Biuletyn edukacyjny BODiE
Nr 1/07/2018

PSD 2: szanse i wyzwania dla bankowości spółdzielczej

Małgorzata Azembska

Polska, podobnie jak kilka innych państw, nie zdążyła na czas z wdrożeniem unijnej dyrektywy PSD 2. Termin minął 13 stycznia br. Co trzeci polski bank traktuje nowe rozwiązania jako szansę. Jednak 14% banków obawia się ich, upatrując w nich rozmaite zagrożenia dla swojej działalności.

Dyrektywa PSD 2 zawierająca unijne przepisy o usługach płatniczych przynosi wiele istotnych zmian. W swoim założeniu, wprowadzą one w obszarze usług płatniczych większą przejrzystość i bezpieczeństwo transakcji. Dyrektywa ma sprzyjać wzrostowi konkurencji, poprawić spójność prawa oraz uzupełnić istniejące już regulacje, dostosowując je do rozwijających się nowych technologii, a także ujednolicić rynek płatności w UE. Tym samym PSD 2 ma wpłynąć na działalność wielu instytucji, m.in. banków, instytucji płatniczych, podmiotów oferujących karty sklepowe i karty paliwowe oraz niezależnych operatorów bankomatów czy innych niebankowych dostawców usług płatniczych.

Dlaczego nowa dyrektywa?

PSD 2 całkowicie zastąpi poprzednie przepisy, wprowadzone przez funkcjonującą w Polsce od 2011 r. tzw. pierwszą PSD. Od tamtego czasu wiele się jednak zmieniło – ludzie powszechnie zaczęli korzystać z płatności elektronicznych i realizować je przy użyciu urządzeń przenośnych. Na rynku pojawiły się całkiem nowe rodzaje usług płatniczych, takie jak np. usługi inicjowania transakcji płatniczej, dostępu do informacji o rachunku oraz usługi potwierdzania dostępności środków na rachunku płatniczym. Wchodząca w życie dyrektywa reguluje m.in. zasady ich świadczenia. Zadbano też o bezpieczeństwo płatności i danych użytkowników. Wprowadzono m.in. „otwartą bankowość" umożliwiającą klientom zarządzanie kontami od różnych dostawców za pomocą jednej aplikacji.

Największą zmianą, jaką niesie ze sobą PSD 2 dla wszystkich banków, nie wyłączając spółdzielczych, a także ich klientów, jest wprowadzenie nowego typu instytucji płatniczych. Jedne będą inicjować płatność, a dokładniej mówiąc, świadczyć usługi przeprowadzenia płatności w Internecie w imieniu klienta. Inne – usługi informacyjne o rachunku. Dostarczą one klientowi zagregowane informacje dotyczące posiadanych przez niego rachunków, przygotowując w miarę potrzeb, niezbędne analizy, czy porównania transakcji. Jak informuje Paweł Gałązka, ekspert ZBP, w naszym kraju tego typu podmioty już w jakimś zakresie funkcjonują, świadcząc np. usługi realizacji płatności w sklepach internetowych.

Bezpieczniej, czy mniej bezpiecznie?

Wszystkie nowe instytucje, wraz z wejściem dyrektywy, będą upoważnione do posiadania loginów i haseł do kont bankowych swoich klientów. Zainteresowanym podadzą te informacje np. na dedykowanej temu stronie danej instytucji płatniczej. To właśnie niepokoi cześć środowiska bankowego, dostrzegającego ryzyko związane ze stosowaniem nowych przepisów. System płatniczy musi być przecież niezawodny i dostępny. Istotne jest, by interesy klientów banków zostawały dobrze zabezpieczone, szczególnie w zakresie, ich prywatności i bezpieczeństwa obrotu elektronicznego. To jednak musi też kosztować.

– Dla banków spółdzielczych, które prowadzą rachunki płatnicze, ta dyrektywa oznacza więc, że będą one musiały w bezpieczny sposób udostępniać dane zewnętrznym podmiotom, a to wymusza zmiany w architekturze IT poprzez przygotowanie API – przyznaje Bartosz Kublik, prezes Banku Spółdzielczego w Ostrowi Mazowieckiej.

