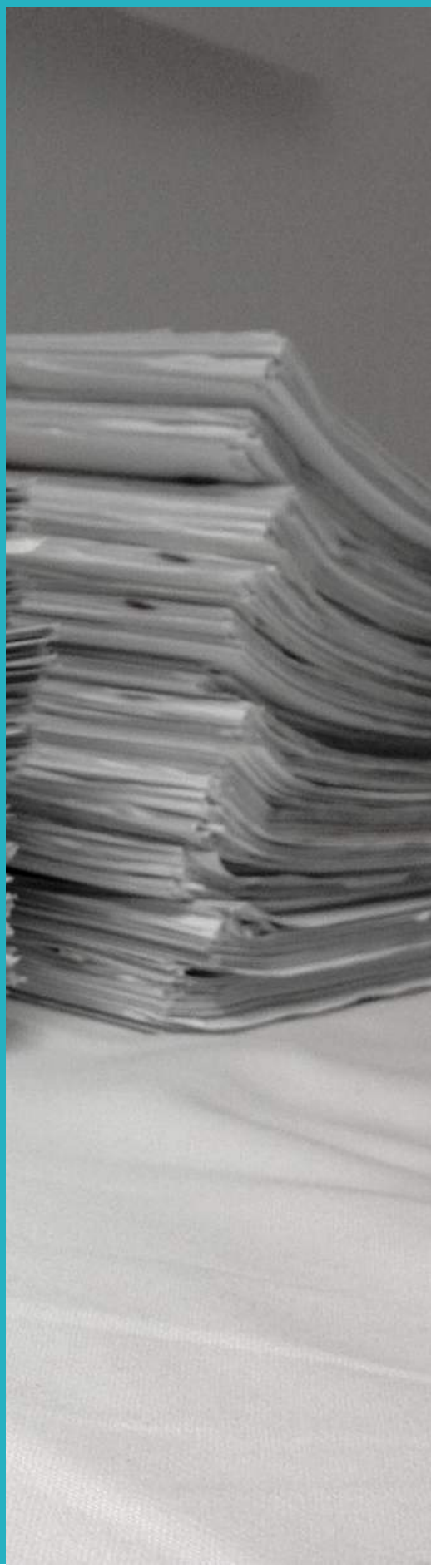
Administrator nie ma obowiązku usunięcia danych (w tym danych wrażliwych wykraczających poza dane, które miał zamiar zebrać), jeżeli z przyczyn technicznych nie jest możliwe ich usunięcie bez jednoczesnego usunięcia danych, które administrator ma prawo przetwarzać (np. kiedy dane wrażliwe znajdują się w jednym piśmie z żądaniem klienta lub jego danymi kontaktowymi).
W takim wypadku wystarczające dla ochrony danych osobowych jest, jeżeli administrator:

- nie ma możliwości i nie będzie podejmował próby użycia tych danych osobowych w stosunku do osoby, której dane dotyczą ani też przechowywanie danych nie będzie miało wpływu na tę osobę,
- nie udostępnia tych danych ani nie umożliwia dostępu do nich innemu podmiotowi,
- zabezpiecza dane osobowe odpowiednimi środkami technicznymi i organizacyjnymi,
- usuwa dane niezwłocznie, kiedy jest to możliwe.

Uzasadnienie

Należy zwrócić uwagę na problematyczną kwestię otrzymywania przez administratorów danych, w tym danych wrażliwych (tj. danych osobowych określonych w art. 9 RODO) przekazywanych przez klientów z ich własnej inicjatywy, tj. bez uprzedniej wiedzy oraz sygnalizowanej przez administratorów potrzeby przekazania takich danych. W swej praktyce administratorzy (na przykład banki) często otrzymują od klientów tak określone dane. W praktyce można zaobserwować, iż klienci bardzo często z własnej inicjatywy przekazują administratorom dane wrażliwe – na przykład klient przekazuje bankowi informacje o swoim stanie zdrowia, które mają stanowić uzasadnienie wniosku klienta o restrukturyzację zadłużenia. Często również administratorzy – nie mając jakiejkolwiek intencji pozyskiwania takich kategorii danych – uzyskują od klientów dane wrażliwe takie jak informacje o przynależności do partii politycznej lub przynależności religijnej. Przykładowo, tak określone informacje są przekazywane bankom nie tylko w toku zawierania umów z podmiotami takimi jak partie polityczne czy związki wyznaniowe, lecz również w ramach wykonywania umowy rachunku bankowego osoby fizycznej (na przykład: klient w tytule przelewu bankowego wpisuje swoje imię, nazwisko oraz sformułowanie dotyczące składki członkowskiej na określoną partię polityczną).

