RODO - blaski i cienie nowej regulacji unijnej

W dniu 25 maja 2018 roku zaczęło obowiązywać w Polsce 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) – RODO.

Od tej daty w całej Unii Europejskiej obowiązuje jeden zbiór przepisów dotyczących ochrony danych mający zastosowanie do wszystkich firm prowadzących działalność w UE, niezależnie od miejsca ich siedziby.

Wprowadzane przepisy zaostrzają zasady dotyczące ochrony danych:

- obywatele zyskają większą kontrolę nad swoimi danymi osobowymi
- przedsiębiorcy otrzymają korzyści wynikające z równych warunków działania.

W ślad za RODO została znowelizowana w Polsce ustawa o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).

Obecnie organem właściwym do spraw ochrony danych osobowych na terytorium Polski jest Prezes Urzędu Ochrony Danych Osobowych- PUODO utworzony ustawą z 10 maja 2018 r. o ochronie danych osobowych. Jest to również organ nadzorczy w rozumieniu RODO. Prezes Urzędu jest prawnym kontynuatorem Generalnego Inspektora Ochrony Danych Osobowych- GIODO. Zachował jego majątek, wierzytelności oraz przejął wszczęte przez niego postępowania. Prezesa Urzędu powołuje i odwołuje Sejm za zgodą Senatu. Kadencja Prezesa Urzędu trwa 4 lata, licząc od dnia złożenia ślubowania. Prezes Urzędu po upływie kadencji wykonuje swoje obowiązki do czasu objęcia stanowiska przez nowego Prezesa. Obecnym Prezesem Urzędu jest od 16 maja 2019 r. Jan Nowak.

Czym zajmuje się PUODO?

W przypadku naruszenia przepisów o ochronie danych osobowych, osoba, której dane dotyczą, może złożyć skargę do Prezesa Urzędu Ochrony Danych Osobowych. Po przeprowadzeniu postępowania w sprawie, Prezes Urzędu – jeżeli doszło do naruszenia – w drodze decyzji administracyjnej nakazuje przywrócenie stanu zgodnego z prawem. PUODO nakłada kary pieniężne za naruszenie przepisów o ochronie danych osobowych.

Od decyzji PUODO można odwołać się do sądu administracyjnego.

UODO zajął się wieloma sprawami z zakresu stosowania RODO.

Najwyższą karę za naruszenie prawa o ochronie danych osobowych otrzymała Spółka Bisnode. Dr Edyta Bielak-Jomaa, ówczesny prezes UODO ukarała jedną z firm zajmujących się dostarczaniem informacji o kontrahentach. Zarzuciła jej, że nie dopełniła obowiązku

informacyjnego wobec osób prowadzących jednoosobową działalność gospodarczą i nałożyła 220 tys. euro kary. Chodzi o dane 3,6 mln osób prowadzących aktualnie działalność gospodarczą i 2,33 mln tych, którzy ją zawiesili. Firma będąc świadoma podjętej przez Urząd Ochrony Danych Osobowych decyzji poinformowała, że **nie planuje wykonać obowiązku informacyjnego wobec osób, co do których nie ma adresu mailowego. Skłania się do usunięcia ich rekordów ze swojej bazy.** Jednocześnie spółka podkreśla, że kwestionuje interpretację UODO dotyczącą proporcjonalnego wysiłku. Jak podaje spółka w przypadku posiadania adresu mailowego (posiadali 679 000 adresów mailowych) obowiązek informacyjny został spełniony poprzez wysyłanie wiadomości na znane adresy mailowe. Żądanie dodatkowego wysłania informacji na 5,7 miliona adresów właścicieli spółek jednoosobowych oraz członków zarządów między innymi pocztą tradycyjną lub telefonicznie, nie może być postrzegane jako podejmowanie proporcjonalnych starań. Dlatego spółka miała zamiar odwołać się do Wojewódzkiego Sądu Administracyjnego, a jeśli będzie tak potrzeba również do Trybunału Sprawiedliwości UE. W tej sprawie wydaje się naturalnym zadanie pytania prawnego do TSUE – ocenił dr Paweł Litwiński, adwokat, partner w kancelarii Barta Litwiński. - **Pojęcie niewspółmiernie dużego wysiłku** było znane już w dyrektywie 95/46/WE, a **nigdy nie było interpretowane na poziomie europejskim. Co więcej, z wypowiedzi samej spółki wynika, że była kontrolowana w innych krajach UE, gdzie stosuje te same praktyki i te praktyki nie zostały zakwestionowane. Mamy więc przykład braku spójności w stosowaniu przepisów RODO, a przecież zapewnienie tej właśnie spójności było jednym z celów przyjęcia RODO** - podkreśla Paweł Litwiński. Zdaniem spółki udzielanie informacji poprzez kanały cyfrowe, pocztą elektroniczną lub umieszczanie ogłoszeń w ogólnopolskich portalach informacyjnych jest bardziej pożądane, zarówno przez odbiorców, jak i wysyłających. Dr Mirosław Gumularz, radca prawny z kancelarii GKK Gumularz Kozik uważa jednak, że to, czy to dobry sposób powinno wynikać z analizy ryzyka. - Dopiero analiza ryzyka może wskazać, czy sposób realizacji wymogu przewidziany przez administratora (np. wysyłka listu, telefonicznie, w mediach, etc.) jest odpowiedni. Urząd słusznie zwrócił uwagę, że brak spełnienia obowiązku informacyjnego może być źródłem ryzyka (np. możliwość pozbawienia praw). Nie mniej brakuje informacji co do jego poziomu. Czy jest ono wysokie, niskie, etc.?. A to jest kluczowe. Zadał pytanie czy Urząd weryfikował jak spółka szacowała ryzyko? Czy w ogóle spółka je szacowała? Z decyzji to wprost nie wynika - podkreślił Mirosław Gumularz (prawo.pl- *https://www.prawo.pl › kogo-ukaral-uodo-za-naruszenie-rodo,391858).*