Do momentu wejścia dyrektywy w życie, hasła oraz loginy do kont klienci wprowadzali jedynie na stronie www banku. To gwarantowało bezpieczeństwo środków. Wraz z nadchodzącymi zmianami, gdy dane te pozyskają podmioty trzecie, można obawiać się, że niektórzy klienci padną ofiarą oszustów. Jeśli tak się stanie, wpłynie to na zmniejszenie liczby transakcji w Internecie. Jak pokazuje historia, próbom wyłudzenia może nie przeszkadzać nawet fakt, że nowe instytucje prowadzące usługi płatnicze bezwzględnie muszą się zarejestrować i posiadać licencję KNF, zakładając nawet objęcie ich nadzorem UKNF.

RTS-y na pomoc

Dla poprawy bezpieczeństwa Komisja Europejska przyjęła rozporządzenie RTS, które wejdzie w życie we wrześniu 2019 r. RTS-y, czyli regulacyjne standardy techniczne, definiują kwestię dostępu do rachunków klientów. Mają zapewnić korzystanie z bezpieczniejszej i bardziej innowacyjnej elektronicznej bankowości. Określają wymagania dotyczące silnego uwierzytelniania SCA. By dokonać transferu środków, właściciel rachunku będzie musiał skorzystać równocześnie z co najmniej dwóch, a nawet z trzech dostępnych metod weryfikacji. Może to być hasło lub PIN oraz dodatkowo np. urządzenie mobilne, czy któreś z rozwiązań biometrycznych**.** Obostrzenia dotyczą jednak tylko rachunków wykorzystywanych do wykonywania transakcji płatniczych. RTS-y zobowiązują także każdego dostawcę usług płatniczych – o ile prowadzi rachunek dostępny za pośrednictwem Internetu – do udostępnienia co najmniej jednego interfejsu umożliwiającego komunikację z podmiotami trzecimi (TPP). Może on to zrobić np. poprzez modyfikację dotychczasowego systemu bankowości internetowej. KNF uznało jednak za bezpieczniejsze utworzenie dedykowanego interfejsu (API). Prowadzone są obecnie prace nad stworzeniem takiego standardu komunikacji z TPP. Patronuje im przede wszystkim Związek Banków Polskich.

Co na to banki?

Jak wskazują badania Deloitte, chociaż banki wyrażają wiele obaw, to prawie co trzeci traktuje dyrektywę PSD 2 jednak jako szansę. Najczęściej są to więksi gracze, ale nie tylko. Pozostali mają do czekających ich zmian stosunek neutralny, a 14% się ich wręcz obawia.

Z optymizmem podchodzi do nowej dyrektywy Bank Spółdzielczy w Jarocinie:

– Banki Spółdzielcze będą mogły zapewnić klientom dostęp do danych wszystkich rachunków klienta w różnych instytucjach finansowych, w tym w bankach komercyjnych oraz podmiotach gospodarczych. Klienci, poprzez bankowość elektroniczną lub aplikację mobilną Banku Spółdzielczego, sprawdzą saldo lub zainicjują płatności z rachunków, które posiadają w innych bankach. – przewiduje Jan Grzesiek, prezes BS w Jarocinie.Także Bartosz Kublik dostrzega w PSD 2 dużą szansę dla banków spółdzielczych:

– Niektóre z tych zmian mogą w znacznym stopniu korzystnie wpłynąć na sferę ekonomiczną sektora. Z całą pewnością wzbogacą wiedzę o klientach będących w portfelu BS poprzez ujawnienie nowych obszarów informacyjnych (produkty w innych bankach, bądź ich całkowity brak). Jeśli tę wiedzę mądrze się wykorzysta, skutkować to będzie silniejszym związaniem się z klientem, kompleksowym dostosowaniem do jego potrzeb. Może to wywoła skuteczniejszy cross selling usług w bankach spółdzielczych, którego brak jest, moim zdaniem, ogromną bolączką naszego sektora – mówi prezes Banku Spółdzielczego w Ostrowi Mazowieckiej.

Jak prognozuje Deloitte, wraz z wejściem nowych możliwości technicznych rozpocznie się walka o klientów. Głównie o tych, którzy dotychczas chętniej odwiedzali oddziały niż korzystali z innych rozwiązań, uważając je za zbyt czasochłonne i skomplikowane. W Polsce jest to ok. 20% właścicieli kont, czyli 5,2 mln osób. Nie będzie to jednak proste. Polacy są z natury nieufni i niechętnie udostępniają swoje dane osobowe. W trudnej sytuacji znajdą się szczególnie nowe instytucje płatnicze. Aż 43% osób uznało za niekomfortowe podzielenie się z nimi danymi dotyczącymi konta. Ale także banki będą chciały przecież pozyskiwać nowych klientów, a dotychczasowych skutecznie i przyjaźnie zachęcić do korzystania z nowych możliwości.