W powyższym kontekście należy zwrócić szczególną uwagę na dane dotyczące skazań klientów na mocy wyroków skazujących. Zgodnie z art. 10 RODO: „Przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych". Należy zauważyć, iż w swej codziennej działalności administratorzy są często postawieni przed koniecznością zapoznania się z danymi osobowymi klientów dotyczącymi wyroków skazujących, naruszeń prawa lub powiązanych środków bezpieczeństwa. Przykładowo, takie kategorie danych są często przekazywane w komunikacji z bankami przez samych klientów lub też członków ich rodzin, co ma miejsce zarówno w przypadku komunikacji pisemnej (wszelkiego rodzaju pisma), jak i ustnej (na przykład – rozmowy telefoniczne). Klienci przekazują tak określone dane z własnej inicjatywy – na przykład w celu restrukturyzacji kredytu lub wstrzymania windykacji, kiedy to fakt pobytu w areszcie lub zakładzie karnym ma stanowić uzasadnienie wniosku w powyższym przedmiocie. Klienci przekazują wskazane kategorie danych również przy składaniu reklamacji czy też w przypadku ustanawiania pełnomocnictw, kiedy to – przykładowo – klient odbywający karę pozbawienia wolności przesyła bankowi pełnomocnictwo dla osoby trzeciej sporządzone w zakładzie karnym.



Uzasadnienie

W tym też miejscu należy podkreślić, iż z samej istoty celów, dla których klienci przekazują administratorom tak określone kategorie danych osobowych wynika, iż brak jest możliwości usuwania tychże danych z pism lub wniosków klientów, czy też zapisów rozmów z klientami. Skutkowałoby to bowiem utratą tych informacji, które klient celowo przekazał w celu zainicjowania (często również uzasadnienia) określonych działań na jego rzecz. Przykładowo w przypadku działalności banków mowa tu o wniosku klienta dotyczącego restrukturyzacji jego zobowiązania, wniosku o wstrzymanie windykacji, kwestii respektowania przez bank pełnomocnictwa ustanowionego przez klienta podczas pobytu w zakładzie karnym, czy też udzielenia przez bank odpowiedzi na reklamację, w której klient informuje, iż przebywa w zakładzie karnym.

Podobne problemy dotyczą przedsiębiorców telekomunikacyjnych, którzy otrzymują od abonentów szereg danych wrażliwych w reklamacjach lub w toku szeroko rozumianej windykacji. Analogicznie jak w przypadku instytucji finansowych, tak i w tym przypadku informacje o stanie zdrowia lub wyrokach skazujących podawane są na uzasadnienie różnorodnych wniosków, w tym o odroczenie płatności, rozłożenie na raty lub zmniejszenie faktury. Informacje te nie są przy tym istotne dla rozstrzygnięcia, a przedsiębiorcy telekomunikacyjni nie mają zamiaru ich zbierania i dalszego przetwarzania.

Zgodnie z art. 2 ust. 1. RODO rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych. Przetwarzanie natomiast, zgodnie z definicją zawartą w art. 4 pkt 2) RODO oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, m.in. taką jak zbieranie. Zbieranie danych osobowych musi odbywać się w sposób intencjonalny tj. administrator musi mieć zamiar zebrania danych osobowych. Świadczy o tym zawarty w przepisie zwrot „mają stanowić" część zbioru danych. Jak wskazuje się w literaturze, posłużenie się tym zwrotem wskazuje na intencję towarzyszącą procesowi gromadzenia danych osobowych W przypadku, gdy osoba, której dane dotyczą, podaje administratorowi z własnej inicjatywy swoje dane osobowe, w tym dane wrażliwe, natomiast administrator nie ma intencji dokonywania na tych danych żadnych operacji, nie można w ogóle mówić o przetwarzaniu danych osobowych, a zatem obowiązki wynikające z RODO nie mają tu zastosowania. Należy też stwierdzić, że samo wejście w posiadanie danych, bez intencji i woli ich adresata i bez zamiaru dalszego przetwarzania, nie jest zbieraniem danych osobowych.