Informacyjnie można podać, że pierwszą nałożoną karą przez Urząd była kara w wysokości 943 tys. zł. za niedopełnienie obowiązku informacyjnego.

Jak z tego wynika Urząd korzysta ze swoich prerogatyw i jeżeli w wyniku kontroli stwierdzi uchybienia w zakresie stosowania RODO nie wacha się sięgać bo wysokie kary finansowe.
Zamierzeniem RODO jest ochrona podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych.
RODO rozpoczyna się od motywów jest ich 173. Znajomość tych ogólnych klauzul jest istotna i pomaga zrozumieć często wydawałoby się niejednoznaczne sformułowania artykułów.
Jak wyżej wspomniano ma ono zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną w krajach należących do Unii Europejskiej.
Żeby właściwie odczytywać ten akt prawny to oprócz zakresu terytorialnego uregulowanego w art. 3 ważne są podstawowe definicje takie jak: administrator, dane osobowe, przetwarzanie, profilowanie pseudonimizacja; dlatego w tym miejscu postaram się je przybliżyć. Przez administratora należy rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innym ustala cele i sposoby przetwarzania danych osobowych. Dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, w szczególności imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy, jeden lub kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adoptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowanie lub łączenie, ograniczanie, usuwanie lub niszczenie. Profilowanie to dowolna forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się. Natomiast pseudonumizacja oznacza przetworzenie danych osobowych w taki sposób by nie można już było ich przypisać konkretnej osobie, której dane dotyczą bez użycia dodatkowych informacji.
Jak wynika z przytoczonych definicji są to pojęcia bardzo szerokie do tego stopnia, że powstała wątpliwość czy posiadanie kalendarza z wizytówkami implikuje konieczność stosowania rygorów z RODO. Cała trudność polega na właściwej interpretacji żeby zachować się zgodnie z prawem, a jednocześnie uniknąć absurdalnych rozwiązań.

Zgodność przetwarzania danych osobowych jest spełniona jeżeli zachodzi jeden z poniższych warunków (art. 6):

- osoba której dane dotyczą wyraziła zgodę;
- jest niezbędne:

do wykonania umowy;

do wykonania obowiązku prawnego administratora;

do ochrony żywotnych interesów osoby;

do wykonania zadania realizowanego w interesie publicznym (e);

do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub osobę trzecią (f).

Jeżeli przetwarzanie danych odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą wyraziła taką zgodę. Zgoda musi być pisemna. Zapytanie o zgodę musi być przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej łatwo dostępnej formie, jasnym i prostym językiem. Zgoda może zostać w dowolnym momencie wycofana. Wycofanie zgody musi być równie łatwe jak jej złożenie.

Administrator podczas pozyskiwania danych osobowych podaje następujące informacje : swoją tożsamość i dane kontaktowe, dane kontaktowe inspektora danych osobowych, cel przetwarzania oraz podstawę prawną, a także gdy jest to wymagane prawnie uzasadniony interes administratora lub strony trzeciej (art. 6 ust. 1 f), informacje o odbiorcach lub kategoriach odbiorców, jeżeli ma to zastosowanie informacje o zamiarze przekazania danych do państwa trzeciego lub organizacji międzynarodowej. W tym celu opracowuje się klauzule informacyjne, które dostarcza się osobie, której dane mają być przetwarzane.