Jak twierdzi prezes Jan Grzesiek, trzeba działać. Jarociński bank wdraża więc nowoczesne oraz intuicyjne narzędzie bankowości internetowej eBank z trzema kanałami obsługi: przeglądarką internetową, przeglądarką mobilną oraz dedykowaną aplikacją na urządzenia mobilne. Przygotowuje się też do wdrożenia systemu płatności mobilnych BLIK i szybkich przelewów Bluecash.

Prace, by przystosować się do stawianych przez PS wymogów, trwają już w bankach spółdzielczych. Ponieważ Polska, jako kraj ma tu opóźnienie, nowe przepisy będą gotowe zapewne dopiero w czerwcu br. Dzięki temu banki zyskały nieco dodatkowego czasu. Także na zaktualizowanie umów z klientami o zmiany, które wprowadza dyrektywa – m.in. zostaną skrócone o połowę terminy na rozpatrywanie skarg z 30 do 15 dni, a także wprowadzone nowe zasady obsługi płatności nieautoryzowanych. Banki będą musiały to zrobić podczas sześciomiesięcznego vacatio legis.

Podzielona płatność w bankach

Małgorzata Azembska

Split Payment, system mający zapobiegać oszustwom na VAT, wchodzi w życie już od 1 lipca br. i banki muszą się dostosować do nowego prawa. Oznacza to, że i banki spółdzielcze, mają obowiązek założyć przedsiębiorcom dodatkowe rachunki, na które oddzielnie będzie odprowadzona należność VAT-owska.

Na razie jeszcze właściciele firm nie muszą korzystać z nowych rachunków – dla firm jest to dobrowolne. Jednak ustawodawca przewidział dla nich różne zachęty. Przedstawiamy pokrótce szczegóły dotyczące nowego prawa, będącego m.in. efektem dobrej współpracy środowiska bankowego z Ministerstwem Finansów oraz z Krajową Izbą Rozliczeniową.

Na czym to polega

Najpierw o tym, jak to wygląda od strony klientów. Tak zwany Split Payment (podzielona płatność) umożliwia podatnikowi, a zarazem klientowi banku, zapłatę kontrahentowi faktury VAT w dwóch strumieniach finansowych: netto i VAT. Kwota netto będzie do dyspozycji biznesowego partnera na starych zasadach, zaś VAT może, a nawet powinien wpływać na specjalnie dedykowane i założone klientowi konto.

„Dla banków system jest obligatoryjny, każdy bank ma obowiązek do 30.06.2018 utworzyć rachunki VAT swoim klientom firmowym – czytamy w stanowisku przesłanym przez SGB Bank. „Dobrowolność systemu leży wyłącznie po stronie płatnika faktury, ma on możliwość zdecydować, czy rozliczy się w dotychczasowej formule, czy w formule Split Payment. Odbiorca zlecenia musi odebrać zlecenie także w takiej formule, na jaką zdecydował się płatnik. Domyślnie zakłada się, że będzie utworzony co najmniej jeden rachunek VAT dla jednego klienta niezależnie od tego, ile posiada on rachunków rozliczeniowych. Klient będzie mógł wnioskować o otwarcie dodatkowych rachunków VAT w celu zapewnienia lepszej transparentności własnych operacji, a Bank każdorazowo będzie zobligowany, aby taki wniosek obsłużyć. SGB-Bank jest w trakcie testów technicznych i funkcjonalnych swojego rozwiązania. Wdrożenie rozwiązania zakładamy w drugiej połowie czerwca br. Posiadamy już systemy, które obsłużą zlecenia banków spółdzielczych w formule Split Payment, rozpoczynamy testy z bankami spółdzielczymi w celu potwierdzenia gotowości po stronie banków.” – poinformował redakcję SGB Bank. Należy pamiętać, że klient – przedsiębiorca, będzie miał ograniczone możliwości dysponowania znajdującymi się na rachunku VAT kwotami. Możliwości te sprowadzają się do opłacania VAT poddostawcom także na specjalne konto lub bezpośredniego odprowadzania podatku do izby skarbowej. Znowelizowana ustawa o VAT wprowadza przy tym system zachęt, który ma skłaniać przedsiębiorców do korzystania z rachunków vatowskich, zwłaszcza w tych przypadkach, w których przedsiębiorca może mieć wątpliwości, co do uczciwości swojego kontrahenta. Zachęty to m.in.: przyspieszony do 25 dni zwrot VAT, brak stosowania sankcji, zwolnienie z tzw. odpowiedzialności solidarnej.