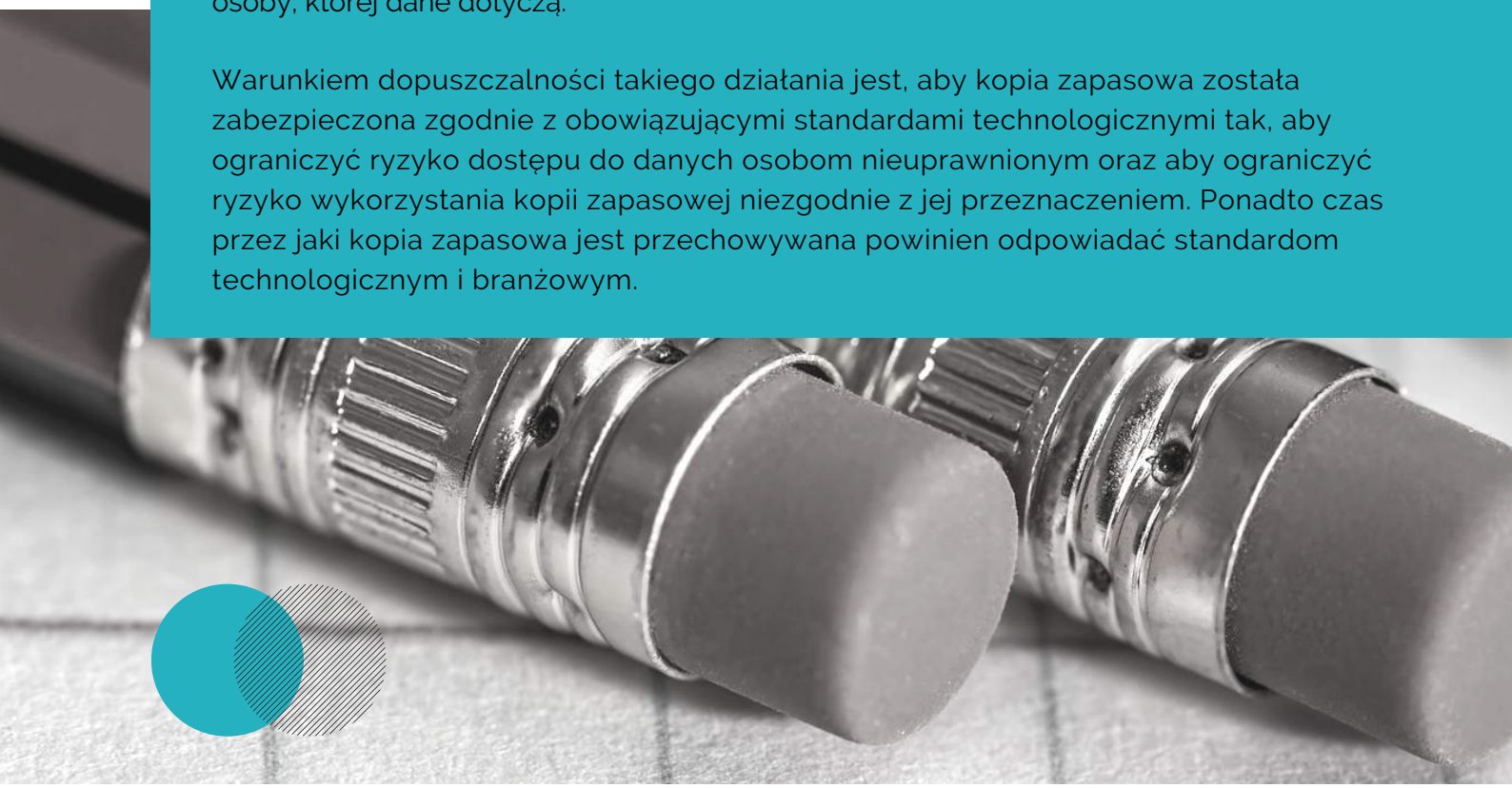
Pytanie 5.

Kiedy powstaje obowiązek usunięcia danych osobowych z kopii zapasowych systemów informatycznych?