Natomiast jeżeli danych osobowych nie pozyskano od osoby, której dotyczą to administrator jest zobowiązany wypełnić obowiązek informacyjny z art. 14 RODO, ale może zwolnić się z tego obowiązku w przypadku gdy osoba, której dane dotyczą, dysponuje tymi informacjami, udzielenie takich informacji okazuje się nie możliwe lub wymagałoby niewspółmiernie dużego wysiłku, pozyskanie lub ujawnienie jest wyraźnie uregulowane prawem UE lub państwa członkowskiego, dane muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej.

Osoba, której dane są przetwarzane ma prawo dostępu do tych danych, sprostowania, ograniczenia przetwarzania oraz żądania usunięcia - tak zwane prawo do bycia zapomnianym. Żeby skorzystać z tego prawa muszą być spełnione warunki opisane z art. 17 RODO.

Ważnym także uprawnieniem dla osób fizycznych jest prawo do zgłoszenia sprzeciwu. Osoba, której dane dotyczą ma prawo w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już

przetwarzać tych danych chyba, że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą.
Generalnie zabronione jest przetwarzanie danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej chyba, że osoba , której dane dotyczą wyraziła zgodę lub prawo UE lub państwa członkowskiego przewiduje, iż taka osoba nie może uchylić się zakazu, o którym mowa powyżej. Zresztą wyjątków od tego zakazu jest więcej i opisane są one szczegółowo w art. 9 ust.2 RODO.
Administrator jest odpowiedzialny za przestrzeganie zasad dotyczących przetwarzania danych osobowych i musi być w stanie wykazać ich przestrzeganie (zasada rozliczalności).
Administrator zobowiązany jest więc wdrażać odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to udowodnić gdy zajdzie taka potrzeba.
Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania są oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy określają zakresy swojej odpowiedzialności chyba, że przypadające im obowiązki określa prawo UE lub państwa członkowskiego.
Administrator może powierzyć przetwarzanie danych osobowych innemu podmiotowi. Jeżeli przetwarzanie ma być dokonane w imieniu administratora zobowiązany jest on korzystać wyłącznie z usług tych podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dotyczą.
W tym miejscu chcę wskazać najświeższą sprawę, która dotyczy kary 40 tysięcy złotych, którą nałożył Urząd Ochrony Danych Osobowych na burmistrza Aleksandrowa Kujawskiego. To pierwsza taka kara dla instytucji publicznej. Samorząd udostępnił dane osobowe zewnętrznej firmie bez podstawy prawnej. Urząd Ochrony Danych Osobowych dopatrzył się nieprawidłowości przy prowadzeniu Biuletynu Informacji Publicznej w urzędzie miejskim w Aleksandrowie Kujawskim. Dwie spółki obsługiwały tam stronę internetową urzędu. Pierwsza udostępniła biuletyn ze swoich serwerów, a druga dostarczała oprogramowanie do stworzenia i serwisowania BIP. Prezes UODO stwierdził, że obie firmy dysponowały danymi osobowymi, ale nie było żadnej podstawy prawnej. Samorząd nie zawarł bowiem umowy powierzenia przetwarzania danych osobowych. A to już naruszenie RODO (Rzeczpospolita - *https://www.rp.pl › Prawo › Samorząd › Zadania).*

Każdy administrator lub jego przedstawiciel prowadzi rejestr czynności przetwarzania danych, za

który odpowiada.

Administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne aby zapewnić odpowiedni stopień bezpieczeństwa przetwarzania danych. W tym celu stosuje się m. in. pseudonimizację i szyfrowanie oraz zabezpieczenie poufności, integralności, dostępności i odporności systemów i usług przetwarzania.

W tym zakresie ważne jest orzeczenie WSA w Krakowie z dnia 09.04.2019, sygn. II SA/Kr 133/2019, w którym sąd stwierdził, że w razie kolizji między zasadą jawności informacji publicznych , a ochrona prywatności i danych osobowych osób fizycznych, dopuszczalny będzie jedynie taki sposób udostępniania informacji publicznej, który nie naruszy dóbr chronionych (np. anonimizacja danych wrażliwych). W przypadku gdy pomimo dokonania takiego zabiegu możliwa będzie identyfikacja osoby, której dane dotyczą należy odmówić udostępnienia informacji publicznej.

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki (w miarę możliwości nie później niż 72 godz. od naruszenia) zgłasza je organowi nadzorczemu. W prawie polskim- jak wyżej wspomniano- takim organem jest PUODO.

Aby przyczynić się do spójnego stosowania RODO organy nadzorcze krajów unijnych współpracują ze sobą, a także z Komisją Europejską stosując mechanizm spójności, o którym mowa w art. 63 i następnych. W tym też celu powołano Europejską Radę Ochrony Danych, która monitoruje, doradza, wydaje wytyczne, opinie i rozstrzyga spory.