– „Środki zgromadzone na tym rachunku będą należały do przedsiębiorcy, ale możliwość ich wykorzystania jest ustawowo ograniczona do wykonywania wyłącznie przelewów na inny rachunek VAT oraz opłacania zobowiązań podatkowych przedsiębiorcy – informuje redakcję Bank BPS. Bank BPS jest przygotowany do wdrożenia Mechanizmu Podzielonej Płatności. Zgodnie z harmonogramem przed 01 lipca 2018 r. zostaną dla wszystkich klientów posiadających rachunek rozliczeniowy otwarte rachunki VAT. (…). Jako Bank Zrzeszający opracowaliśmy stosowne wzorcowe regulacje produktowe, które zostaną udostępnione zrzeszonym Bankom Spółdzielczym, opracowujemy inne materiały informacyjne pomocne dla Banków Spółdzielczych, pośredniczymy w przekazywaniu aktualnych interpretacji Ustawy wypracowanych na forum Związków Banków Polskich”. Split Pay-

-ment jest jednym z rozwiązań proponowanych przez Komisję Europejską w „Studium wykonalności alternatywnych metod poprawy oraz uproszczenia poboru podatku VAT" („Study on feasibility of alternative methods for improving and simplyfing the collection of VAT through the means of modern technologies and/or financial intermediaries"). Uchodzi za bodaj najskuteczniejsze narzędzie zapobiegania oszustwom podatkowym.

Były pewne kontrowersje

Jeszcze przed przyjęciem przez sejm nowelizacji, sejmowa Komisja Finansów Publicznych nie wyraziła zgody na to, żeby – po wprowadzeniu podzielonej płatności VAT umożliwić bankom pobieranie opłat za prowadzenie rachunków VAT. Zdaniem wiceprezesa ZBP Jerzego Bańki, które wyraził podczas historycznego już posiedzenia Komisji, zapłacą za to pozostali klienci – w wyższych opłatach lub niższych odsetkach. Z pewnością sektor bankowy musi ponieść nakłady inwestycyjne, nawet rzędu kilkuset milionów złotych, ale taka była wola sejmu i rachunki będą darmowe. Za to zgłoszono i przyjęto wówczas kilka istotnych poprawek merytorycznych. Jedna z nich „ma na celu przyspieszenie doręczeń bankom oraz SKOK-om postanowień zawierających zgodę naczelnika urzędu skarbowego na przekazanie środków zgromadzonych przez podatnika rachunku VAT". Inna pozwala na to, by bank otwierał tylko jeden rachunek VAT dla wszystkich prowadzonych rachunków rozliczeniowych, zaś posiadacz tych rachunków mógł złożyć wniosek o prowadzenie więcej niż jednego rachunku VAT – o ile uzna to za wygodniejsze rozwiązanie. Pierwotnie projekt przewidywał, że do każdego rachunku rozliczeniowego miał być przypisany jeden rachunek VAT.

W Europie istnieją dwa sposoby korzystania ze Split Payment. Pierwszy polega na automatycznym, wspartym technologią IT, podziale kwoty brutto należności już w procesie płatności za towar lub usługę przez nabywcę. Kupujący towar czy usługę jednym poleceniem przelewu płaci za transakcje, ale kwota dzielona jest przez system na kwotę netto oraz kwotę podatku VAT. Za rozdzielenie płatności odpowiada automatyczny, specjalnie stworzony system rozrachunkowy, wykorzystywany do danego rodzaju płatności, lub sam bank. Drugi system to tzw. manualny Split Payment. Nabywca sam wylicza i rozdziela płatności dokonując przelewu na wartość płatności netto dla sprzedawcy oraz z osobnego przelewu – samego podatku na rachunek VAT.