Tworzenie i przechowywanie kopii zapasowych systemów informatycznych, obejmujących dane osobowe, stanowi techniczny sposób zabezpieczenia danych osobowych, co do których administrator ma podstawę prawną przetwarzania w określonych celach. Nie jest zatem konieczne poszukiwanie niezależnej podstawy prawnej dla tworzenia i przechowywania takich kopii zapasowych. W przypadku ustania podstawy prawnej przetwarzania danych osobowych utrwalonych w kopii zapasowej, dane te powinny zostać usunięte (lub zanonimizowane), jednak przy uwzględnieniu ograniczeń wynikających z technologicznych uwarunkowań kopii zapasowych oraz ryzyka naruszenia praw i wolności wszystkich osób, których dane osobowe są przechowywane w kopii zapasowej.

Biorąc pod uwagę te uwarunkowania należy uznać, że akceptowalnym rozwiązaniem jest, aby dane osobowe były kasowane tylko razem z całą kopią zapasową, po ustaniu podstaw przetwarzania wszystkich zawartych w niej danych osobowych lub po ustaniu przydatności kopii zapasowej. Do tego czasu, kopia zapasowa (zapisane w niej dane osobowe) powinny zostać „wyłączone z przetwarzania" co oznacza, że mogą być dalej przetwarzane, jednak należy ograniczyć ich przetwarzanie tylko do przechowywania. Dane zawarte w kopii nie mogą być zatem wykorzystywane z zastrzeżeniem sytuacji, w której zaistnieje konieczność wykorzystania kopii zapasowej, zgodnie z jej przeznaczeniem, np. na skutek awarii systemu. Jednocześnie, z uwagi na konieczność zapewnienia integralności kopii zapasowej, dane osobowe w niej utrwalone nie muszą być kasowane w sposób selektywny, np. na żądanie osoby, której dane dotyczą.

Warunkiem dopuszczalności takiego działania jest, aby kopia zapasowa została zabezpieczona zgodnie z obowiązującymi standardami technologicznymi tak, aby ograniczyć ryzyko dostępu do danych osobom nieuprawnionym oraz aby ograniczyć ryzyko wykorzystania kopii zapasowej niezgodnie z jej przeznaczeniem. Ponadto czas przez jaki kopia zapasowa jest przechowywana powinien odpowiadać standardom technologicznym i branżowym.



Rozszerzenie stanowiska:

Administrator jest zobowiązany na gruncie RODO do stosowania środków technicznych i organizacyjnych mających zapewnić poziom bezpieczeństwa przetwarzania danych stosowny do ryzyka, uwzględniając stan wiedzy technicznej, koszty wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania.
Kopie zapasowe (kopie bezpieczeństwa) to kopie danych, które mają służyć do odtworzenia oryginalnych danych w przypadku ich utraty lub uszkodzenia.

Tworzenie kopii zapasowych przez administratorów danych związane jest z koniecznością realizacji obowiązku wynikającego z art. 32 ust. 1 RODO, czyli obowiązku wdrożenia środków zapewniających bezpieczeństwo przetwarzania. W szczególności tworzenie kopii zapasowych danych (czy też backupu systemowego lub sprzętowego) jest jednym ze środków służących ciągłemu zapewnianiu dostępności i odporności systemów oraz usług polegających na przetwarzaniu danych (art. 32 ust. 1 lit b RODO). Zapewnia także zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego (art.32 ust. 1 lit c RODO).

Dostępność systemu przetwarzającego dane osobowe rozumiana jest jako zapewnienie możliwości wykorzystania systemu każdorazowo w przypadku zaistnienia takiej konieczności. Dostępność systemu może ulegać naruszeniu z wielu przyczyn np. błędów sprzętowych lub błędów oprogramowania, czy też braku dostępu do sieci. Natomiast odporność systemu to jego zdolność do prawidłowego funkcjonowania pomimo dużego obciążenia. Zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego nakierowana jest na dostępność danych w szczególnej sytuacji jaką jest zaistnienie incydentu. Znaczenie kopii zapasowych jako środka zabezpieczającego zostało potwierdzone już na gruncie przepisów obowiązujących w Polsce przed 25 maja 2018 r., tj. w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, gdzie w § 5 pkt. 4 wskazywano, jako konieczny element instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, procedury dotyczące tworzenia kopii zapasowych.