Ważnym punktem unijnego rozporządzenia są środki ochrony prawnej, odpowiedzialność i sankcje za niestosowanie się do przepisów dotyczących ochrony danych osobowych.

Sprawą przed Trybunałem Sprawiedliwości, która w ostatnich latach była niezwykle istotna, była sprawa C-131/12, *Google Spain*. W wyroku Trybunał odniósł się nie tylko do kwestii tzw. prawa do bycia zapomnianym, ale także, czemu poświęcono znacznie mniej uwagi, do zagadnienia zakresu terytorialnego stosowania przepisów dyrektywy 95/46/WE. W swoim rozstrzygnięciu Trybunał uznał hiszpańską jurysdykcję nad administratorem danych osobowych mającym swoją siedzibę w Stanach Zjednoczonych. W tym celu Trybunał dokonał wykładni przepisów dyrektywy 95/46/WE w zakresie prowadzenia działalności gospodarczej. Trybunał uznał, iż art. 4 ust. 1 lit. a dyrektywy 95/46/WE należy interpretować w ten sposób, że przetwarzanie danych osobowych ma miejsce w ramach działalności gospodarczej prowadzonej przez administratora danych odpowiedzialnego za to przetwarzanie na terytorium danego państwa członkowskiego w rozumieniu tego przepisu, jeśli operator wyszukiwarki internetowej ustanawia w danym państwie członkowskim oddział lub spółkę zależną, których celem jest promocja i sprzedaż powierzchni reklamowych oferowanych za pośrednictwem tej wyszukiwarki, a działalność tego

oddziału lub spółki zależnej jest skierowana do osób zamieszkujących to państwo. Wyrok ten zaskoczył samego powoda w sprawie, Google Inc., który pozwał hiszpański organ ochrony danych osobowych po to, żeby potwierdzić brak jego jurysdykcji nad tym zarejestrowanym w amerykańskim stanie Kalifornia internetowym gigantem. Trybunał jednoznacznie wskazał, że szeroka wykładnia art. 4 ust. 1 lit. a dyrektywy 95/46/WE jest niezbędna, gdyż ma na celu, w dobie społeczeństwa informacyjnego, zapobieżenie pozbawiania jednostek ochrony ich danych osobowych: „(...) z motywów 18–20 i z art. 4 dyrektywy 95/46/WE wynika, iż celem prawodawcy unijnego było niedopuszczenie do pozbawienia jednostek ochrony, do której mają one prawo na mocy tej dyrektywy, i dlatego przewidział on w przypadku tejże ochrony szczególnie szeroki terytorialny zakres jej zastosowania.

Odmiennie niż w wyroku w sprawie C-131/12, *Google Spain,* w sprawie C-230/14, *Weltimmo,* problemy w zakresie jurysdykcji dotyczyły ustalenia prawa właściwego wewnątrz Unii Europejskiej: czy do działania w przedstawionym stanie faktycznym uprawniony jest organ nadzorczy ze Słowacji, czy z Węgier, a także w zgodzie z którymi regulacjami krajowymi powinno się ono odbyć. Weltimmo, spółka prawa słowackiego, twierdziło, że prowadzi działalność gospodarczą wyłącznie w Słowacji, tj. w państwie członkowskim, w którym posiada siedzibę rejestrową. Jednocześnie węgierski organ nadzorczy, opierając się na wykładni art. 4 ust. 1 lit. a dyrektywy 95/46/WE, uznał swoją właściwość względem tej spółki, argumentując, że działalność Weltimmo, operatora strony internetowej z ogłoszeniami, koncentrowała się na terytorium Węgier.

Także i w tej sprawie Trybunał wskazał jako słuszną szeroką interpretację art. 4 ust. 1 lit. a dyrektywy 95/46/WE, uwzględniając przy swojej ocenie rolę internetu. Zgodnie ze stanowiskiem Trybunału z przepisów dyrektywy 95/46/WE wyłania się „elastyczna koncepcja pojęcia prowadzenia działalności gospodarczej, odbiegająca od podejścia formalistycznego, zgodnie z którym przedsiębiorstwo prowadzi działalność gospodarczą wyłącznie w miejscu, w którym jest zarejestrowane. Tym samym w celu ustalenia, czy dana spółka będąca administratorem danych prowadzi działalność gospodarczą w rozumieniu dyrektywy 95/46/WE w innym państwie członkowskim niż państwo członkowskie lub trzecie, w którym jest zarejestrowana, należy ocenić stopień stabilności rozwiązania organizacyjnego, jak również faktyczny charakter prowadzenia działalności w tym drugim państwie członkowskim, z uwzględnieniem szczególnego charakteru rozpatrywanej działalności gospodarczej oraz świadczenia rozpatrywanych usług. Dotyczy to w szczególności przedsiębiorstw, które zajmują się oferowaniem usług wyłącznie za pośrednictwem internetu. Jednocześnie Trybunał przyjął bardzo szerokie rozumienie pojęcia „prowadzenia działalności gospodarczej", zakładając, iż „obecność pojedynczego przedstawiciela może w pewnych okolicznościach wystarczyć, aby