System Split Payment zakłada, że dla danego okresu rozliczeniowego (miesięcznego/ kwartalnego) po złożeniu deklaracji przez podatnika, podatnik i organ podatkowy dokonują wzajemnych rozliczeń VAT w oparciu o złożoną deklarację oraz aktualny stan konta VAT. W efekcie przedsiębiorca od razu wie, czy ma podatek VAT do dopłaty, czy też może wystąpić o zwrot.

Obowiązek na przyszłość

Obowiązkowy Split Payment w niektórych obszarach wejdzie od 1 stycznia 2019 r., ewentualnie od pierwszego kwartału przyszłego roku – zapowiadał w mediach wiceminister finansów Paweł Gruza. Ale może to nastąpić dopiero po akceptacji Komisji Europejskiej. Obowiązkowa, podzielona płatność dotyczyłaby tylko tych obszarów, które Ministerstwo Finansów uznało za narażone na ryzyko wykorzystywania określonych towarów do wyłudzeń VAT. Na razie nie sprecyzowano jednak, które to miałyby być obszary.

Piotr Alicki, prezes zarządu Krajowej Izby Rozliczeniowej S.A.

Split Payment działa już w niektórych państwach europejskich, gdzie również ma za zadanie utrudnić powstawanie nadużyć i działania na szkodę budżetu państwa. Ministerstwo Finansów jest tu inicjatorem i wiodącym podmiotem. Zgodnie z założeniami Ministerstwa Finansów, mechanizm ma zapewnić poprawę ściągalności podatku o ponad 80 mld zł na przestrzeni 10 lat.

Ważną rolę do odegrania w redukcji luki podatkowej mają również systemy analityczne, które w sposób automatyczny mogą wskazać na podmioty podejrzane o unikanie podatków. Funkcjonowanie takich narzędzi wymaga ścisłej współpracy administracji państwowej oraz sektora bankowego. Takim właśnie narzędziem jest wdrożony przez KIR system STIR. Jego rolą jest automatyczna analiza danych z banków i SKOK-ów dotyczących poszczególnych firm i przekazywanie do Krajowej Administracji Skarbowej wyników analizy ryzyka. Na tej podstawie KAS może podjąć decyzję o przeprowadzeniu kontroli skarbowej w danej firmie.

Często mówiliśmy o konieczności sektorowego działania – choćby w zakresie cyberbezpieczeństwa czy rozwiązań antyfraudowych – i STIR jest odpowiedzią na te potrzeby. STIR pozwala zgromadzić informacje o wszystkich rachunkach podmiotów gospodarczych, przedsiębiorstw, itp. Następnie, stosując odpowiednie algorytmy, ocenia się prawdopodobieństwo tego, że dane rachunki, czy też ewentualnie dany obieg pieniądza, wskazuje na działanie tzw. karuzeli VAT-owskiej lub innego sposobu wykorzystywania rachunków bankowych w celu wyłudzeń VAT-owskich. Z szacunków Ministerstwa Finansów wynika, że m.in. dzięki samemu STIR, do budżetu może w ciągu 10 lat trafić dodatkowe 32,1 mld złotych.

Pod czujnym okiem kamer...

czyli o przesłankach przetwarzania przez pracodawcę danych osobowych pracowników na gruncie RODO

Marta Gosk, radca prawny, Kancelaria Radców Prawnych A. Pieścik, W. Pietrzykowski, W. Wolniewicz

Bank spółdzielczy, jako stabilny i solidny pracodawca, zobowiązany jest do gromadzenia danych osobowych pracowników w sposób adekwatny do osiągnięcia założonych celów, czy to w procesie rekrutacji, czy zatrudnienia pracownika. Stosowne wymogi w tym zakresie wprowadza 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) dalej: RODO, które należy stosować od dnia 25 maja 2018 r.

