ALERT BEZPIECZNA FIRMA

BDO

Nr 4/2021

Szanowni Państwo,

Oddajemy dziś w Państwa ręce kolejne wydanie naszego alertu „Bezpieczna Firma". Mamy nadzieję, że kolejna porcja informacji na temat planowanych zmian w przepisach o przeciwdziałaniu praniu pieniędzy i zwalczaniu terroryzmu (AML) oraz informacje dotyczące RODO i cyberbezpieczeństwa okażą się dla Państwa przydatne i ciekawe. Państwa uwagę chcielibyśmy zwrócić na kolejne już zmiany dotyczące ustawy o przeciwdziałaniu praniu pieniędzy i zwalczaniu terroryzmu, wynikające z uchwalonej niedawno przez Sejm nowelizacji. Szczególnej uwadze chcielibyśmy polecić tekst dotyczący zmian odnoszących się do obowiązku aktualizacji danych zgłaszanych do Centralnego Rejestru Beneficjentów Rzeczywistych (CRBR). Wprowadzono nie tylko obowiązek weryfikowania zgłaszanych danych, ale także wysokie kary za brak aktualizacji danych już zgłoszonych do CRBR. Pozwolę sobie przypomnieć, że wynikające z nowelizacji zmiany regularnie opisywaliśmy w ostatnich miesiącach na lamach naszego alertu. Uwagę warto także zwrócić na pozostałe teksty, dotyczące zabezpieczenia danych przechowywanych na kontach w mediach społecznościowych oraz prób włamywania się do systemów firmowych za pomocą specjalnie spreparowanego maila informującego o „przepełnieniu" skrzynki mailowej. Z punktu widzenia bezpieczeństwa informatycznego, są to dość istotne kwestie. Jak zwykle życzymy przyjemnej lektury, a w przypadku, gdyby były Państwu potrzebne dodatkowe, bardziej szczegółowe informacje, zachęcamy do bezpośredniego kontaktu z naszą firmą i ekspertami.

DR ANDRÉ HELIN, Prezes BDO

Zmiany w przepisach o przeciwdziałaniu praniu pieniędzy z podpisem prezydenta

Nowelizacja ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw została już uchwalona. Nowe przepisy adresowane są do instytucji zobowiązanych, na które nakładają wiele nowych obowiązków.

Na początku kwietnia prezydent podpisał nowelizację ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw.

W wyniku nowelizacji na tzw. podmioty zobowiązane nałożono wiele nowych obowiązków, które obecnie powinny być pilnie uwzględnione w procedurach adresatów nowych przepisów.

Nowe przepisy: uszczegóławiają definicje m.in. beneficjenta rzeczywistego, państwa członkowskiego oraz grupy; poszerzają zakres statystyk gromadzonych przez Generalnego Inspektora Informacji Finansowej; określają zasady przechowywania przez instytucje obowiązane dokumentów i informacji uzyskanych w wyniku stosowania środków bezpieczeństwa finansowego, jak również zasady działań podejmowanych przez nie w zakresie relacji związanych z państwami trzecimi wysokiego ryzyka; wprowadzają mechanizmy weryfikacji danych zawartych w Centralnym Rejestrze Beneficjentów Rzeczywistych oraz obowiązek rejestrowania podmiotów świadczących usługi wymiany walut pomiędzy walutami wirtualnymi oraz dostawców kont waluty wirtualnej; wprowadzają obowiązek publikacji i aktualizacji wykazu stanowisk i funkcji publicznych, które zgodnie z prawem krajowym kwalifikują się jako eksponowane stanowiska polityczne.

Wśród nowych instytucji obowiązanych znajdą się, poza doradcami podatkowymi, którzy już dziś podlegają przepisom, także podmioty świadczące usługi polegające na sporządzaniu deklaracji, prowadzeniu ksiąg podatkowych, udzielaniu porad, opinii lub wyjaśnień z zakresu przepisów prawa podatkowego lub celnego. Przepisy ustawy będą musiały stosować także ci przedsiębiorcy, którzy prowadzą działalność w obrocie dziełami sztuki, przedmiotami kolekcjonerskimi lub antykami, w tym, gdy działalność ta prowadzone jest w galeriach sztuki lub w domach aukcyjnych (gdy wartość transakcji albo wielu powiązanych transakcji) wyniesie 10 tys. euro). Taki sam obowiązek dotyczył będzie podmiotów prowadzących działalność polegającą na przechowywaniu dzieł sztuki, przedmiotów kolekcjonerskich oraz antyków.