istniało stabilne rozwiązanie organizacyjne, jeżeli działa on z wystarczającym stopniem stabilności, przy pomocy niezbędnych środków do świadczenia konkretnych rozpatrywanych usług, w danym państwie członkowskim. (orzeczenia za Polska i europejska reforma ochrony danych osobowych Bielak-Jomaa E. (red.), Lubasz D. (red.), Banyś T.A.J., Byczkowski M., Chomiczewski W., Czerniawski M., Kaczmarek-Templin B., Kaczorowski M., Karwala D., Kawczyński P., Kawecki M., Konarski X., Kuba M., Lewiński A., Litwiński P., Łuczak J., Piech M., Sibiga G., Witkowska K., Wyka T. WK 2016).
Chociaż orzeczenia te wydano pod rządami poprzedniego rozporządzenia, które obecnie zostało zastąpione RODO to utrzymują one nadal swoją aktualność.

Wracając do polskiego ustawodawstwa należy stwierdzić, że administrator odpowiada przed organem nadzorczym, a także przed osobą fizyczną, której prawa naruszył.
Organ nadzorczy nakłada kary pieniężne rozpatrując indywidualnie każdy przypadek, Kary mają być skuteczne, proporcjonalne i odstraszające. Stad możliwość nakładania wysokich kar do 10.000.000 EUR/20.000.000 EUR, a w stosunku do przedsiębiorstw do 2%/ 4% całkowitego rocznego światowego obrotu z poprzedniego roku. (art. 83 RODO).
Z przeglądu decyzji wydawanych przez PUODO wynika, że oprócz decyzji odmawiających uwzględnienia wniosku lub umarzających postepowanie są też decyzje w których organ przychyla się do skarg osób fizycznych i nakłada kary na administratora.
Jak wyżej wspomniano każda osoba, której dane dotyczą ma prawo wnieść skargę do organu nadzorczego jeżeli uważa, że przetwarzanie jej danych osobowych narusza przepisy RODO. Od decyzji organu nadzorczego (w naszym przypadku PUODO) przysługuje odwołanie do sądu administracyjnego. Postępowanie przed organem administracyjnym jest jednoinstancyjne, a przed sądem dwuistancyjne.
Oprócz kar pieniężnych nakładanych na administratora (o których powyżej) administrator ponosi odpowiedzialność w stosunku do osoby, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia postanowień unijnego rozporządzenia. Administrator lub podmiot przetwarzający może zwolnić się z tej odpowiedzialności jeżeli wykaże, że nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody.
W zakresie stosowania RODO na uwagę zasługuje Komentarz RODO. Ogólne rozporządzenie o ochronie danych autorów: Edyta Bielak-Jomaa (red.), Dominik Lubasz (red.), Witold Chomiczewski, Michał Czerniawski, Piotr Drobek, Urszula Góral, Magdalena Kuba, Joanna Łuczak, Paweł Makowski, Katarzyna Witkowska-Nowakowska, Natalia Zawadzka WKP, 2018, a także Komentarz do art.1 rozporządzenia nr 2016/679 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) Pawełа Fajgielskiego WKP, 2018.
Warto wskazać, że z komentarzy praktycznych ukazało się opracowanie Wojciecha Kapicy- RODO a prawo bankowe. LEX/el. 2019 oraz praca pod redakcją Wojciecha Kapicy, Michał Ćwiakowski, Maciej Gawroński, Joanna Grynfelder, Wojciech Ługowski, Radosław Obczyński, Andrzej Otto, Elwira Patsiotos, Beata Paxford, Zuzanna Piotrowska, Jakub Stolarczyk- Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Praktyczny przewodnik.