Przyczyn, dla których pracodawca wykonuje operacje na danych osobowych swoich pracowników, nie trzeba szukać daleko. Już sam proces rekrutacji wymaga przetworzenia danych osobowych kandydata – bo przecież dane osobowe konieczne są do nawiązania stosunku pracy, jego rozwiązania, a także w procesie planowania, zarządzania i organizowania pracy w sposób bezpieczny, prawidłowy i zapewniający ciągłość wykonywanych zadań, w tym także ochronę własności pracodawcy. Realizacji tych celów coraz częściej służą technologie umożliwiające śledzenie pracowników w miejscu pracy za pomocą urządzeń takich jak: monitoring wizyjny, kontrola dostępu do poszczególnych pomieszczeń (również z wykorzystaniem zabezpieczeń biometrycznych), ale również popularne – wyposażanie pracowników w pojazdy, smartfony, komputery osobiste, tablety, które gromadzą dane osobowe o swoich użytkownikach. O ile uzasadnionym z perspektywy banku spółdzielczego, jako instytucji zaufania publicznego (zobligowanej do dołożenia niezbędnych starań, by bezpieczeństwo środków zgromadzonych przez klientów było zapewnione, a dane objęte tajemnicą bankową nie zostały ujawnione postronnym osobom), jest cel w postaci wykrywania zachowań pracowników godzących w interesy klientów banku i samego banku, jako instytucji, o tyle zawsze należy mieć na uwadze, iż nowoczesne technologie monitorowania i komunikacji mogą mieć również, niepomiernie większy, negatywny wpływ na podstawowe prawa pracowników (w tym zachowania pewnych informacji jako poufnych). RODO wymaga wyważenia tych wartości tj. interesów administratora oraz praw i wolności osób fizycznych, których dane są przetwarzane. Zasada przetwarzania danych osobowych pracowników w świetle uzasadnionych interesów pracodawcy doznaje więc wielu ograniczeń – choćby takich, że pracownik winien mieć świadomość, jakie jego dane osobowe są przetwarzane i do jakich celów.

Zgoda... czyli kolos na glinianych nogach

Powszechna dotąd i asekuracyjna praktyka pracodawców uzyskiwania zgód od pracowników na wszelkie możliwe operacje przetwarzania danych osobowych, w możliwie szerokim zakresie (ponad standard wyznaczony w art. 22^1 Kodeksu pracy) na gruncie RODO osiągnie swój kres. Zgoda na przetwarzanie danych osobowych musi być wyraźna, świadoma, konkretna oraz dobrowolna, co w stosunkach pracowniczych jest o tyle problematyczne, że pracownik – z uwagi na nierównowagę podmiotów – w celu utrzymania lub uzyskania pracy, nie jest w swej decyzji całkowicie pozbawiony wpływu rozmaitych czynników nacisku. Zgoda wyrażona w sposób niedobrowolny nie jest ważna, a pracodawcy pozostaje poszukiwanie innych przesłanek, na podstawie których, dane osobowe mogą być przetwarzane. Należy pamiętać, że zgoda wyrażona jest tylko wówczas dobrowolnie i świadomie, kiedy z perspektywy pracownika, po rozważeniu istoty, znaczenia i ryzyka innych proponowanych rozwiązań, prowadzi do osiągnięcia tego samego celu, niezależnie od tego, czy ją wyrazi, czy też nie.

Dla przykładu: pracodawca zamierza zastosować system dostępu do pomieszczeń za pomocą odcisku palca – zgoda na przetwarzanie danych biometrycznych będzie ważna i skuteczna, jeżeli pracownik decydując, czy wyrazi zgodę na przetwarzanie swoich danych biometrycznych, ma alternatywę w postaci możliwości logowania się do systemu za pomocą innego narzędzia (np. identyfikatora zawierającego pasek magnetyczny) i to, że gdy odmówi zgody na przetwarzanie danych biometrycznych, fakt ten nie spowoduje dla niego negatywnych konsekwencji.

Umowa i obowiązek prawny ciążący na administratorze (pracodawcy)

Skoro stosunki pracy opierają się na umowie o pracę zawartej między pracodawcą, a pracownikiem, w zakresie wypełniania obowiązków umownych, pracodawca legalizując przetwarzanie danych osobowych swoich pracowników, powołać się może na wypełnianie obowiązków wynikających z tej umowy, takich jak wypłacanie pracownikowi wynagrodzenia – wówczas podstawą prawną przetwarzania jest art. 6 ust. 1 lit b) RODO. Nie budzi również większych wątpliwości, iż prawo pracy nakłada na pracodawcę obowiązki prawne, które wymagają przetwarzania danych osobowych (np. do celów obliczenia wysokości podatku, obliczania wynagrodzeń, dokonywania potrąceń z wynagrodzenia, czy zgłoszenia do systemu ubezpieczeń społecznych) wówczas podstawą prawną przetwarzania danych osobowych będzie art. 6 ust. 1 lit c) RODO.