Nowelizacja zobowiązuje także zajmujące się obrotem walutami wirtualnymi uzyskania wpisu do nowego rejestru prowadzonego przez ministra finansów (nowelizacja wprowadza obowiązek rejestracji obrotu walutami wirtualnymi przy transakcjach powyżej 1 tys. euro przy transakcjach powyżej 1 tys. euro).

Nowelizacja przewiduje też nowe kary. Podmiot prowadzący działalność na rzecz spółek lub trustów, który będzie wykonywał działalność bez uzyskania wpisu do rejestru działalności na rzecz spółek lub trustów, będzie mógł być ukarany karą pieniężną do 100 tys. zł. Taka sama kara będzie groziła podmiotom prowadzący działalność w zakresie walut wirtualnych, jeśli nie uzyskają wpisu do rejestru działalności w zakresie walut wirtualnych.

W momencie kończenia prac nad naszym alertem nowelizacja nie została jeszcze opublikowana w Dzienniku Ustaw.

Będzie milion złotych kary za błąd w zgłoszeniu do CRBR

Ministerstwo Finansów sprawdzi nie tylko, czy spółki zobowiązane do złożenia danych do CRBR faktycznie wywiązały się z zadania, ale także, czy zrobiły to rzetelnie. Wkrótce za nierzetelne podanie danych będzie grozić kara do miliona złotych.

Uchwalona przez Sejm 30 marca 2021 r. nowelizacja ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw wprowadza trzy ważne zmiany w zakresie zgłoszeń do Centralnego rejestru Beneficjentów rzeczywistych (CRBR).

Po pierwsze nowelizacja nakłada na instytucje obowiązane nowy obowiązek dotyczący weryfikacji poprawności danych zgłoszonych do CRBR. Na podstawie tych przepisów wewnętrzna procedura instytucji zobowiązanych w zakresie przeciwdziałania praniu pieniędzy ma w szczególności określać zasady odnotowywania rozbieżności pomiędzy informacjami zgromadzonymi w CRBR, a informacjami o beneficjentach rzeczywistych klienta ustalonymi w związku ze stosowaniem ustawy.

Po drugie, instytucje zobowiązane będą musiały odnotowywać rozbieżności pomiędzy informacjami zgromadzonymi w rejestrze, a ustalonymi przez nią informacjami.

Oznacza to, że instytucje zobowiązane (w tym mi.in banki, ubezpieczyciele, pośrednicy nieruchomości, brokerzy, kantory, notariusze, biegli rewidenci, doradcy podatkowi) będą musiały weryfikować rzetelność przekazanych przez klienta informacji o beneficjentach rzeczywistych w zestawieniu z rejestrem, a w przypadku zidentyfikowania rozbieżności zgłosić je fiskusowi.

Trzecia zmiana dotyczy przewidzianych ustawą kar. Obecnie, zgodnie z art. 153 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw, do miliona złotych kary grozi jedynie za niedopełnienie obowiązku zgłoszenia beneficjentów rzeczywistych do CRBR (Centralny Rejestr Beneficjentów Rzeczywistych). Po nowelizacji nie tylko spółki, które nie dokonały zgłoszenia, ale również te, które nie zaktualizowały informacji lub podały dane niezgodne ze stanem faktycznym, będą podlegały karze pieniężnej do wysokości 1 mln zł. W przypadku osób zajmujących stanowiska kierownicze kara będzie wynosiła do 50 tys. zł. Warto pamiętać, że już dziś obowiązujące przepisy nakładają obowiązek aktualizacji zgłoszenia do CRBR po każdej zmianie, w terminie 7 dni.