Trzeba wyraźnie podkreślić, że RODO w bardzo szerokim zakresie dotyczy banków. Z tego też powodu Związek Banków Polskich z udziałem przedstawicieli wszystkich większych banków w Polsce opracował Kodeks dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe. Można to określić jako „podręcznik" właściwego postępowania przez banki w zakresie ochrony danych osobowych.
Jak wspomniano należy postępować tak aby wypełniać należycie obwiązki unijnego rozporządzenia przy jednoczesnym niezakłóconym prowadzeniu usług bankowych.
Przeanalizujmy najczęściej wykonywane czynności bankowe takie jak przelewy zewnętrzne. Czy Bank realizując przelew dla Klienta ma obowiązek informacyjny z RODO?
Zgodnie z opinią dr Arwida Mednisa przy przelewach należy ograniczyć dane osobowe i posługiwać się wyłącznie imieniem i nazwiskiem bez podawania adresu zamieszkania. W takim wypadku można byłoby rozważyć, że obowiązek informacyjny nie występuje.
Biorąc pod uwagę ilość realizowanych takich usług jak przelewy trzeba mieć także na uwadze aby przyjęte rozwiązanie nie było antybiznesowe i antyklientowskie.
Częstym instrumentem, którym posługują się klienci banków jest polecenie zapłaty. Usługa ta daje poczucie bezpieczeństwa, iż należność zostanie zapłacona (jeżeli oczywiście są środki na rachunku) bez dodatkowych czynności po stronie płatnika wszystko samodzielnie wykona Bank. Usługa ta polega na tym, że klient Banku będący odbiorcą w usłudze polecenia zapłaty uzyskuje od swojego kontrahenta (płatnika) pisemne zgody na obciążanie rachunku, następnie klient dostarcza paczkę zgód do Banku. Pracownik Banku przekazuje je do banku płatnika celem ich weryfikacji i akceptacji/odrzucenia zgody. Na formularzu zgody umieszczone są dane płatnika takie jak: imię, nazwisko, adres zamieszkania, numer rachunku oraz podpis płatnika. Nie są podawane dane takie jak pesel, czy numer dowodu osobistego. Dokumenty papierowe zgód są archiwizowane w Banku. W umowie podpisanej z klientem obecnie nie ma klauzuli o przetwarzaniu danych osobowych osób trzecich (płatników).

W związku z powyższym powstaje pytanie jak Bank powinien zachować się i czy usługa polecenia

zapłaty będzie podlegała wszelkim rygorom z RODO ?

Jak wyżej wspomniano polecenia zapłaty są jedną z form płatności, którą klienci realizują za pośrednictwem banków. Bank w swojej działalności opiera się na przepisach prawa w tym działa zgodnie z ustawą prawo bankowe i ustawą o usługach płatniczych. Zgodnie z art. 3 ust. 2 ustawy o usługach płatniczych „polecenie zapłaty oznacza usługę płatniczą polegającą na obciążeniu określoną kwotą rachunku płatniczego płatnika na skutek transakcji płatniczej zainicjowanej przez odbiorcę, dokonywanej na podstawie zgody, której płatnik udzielił odbiorcy, dostawcy lub dostawcy płatnika". Jak wynika z treści przepisu, zgoda płatnika jest elementem niezbędnym do wykonania przez Bank odbiorcy płatności w ramach tej usługi.

W związku z powyższym można rozważyć w tej usłudze wyłączenie z obowiązku informacyjnego na podstawie: art. 14 ust. 5 lit c) pozyskanie tych informacji jest uregulowane prawem, art. 14 ust. 5 lit d) dane osobowe muszą pozostać poufne w związku z obowiązkiem zachowania poufności. W przeciwnym wypadku banki byłyby zobowiązane osobom, z którymi de facto nie łączy ich żaden stosunek prawny do wręczanie klauzul informacyjnych.

Druga często wykonywaną czynnością po stronie Płatnika, jest wnoszenie opłat za pomocą tak zwanych opłatomatów. Tu też pojawia się zagadnienie związane z ochroną danych osobowych.

Bank oferuje urządzenia – opłatomaty, które pozwalają na dokonanie opłat administracyjnych na rzecz urzędu przez osoby fizyczne. Często urzędy wymagają aby przy dokonywaniu płatności osoby fizyczne podawały swoje dane osobowe: imię i nazwisko, pesel, adres zamieszkania. Dane te są przetrzymywane w dziennikach urządzeń i są przekazywane do systemów bankowych w tytule przelewu.

W związku z powyższym obecnie osoby fizyczne aby dokonać opłaty akceptują na ekranie opłatomatu klauzulę zgodną z zapisami RODO. Bez akceptacji tej klauzuli wykonanie zapłaty w opłatomacie nie jest możliwe.

Obecnie obserwujemy bum w budownictwie. Powstają nowe domy, osiedla, apartamentowce. Zatrzymajmy się na chwilę nad rolą dewelopera i banku przy przetwarzaniu danych osobowych nabywców w związku z prowadzeniem przez bank mieszkaniowych rachunków powierniczych, do których banki są zobowiązanie zgodnie z ustawą o ochronie praw nabywcy lokalu mieszkalnego lub domu jednorodzinnego.