Uzasadniony interes administratora

Kolejną przesłankę przetwarzania danych osobowych pracowników na gruncie RODO stanowić może uzasadniony interes administratora, przy czym powołanie się na nią wymaga wykazania, iż jest to proporcjonalne i bezwzględnie konieczne ze względów prawnych, a wybrana metoda lub technologia gwarantuje równowagę z podstawowymi prawami i wolnościami pracowników. Rozwiązania techniczne służące do monitorowania obecności pracownika w miejscu pracy oraz śledzenia czasu pracy są już upowszechnione. Pracodawca może przykładowo przetwarzać dane osobowe pracowników w kontekście kontrolowania osób uprawnionych do wejścia na teren lokalu bankowego lub uzyskania dostępu do określonych pomieszczeń w takim lokalu. Uzasadnionym, zwłaszcza w odniesieniu do banku, interesem administratora będzie ochrona danych i mienia przed nieuprawnionym dostępem, zaginięciem bądź utratą dokumentów lub środków pieniężnych zgromadzonych przez klientów. Sprawia to, iż dopuszczalne jest zainstalowanie systemu kontroli dostępu do pomieszczeń, rejestracji wejść i wyjść pracowników do tego pomieszczenia, o ile nie będzie to naruszać prawa pracowników do prywatności i zostaną oni poinformowani o przetwarzaniu ich danych osobowych. Należy jednak zadbać, by zgromadzone w ten sposób dane nie zostały wykorzystane w innym, aniżeli opisany wyżej cel, a dostęp do gromadzonych danych miały wyłącznie osoby upoważnione przez administratora. Przetwarzanie danych osobowych w tym przypadku odbywa się na podstawie przesłanki niezbędności przetwarzania danych osobowych do celów wynikających z prawnie uzasadnionego interesu realizowanego przez administratora tj. art. 6 ust. 1 lit f) RODO. Wprawdzie polski ustawodawca projektując przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, dostosowujące krajowy porządek prawny do

Gwarancją poszanowania

godności pracowników jest fakt, iż na gruncie polskiej ustawy o ochronie danych osobowych – monitorowanie nie może dotyczyć pomieszczeń sanitarnych, szatni, stołówek oraz palarni lub pomieszczeń udostępnianych zakładowej organizacji związkowej, chyba, że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celu i nie naruszy to godności oraz innych dóbr osobistych pracownika,..

przepisów unijnych, wprowadził rozwiązania umożliwiające zapewnienie bezpieczeństwa pracowników lub ochrony mienia, kontroli produkcji, czy zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, poprzez usankcjonowanie wykorzystania środków technicznych umożliwiających rejestrację obrazu (monitoring), niemniej jednak rozwiązania te w aktualnym stanie prawnym nie uwzględniają przetwarzania danych biometrycznych. Przetwarzanie danych osobowych utrwalonych na tych nagraniach z monitoringu będzie możliwe wyłącznie w celach, dla których zostały zebrane, przy czym zarówno o celu przetwarzania, zakresie i sposobie zastosowania, pracodawca zobligowany będzie przesądzić w układzie zbiorowym pracy, regulaminie pracy lub obwieszczeniu (jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy), jak również poinformować każdego z pracowników, w sposób przyjęty zwyczajowo w danym zakładzie pracy, nie później niż 2 tygodnie przed uruchomieniem monitoringu.
Gwarancją poszanowania godności pracowników jest fakt, iż na gruncie polskiej ustawy o ochronie danych osobowych – monitorowanie nie może dotyczyć pomieszczeń sanitarnych, szatni, stołówek oraz palarni lub pomieszczeń udostępnianych zakładowej organizacji związkowej, chyba, że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celu i nie naruszy to godności oraz innych dóbr osobistych pracownika, a także zasady wolności i niezależności związków zawodowych, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób. Ponadto przetwarzanie danych osobowych jest ograniczone czasowo do 3 miesięcy od dnia nagrania, a jeżeli zgromadzone nagrania stanowić będą miały dowód w postępowaniu prowadzonym na podstawie prawa, termin przetwarzania ulega wydłużeniu do zakończenia postępowania. Innym, sprecyzowanym w polskich przepisach novum, jest możliwość stosowania przez pracodawcę kontroli służbowej poczty elektronicznej dla zapewnienia organizacji pracy, umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy. Oczywiście, należy mieć świadomość, iż taka inwigilacja poczty nie może naruszać dóbr osobistych pracownika.
Wspomniana wyżej ustawa jest na końcu ścieżki legislacyjnej i aktualnie czeka na podpis Prezydenta (ustawę przekazano Prezydentowi w dniu 11.05.2018 r.).