W przypadku kopii zapasowych i żądania usunięcia danych na podstawie art. 17 RODO, może realnie zdarzyć się, że nie będzie technicznie możliwe usuniecie danych zawartych w kopii zapasowej lub koszty i wysiłek organizacyjny takiego selektywnego usunięcia danych będą zbyt duże w stosunku do ryzyka naruszenia praw i wolności podmiotu danych. Ponadto selektywne usunięcie danych osobowych z kopii narusza integralność kopii danych, a zatem może powodować ryzyko dla praw i wolności innych osób, których dane są przechowywane w ramach tej samej kopii danych.

Pytanie 6.

Czy przepisy odrębnych ustaw dotyczące działalności podmiotów (tzw. regulacje sektorowe) mogą stanowić lex specialis wobec przepisów RODO?

Odpowiedź:

Jeżeli przepisy odrębnych ustaw (regulacji sektorowych) odnoszące się do przetwarzania informacji, mogących stanowić dane osobowe, przewidują dalej idącą ochronę niż wynika to z RODO i ustawy z dnia 24 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r., poz. 1000), w pierwszej kolejności stosuje się przepisy tychże ustaw jako mających status lex specialis w stosunku do ogólnych przepisów RODO. Przepisy RODO (jako regulację o charakterze ogólnym) stosuje się jedynie uzupełniająco w tych obszarach, w których brak jest szczegółowych regulacji sektorowych.

Przykładowo, aktami normatywnymi, które mają charakter regulacji sektorowych, a które zawierają szczegółowe przepisy dotyczące przetwarzania oraz ochrony danych osobowych, są ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U. z 2015 r. poz. 128 ze zm.), ustawa z 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2014 r. poz. 243 ze zm.) oraz ustawa z 11 września2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (Dz.U. z 2015 r. poz. 1844, ze zm.).

Wyżej wskazane regulacje sektorowe o randze ustawy zawierają specyficzne wytyczne, które ustanawiają dalej idącą ochronę danych osobowych niż przepisy RODO, m.in. poprzez ustanowienie obowiązku zachowania tajemnicy bankowej, telekomunikacyjnej oraz ubezpieczeniowej. Regulacje te stanowią adekwatne i skutecznie gwarancje ochrony wolności i prawnie uzasadnionych interesów osób, których dane dotyczą.