UODO radzi, jak chronić dane dostępne na kontach w mediach społecznościowych

Po ujawnieniu danych, które wykradzione zostały z kont użytkowników w mediach społecznościowych Urząd Ochrony Danych Osobowych opublikował wskazówki dotyczące zarówno ochrony danych w takich serwisach, jak i zasad postępowania w przypadku podejrzenia włamania na konto.

Informacje, które pojawiły się w ostatnim czasie w związku z wyciekiem danych osobowych z kont użytkowników Facebooka, skłoniły Urząd Ochrony Danych Osobowych do opublikowania wskazówek dotyczących zabezpieczenia bezpieczeństwa danych w mediach społecznościowych. Zdaniem urzędu ten aspekt korzystania z sieci musi być traktowany przez wszystkich użytkowników priorytetowo, z uwagi na gigantyczne ilości danych przechowywane na kontach w takich serwisach.

UODO przypomniał zasady, którymi należy się kierować, aby zminimalizować ryzyka związane z korzystaniem z mediów społecznościowych. W tym obszarze zaleca: stosować silne hasło — można w tym celu posłużyć się generatorem haseł; stosować dwuetapowe logowanie — najpierw podajemy login i hasło, a później potwierdzamy logowanie zewnętrznym tokenem, ponieważ zastosowanie takiego klucza sprzętowego skutecznie zabezpieczy przed atakami hakerskimi (phishingiem, przechwytywaniem sesji czy wyłudzeniem danych). Ponadto token nie zadziała podczas logowania na fałszywej stronie; nie logować się na nieznanych urządzeniach; stosować różne hasła do różnych portali i systemów, w czym może pomóc nam manager haseł; nie korzystać z niezaufanego połączenia internetowego (publiczne hot spoty); ograniczyć uprawnienia aplikacji do logowania za pomocą konta w portalu społecznościowego.

W przypadku podejrzenia, że doszło do wycieku danych, zgodnie z zaleceniami UODO: bezwzględnie należy, najszybciej jak to możliwe, zmienić hasło przy zachowaniu zasad tworzenia złożonego hasła; należy zachować szczególną ostrożność przed atakami phishingowy, ponieważ jak podkreśla UODO, ataki te mogą się nasilić po wycieku danych kontaktowych (e-mail); pod żadnym pozorem nie należy używać odnośników znajdujących się w otrzymanej poczcie, w szczególności w korespondencji niezamówionej lub pochodzącej od nieznanych osób, instytucji i firm; należy zachować ostrożność przed atakami socjotechnicznymi, przeprowadzanymi przy użyciu telefonu. Jak wyjaśnia UODO potencjalny hacker może wykorzystać przechwycone z portalu społecznościowego dane, podczas rozmowy telefonicznej z ofiarą ataku uwierzytelnić się a następnie zdobyć bezpośrednio dalsze informacje, w tym dostęp do systemów lub urządzeń użytkownika.

Warto podkreślić, że zasady te dotyczą nie tylko kont prywatnych, ale także kont firmowych w mediach społecznościowych. Jest to szczególnie ważne w przypadku małych i średnich firm, które działają często bez wyspecjalizowanych działów IT.

Wzrasta liczba ataków szyfrujących firmowe dane w celu wyłudzenia okupu

Nadal istnieje wysoki stopień zagrożenia atakami na firmowe sieci komputerowe polegającymi na bezprawnym szyfrowaniu danych, które przywracane są w zamian za okup. Aby uzyskać dostęp do systemów firmy, wykorzystywane są m.in. fałszywe maile o przepełnieniu skrzynki pocztowej.

Trwający stan epidemii COVID-19 i upowszechnienie się z związku z tym pracy zdalnej pracowników z wykorzystaniem firmowych komputerów spowodował znaczący wzrost ataków ransomware. Ten rodzaj ataku polega na blokowaniu dostępu do danych zgromadzonych na komputerze lub na firmowych serwerach. Po uzyskaniu dostępu do danych przestępcy szyfrują je żądając za ich odszyfrowanie wysokiego okupu, najczęściej w wirtualnej walucie. Co istotne do przeprowadzenia ataku wystarcza przestępcom już uzyskanie dostępu do jednego komputera w sieci.