W mojej ocenie szkoda, iż ustawodawca, pomimo wcześniej zaprojektowanych zmian, zrezygnował z ustawowego uregulowania możliwości żądania od pracownika banku danych biometrycznych, w szczególności w postaci odcisków palców, głosu, obrazu rogówki i sieci żył palców, jeżeli podanie takich danych jest konieczne ze względu na kontrolę dostępu do informacji przetwarzanych przez bank, a także pomieszczeń.
Paradoksalnie – choć przetwarzanie danych biometrycznych, jako danych wrażliwych, należałoby poddać większym restrykcjom, ich przetwarzanie nie zostało wyłączone – dopuszczalne będzie na podstawie przesłanki zgody pracownika tj. art. 9 ust. 2 lit a) RODO, a tym samym zarówno cel, sposób, zakres przetwarzanych danych zostanie określony przez administratora, co stwarza mniejsze gwarancje i pewność w zakresie przetwarzania danych w zgodzie z przepisami RODO.

Podsumowanie

Przetwarzanie danych osobowych pracowników w związku z zatrudnieniem, stanowi istotny element wdrożenia przepisów RODO w sektorze banków spółdzielczych i wymaga wyważenia prawnie uzasadnionych interesów administratora, ale jednocześnie wprowadzenia adekwatnych i wnikliwych środków zapewniających osobie, której dane dotyczą, poszanowanie jej godności i praw. W wypadku stosowania przez bank systematycznego monitorowania zachowań pracowników w miejscu pracy należy o tym informować pracowników, w szczególności o celach tego monitorowania oraz okolicznościach, w których się ono odbywa, a także o działaniach, które pracownicy mogą podejmować, aby uniemożliwić gromadzenie ich danych w drodze monitorowania.

Przyjmujemy zapisy na szkolenia realizowane przez BODiE w najbliższym czasie:					
Data	Temat szkolenia	Miejsce	Koordynator	Cena	
				12 os. i pow.	poniżej 12 os.
06.08.2018	**Hipoteka i weksel oraz pozostałe formy zabezpieczeń zapewniających pełną zwrotność zadłużenia kredytowego z przedmiotu zabezpieczenia**	Poznań	Oddział Poznań	490,00 zł	550,00 zł
06.08.2018	**Zmiany w VAT w 2018 r., z uwzględnieniem Split Payment**	Warszawa	Oddział Warszawa	490,00 zł	550,00 zł
06-07.08.2018	**Hipoteka i analiza jakości zabezpieczenia ustanawianego na nieruchomościach**	Tczew	Oddział Bydgoszcz	690,00 zł	750,00 zł
07.08.2018	**Hipoteka i weksel oraz pozostałe formy zabezpieczeń zapewniających pełną zwrotność zadłużenia kredytowego z przedmiotu zabezpieczenia**	Tczew	Oddział Bydgoszcz	490,00 zł	550,00 zł
08.08.2018	**Realizacja umowy o prowadzenie mieszkaniowego rachunku powierniczego**	Poznań	Oddział Poznań	390,00 zł	420,00 zł
10.08.2018	**Wycena nieruchomości komercyjnych w podejściu dochodowym – podstawy teoretyczne, analiza przychodów i kosztów funkcjonowania nieruchomości oraz weryfikacja parametrów wykorzystywanych w procesie wyceny**	Poznań	Oddział Poznań	430,00 zł	500,00 zł
10.08.2018	**Zarządzanie ryzykiem i ciągłością działania jako element Ładu Korporacyjnego**	Warszawa	Oddział Warszawa	400,00 zł	450,00 zł

Zadzwoń lub napisz:

Biuro Szkoleń i Rozwoju

Poznań
61-725
ul. Mielżyńskiego 20
T.: +48 61 42 37 201/202
F.: +48 61 42 37 109
E.: poznan@bodie.pl

Bydgoszcz
85-950
ul. Chodkiewicza 89–91
T.: +48 52 32 35 265/266
F.: +48 52 32 89 252
E.: bydgoszcz@bodie.pl

Warszawa
01-258
ul. Wolska 191 (Hotel Colibra)
T.: +48 22 20 83 882
F.: +48 22 83 69 962
E.: warszawa@bodie.pl