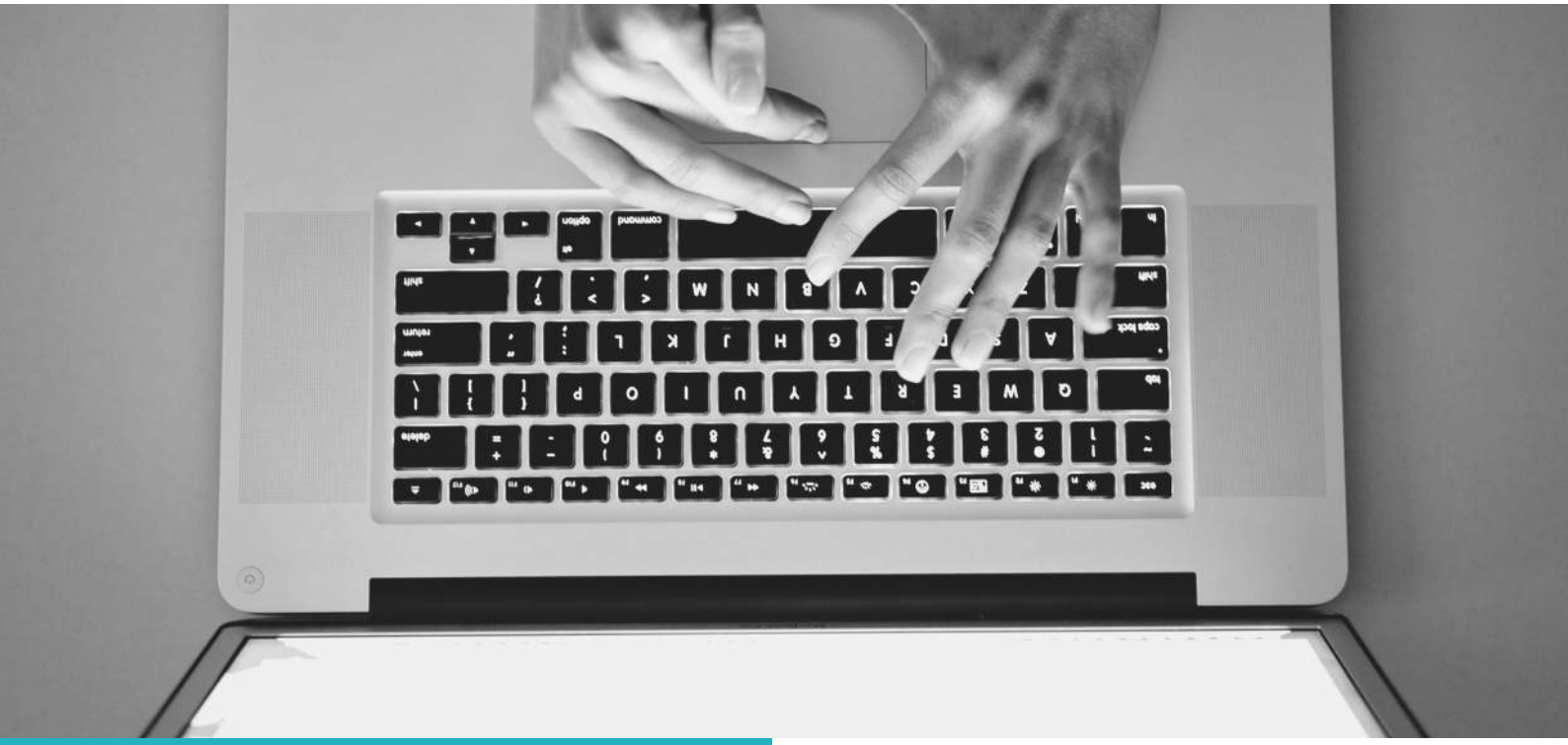
Nie ulega więc wątpliwości, iż przepisy dot. tajemnicy bankowej, telekomunikacyjnej i ubezpieczeniowej – jako lex specialis przewidziane na gruncie przywołanych wyżej ustaw – stanowią regulacje skutecznie gwarantujące adekwatny poziom ochrony praw, wolności i prawnie uzasadnionych interesów osób, których dane dotyczą – i jako tak określone lex specialis powinny mieć pierwszeństwo przed ogólnymi regulacjami wynikającymi z RODO, w sytuacji, gdy zakres normy prawnej wynikającej z przepisu ustawy sektorowej jest zbieżny z normą wynikającą z RODO. W takim przypadku znajdzie zastosowanie norma wynikająca z ustawy sektorowej jako norma określająca wyższy poziom ochrony przetwarzania danych osobowych.

Uzasadnienie:

Należy zwrócić uwagę na zagadnienie relacji pomiędzy regulacjami zawartymi w RODO a odrębnymi przepisami przewidującymi dalej idącą ochronę niż ww. Rozporządzenie, ze szczególnym uwzględnieniem przepisów ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe, ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne czy ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej, oraz przewidzianymi na ich gruncie tajemnicami prawnie chronionymi.

W poprzednim stanie prawnym, tj. na gruncie uchylonej ustawy z dnia z dnia 29 sierpnia 1997 r. o ochronie danych osobowych obowiązywała zasada, zgodnie z którą „jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ochronę, niż wynika to z niniejszej ustawy, stosuje się przepisy tych ustaw" (art. 5 przedmiotowej ustawy). Tak określona regulacja w sposób adekwatny odnosiła się m.in. do tajemnicy bankowej, telekomunikacyjnej i ubezpieczeniowej jako reżimu chroniącego dane osobowe w stopniu wyższym niż same przepisy o ochronie danych osobowych. Wydaje się przy tym, iż obecnie samo RODO (a w efekcie również i obecnie projektowane przepisy wprowadzające) w sposób niewystarczający precyzuje tak określone zagadnienie relacji pomiędzy RODO a przepisami sektorowymi przewidującymi dalej idącą ochronę danych osobowych. Brak jest natomiast uzasadnienia dla równoległego stosowania RODO oraz przepisów bardziej szczegółowych. Taka zdwojona ochrona nie znajduje uzasadnienia, bo regulacje sektorowe zapewniają odpowiedni dla danego sektora poziom ochrony, przy czym standard tej ochrony jest wyższy niż standard określony w RODO.