Należy wyraźnie stwierdzić, że deweloper musi spełnić obowiązek informacyjny wobec nabywców lokali wynikający z RODO., ale co z bankiem ? Czy możliwe jest zastosowanie zwolnienia z wykonywania obowiązku informacyjnego na podstawie art. 14 ust. 5 lit. c?

Jeżeli chodzi o bank to w tym wypadku można rozważyć wyłączenie tego obowiązku właśnie na w/w podstawie prawnej (art. 14 ust. 5 lit. c). Zgodnie z lit. c) bank mógłby się powołać na przepisy prawa krajowego - ustawę deweloperską, która w art. 5 nakazuje bankom prowadzenie

rachunków powierniczych i co za tym idzie konieczność przetwarzania danych nabywców lokali przez Bank w celu prowadzenia czynności ewidencyjnych.
Często klienci korzystają też usługi bakowej „ masowe wypłaty „
Usługa polega na realizacji przez Bank gotówkowych zleceń płatniczych przesyłanych plikowo systemem bankowości elektronicznej przez płatnika (klienta Banku), wystawionych na rzecz wskazanych przez niego świadczeniobiorców, beneficjentów wypłat, z którymi Bank nie posiada żadnych relacji. Do wejścia w życie RODO banki w ramach świadczonej usługi zawierały umowę dwustronną, w której znajdowały się zapisy dotyczące powierzenia bankowi przetwarzania danych osobowych beneficjentów, w zakresie niezbędnym do wykonania usługi zgodnie z tą umową.
Obecnie sytuacja nie uległa zasadniczej zmianie i przeważa koncepcja podobna do przelewów zewnętrznych tj. brak obowiązku informacyjnego. W szczególności, że poza imieniem i nazwiskiem nie są prezentowane żadne dodatkowe elementy w tym adres zamieszkania, pesel itp.

Ostatnia poważna polemika Związku Banków Polskich (ZBP) z UODO dotyczy zakazu wykonywania replik dokumentów publicznych. PUODO uważa, że kopie dokumentów powinny być wykonywane przez bank tylko w określonych sytuacjach; praktyka nie powinna być stosowana np. przy zakładaniu konta, sprawdzania zdolności kredytowej, czy zawierania umowy kredytowej. Natomiast zdaniem ZBP art. 112 b ustawy prawo bankowe stanowi, że banki mogą przetwarzać dane osobowe osób zawarte we wszystkich dokumentach tożsamości o ile ich przetwarzanie jest związane z celem działalności bankowej.
Przepisem, który wprost mówi o możliwości sporządzania kopii dokumentów jest art. 34 ust. 1 ustawy z 01.03.2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowania terroryzmu. Zgodnie z tym przepisem instytucje obowiązane na potrzeby stosowania środków bezpieczeństwa finansowania mogą przetwarzać informacje zawarte w dokumentach tożsamości i sporządzać ich kopie. Instytucje obowiązane z tym banki stosując środki bezpieczeństwa finansowego identyfikują osoby oraz weryfikują tożsamość. Nadto MSWiA wydało komunikat, z którego wynika, że prawo nie nakłada na banki kar za kopiowanie dokumentów. W związku z tym trzeba jasno stwierdzić, że nie ma jednolitości w tym zakresie, a pogląd UODO stoi w kolizji z poglądem ZBP i komunikatem MSWiA.

Podsumowując rozważania należy docenić intencje unijnego ustawodawcy bowiem ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 karty praw podstawowych UE oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii

Europejskiej stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących. Zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych nie mogą – niezależnie od obywatelstwa czy miejsca zamieszkania takich osób- naruszać ich podstawowych praw i wolności, w szczególności prawa do ochrony danych osobowych. Celem RODO jest przyczynianie się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz unii gospodarczej, do postępu społeczno-gospodarczego, do wzmacniania i konwergencji gospodarek na rynku wewnętrznym, a także pomyślności ludzi. Tak więc RODO harmonizuje ochrony podstawowych praw i wolności osób fizycznych w związku z czynnościami przetwarzania danych oraz zapewnienia swobodnego przepływu danych osobowych pomiędzy państwami członkowskimi. Przetwarzanie danych tak należy zorganizować, aby służyło to ludzkości. Prawo do ochrony danych osobowych nie jest prawem bezwzględnym; należy je postrzegać w kontekście jego funkcji społecznej i wyważać względem innych praw podstawowych w myśl zasady proporcjonalności. RODO nie narusza praw podstawowych, wolności i zasad uznanych w karcie praw podstawowych- zapisanych w Traktatach- w szczególności prawa do poszanowania życia prywatnego i rodzinnego, domu oraz komunikowania się, ochrony danych osobowych, wolności myśli, sumienia, i religii, wolności wypowiedzi i informacji, wolności prowadzenia działalności gospodarczej, prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu oraz różnorodności kulturowej, religijnej i językowej. Integracja społeczno-gospodarcza wynikająca z funkcjonowania rynku wewnętrznego doprowadziła do znacznego zwiększenia transgranicznych przepływów danych osobowych. Wzrosła wymiana danych osobowych pomiędzy podmiotami publicznymi i prywatnymi w tym m. in. osobami fizycznymi, zrzeszeniami, przedsiębiorcami w Unii. Od organów krajowych państw członkowskich prawo Unii coraz częściej wymaga, by w celu wykonania swoich obowiązków lub w celu realizacji zadań w imieniu organu innego państwa członkowskiego współpracowały ze sobą i wymieniały się danymi osobowymi. Szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacząco wzrosła. Dzięki technologii zarówno przedsiębiorstwa prywatne, jak i organy publiczne mogą na niespotykana dotąd skalę wykorzystać dane osobowe w swojej działalności. Osoby fizyczne coraz częściej udostępniają informacje osobowe i globalne. Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państwa trzecich i organizacji międzynarodowych, równocześnie zaś powinna zapewniać wysoki stopień ochrony danych osobowych. Przemiany wymagają stabilnych, spójniejszych ram ochrony danych w Unii oraz zdecydowanego ich egzekwowania, gdyż ważna jest budowa zaufania, która pozwoli na rozwój gospodarki cyfrowej na rynku wewnętrznym. Osoby fizyczne powinny mieć kontrolę nad

swoimi danymi osobowymi. (motywy RODO 1-7).

Aby zapewnić wysoki i spójny stopień ochrony osób fizycznych oraz usunąć przeszkody w przepływie danych osobowych w Unii, należy zapewnić równorzędny we wszystkich państwach stopień ochrony praw i wolności osób fizycznych oraz zapewnić spójne i jednolite w całej Unii stosowanie przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z ich przetwarzaniem.

Na koniec należy powrócić do tytułu artykułu i podkreślić, że słuszne założenia i cel RODO nie powinny spowalniać procesów biznesowych, które służą coraz efektywniejszej obsłudze osób fizycznych w różnych rodzajach dziedzin gospodarczych.

Jeszcze dzisiaj możemy nazywać RODO nową regulacją bowiem cały czas wszyscy uczymy się wprowadzanych regulacji popełniając błędy, których konsekwencje bywają często dotkliwe.

Marcjanna Rejman-Jędrczak- adwokat

Bibliografia:

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
2. Ustawa o ochronie danych osobowych Dz.U. z 2018 r. poz. 1000
3. Ustawa o usługach płatniczych Dz. U. 2019.659-jt
4. Ustawa prawo bankowe DZ.U.2018.2187 tj
5. Ustawa o ochronie praw nabywcy lokalu mieszkalnego lub domu jednorodzinnego Dz. U. z 2019 r. poz. 1805- tj.
6. Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowania terroryzmu Dz.U.2019.1115 -j.t.
7. Polska i europejska reforma ochrony danych osobowych Bielak-Jomaa E. (red.), Lubasz D. (red.), Banyś T.A.J., Byczkowski M., Chomiczewski W., Czerniawski M., Kaczmarek-Templin B., Kaczorowski M., Karwala D., Kawczyński P., Kawecki M., Konarski X., Kuba M., Lewiński A., Litwiński P., Łuczak J., Piech M., Sibiga G., Witkowska K., Wyka T. WK 2016
8. Komentarz RODO. Ogólne rozporządzenie o ochronie danych autorów: Edyta Bielak-Jomaa (red.), Dominik Lubasz (red.), Witold Chomiczewski, Michał Czerniawski, Piotr Drobek, Urszula Góral, Magdalena Kuba, Joanna Łuczak, Paweł Makowski, Katarzyna Witkowska-Nowakowska, Natalia Zawadzka WKP, 2018

9. Komentarz do art.1 rozporządzenia nr 2016/679 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) Pawełа Fajgielskiego WKP, 2018
10. Wojciech Kapica- RODO a prawo bankowe. LEX/el. 2019
11. Wojciech Kapica (redaktor), Michał Ćwiakowski, Maciej Gawroński, Joanna Grynfelder, Wojciech Ługowski, Radosław Obczyński, Andrzej Otto, Elwira Patsiotos, Beata Paxford, Zuzanna Piotrowska, Jakub Stolarczyk- Przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. Praktyczny przewodnik.