W powyższym kontekście należy więc wskazać, iż ograniczenia wynikające z tajemnicy bankowej, telekomunikacyjnej i ubezpieczeniowej funkcjonujące na gruncie przywołanych przepisów ustaw sektorowych zapewniają ochronę praw, wolności i prawnie uzasadnionych interesów osób, których dane dotyczą. Ochronę idącą znacznie dalej niż ogólne uregulowania dotyczące ochrony danych osobowych (zarówno w odniesieniu do poprzedniej ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, jak i obecnych regulacji RODO). Nie ulega więc wątpliwości, iż przepisy dot. tajemnicy bankowej, telekomunikacyjnej i ubezpieczeniowej – jako lex specialis przewidziane na gruncie ustaw sektorowych – stanowią regulacje skutecznie i gwarantujące adekwatny poziom ochrony praw, wolności i prawnie uzasadnionych interesów osób, których dane dotyczą – i jako tak określone lex specialis powinny mieć pierwszeństwo przed ogólnymi regulacjami wynikającymi z RODO.



•Pytanie 7.

Czy podstawą przetwarzania danych osobowych na cele przeprowadzenia konkursu jest uzasadniony interes administratora, czy też w tym zakresie zachodzi konieczność pobierania osobnych zgód na przetwarzanie danych osobowych?

Odpowiedź:

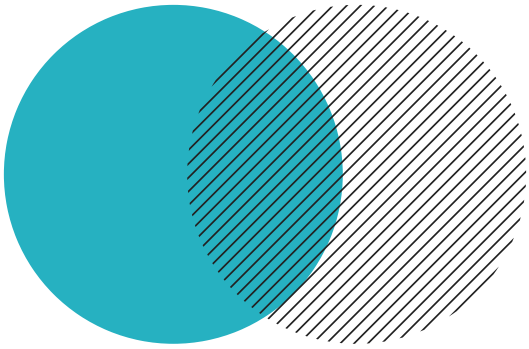
Podstawą przetwarzania danych osobowych na cele przeprowadzenia konkursu jest art. 6 ust. 1 lit. f) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: RODO), a więc prawnie uzasadniony interes administratora danych osobowych.

Administrator danych, organizując konkurs, będący przyrzeczeniem publicznym w rozumieniu art. 919 Kodeksu cywilnego i nast., może przetwarzać dane osobowe uczestnika konkursu na podstawie prawnie uzasadnionego interesu, m.in. w celu: organizacji konkursów, w tym obsługi zgłoszeń, w zakresie pomocy technicznej, informowania o wynikach i wyłaniania zwycięzców oraz przyznawania i wysyłania nagród konkursowych.

Uzasadnienie:

Jeżeli administrator danych osobowych (dalej: ADO), jest jednocześnie organizatorem akcji promocyjnej i przyrzeka publicznie, że uczestnik akcji, który wykona określoną czynność, otrzyma nagrodę (m.in. upust czy inną promocję cenową), to mamy do czynienia z przyrzeczeniem publicznym, określonym w art. 919 i nast. k.c. W takim przypadku ADO składa jednostronne oświadczenie woli, mocą którego podejmuje on zobowiązanie dotrzymania danego przyrzeczenia. Konkurs jest uznawany przez doktrynę za przyrzeczenie publiczne, a nie umowę (tak m.in. Sąd Ochrony Konkurencji i Konsumentów w wyroku z dnia 20 maja 2013 roku, sygn. akt XVII AmC 1555/12 oraz m.in. Sąd Najwyższy w wyroku z dnia 28 stycznia 2015 roku, sygn. akt. I CSK 40/14).

Zgodnie natomiast z art. ust. 1 lit. f) RODO, przetwarzanie jest zgodne z prawem, jeżeli „jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią". Motyw 47 preambuły RODO, precyzując to wskazuje, że „(...) prawnie uzasadniony interes może istnieć wtedy, gdy zachodzi istotny i odpowiedni rodzaj powiązania między osobą, której dane dotyczą a administratorem, na przykład, gdy osoba, której dane dotyczą jest klientem administratora". W zakresie w jakim konsument decyduje o przystąpieniu do konkursu „osoba, której dane dotyczą, ma rozsądne przesłanki by spodziewać się, że może nastąpić przetwarzanie danych w tym celu". Administrator danych osobowych organizując konkurs, jest więc uprawniony oprzeć przetwarzanie danych osobowych w takim przypadku na podstawie prawnie uzasadnionego interesu.



11.2018

• Projekt: Wydział Komunikacji, Ministerstwo Cyfryzacji •