Do zainfekowania komputera dochodzi najczęściej poprzez kliknięcie w link (także w postaci zdjęcia lub reklamy) zamieszczony w wiadomości przesłanej na adres poczty elektronicznej. Wiadomości takie często spreparowane są w ten sposób, że podszywają się pod kontrahenta i zawierają np. fakturę lub wezwanie do zapłaty, co ma sprowokować do kliknięcia w załącznik i w konsekwencji zainfekowania komputera oprogramowaniem szyfrującym. Do zainfekowania dochodzi także z wykorzystaniem tzw. malwertsingu, czyli umieszczenia złośliwego oprogramowania w reklamie.

Poważnym zagrożeniem stają się także maile zawierające pozornie komunikaty związane z bieżącą pracą firmy, np. coraz częściej do ataków dochodzi poprzez odpowiednio spreparowany mail informujący pracownika o konieczności odblokowania przepełnionego konta poczty elektronicznej. Kliknięcie w taki mail powoduje przejęcie dostępu do komputera ofiary przez hakerów i umożliwia im dostanie się do wewnętrznych systemów firmy.

Dlatego kwestiom bezpieczeństwa danych należy poświęcać obecnie znacznie więcej uwagi niż dotychczas. Wymaga to nie tylko opracowania szczegółowych zasad bezpieczeństwa, których pracownicy powinni przestrzegać pracując na firmowym sprzęcie z domu, ale także konsekwentnego i częstego kontrolowania czy zasady te są rzeczywiście przestrzegane. Dobrym zabezpieczeniem przed utratę gromadzonych często latami danych jest także zapewnienie odpowiednich, często wykonywanych kopii bezpieczeństwa. I to nie tylko danych zgromadzonych na firmowych serwerach, ale także lokalnych dyskach wykorzystywanych przez pracowników komputerów. Największe bezpieczeństwo zapewnia w tym przypadku utrzymywanie takich kopii poza strukturą firmowej sieci.

W SKRÓCIE

Europejski Inspektor Ochrony Danych przeciwny rozpoznawaniu twarzy

W Europie powinien zostać wprowadzony zakaz wykorzystywania technologii rozpoznawania twarzy, ponieważ prowadzi ona do „głębokiej i niedemokratycznej ingerencję" w życie prywatne obywateli – wskazał Europejski Inspektor Ochrony Danych (EIOD). Taki komentarz pojawił się dwa dni po ogłoszeniu przez Komisję Europejską propozycji nowych przepisów i standardów dotyczących innowacyjnych rozwiązań dotyczących sztucznej inteligencji. Obecnie EIOD skoncentruje się na ustaleniu precyzyjnych granic dla tych narzędzi i systemów, które mogą stanowić zagrożenie dla praw podstawowych w zakresie ochrony danych i prywatności.

Zielone certyfikaty związane z COVID-19 muszą zapewnić ochronę danych osobowych

We wspólnej opinii Europejska Rady Ochrony Danych (EROD) i Europejski Inspektor Ochrony Danych (EIOD) wezwały kraje unijne do zapewnienia, że zielone zaświadczenie cyfrowe jest w pełni zgodne z unijnymi przepisami o ochronie danych osobowych. Komisarze ochrony danych z całej UE i Europejskiego Obszaru Gospodarczego podkreślają potrzebę zmniejszenia zagrożeń dla podstawowych praw obywateli i mieszkańców UE, które mogą wynikać z wydania zielonego zaświadczenia cyfrowego, w tym jego ewentualnych niezamierzonych wtórnych zastosowań. Celem zielonego zaświadczenia cyfrowego jest ułatwienie korzystania z prawa do swobodnego przemieszczania się w Unii Europejskiej w czasie pandemii COVID-19 poprzez ustanowienie wspólnych ram dla wydawania, weryfikowania i uznawania zaświadczeń o szczepieniu, wyniku testu i o powrocie do zdrowia.

EROD ocenił stopień ochrony danych osobowych w Zjednoczonym Królestwie

W połowie kwietnia Europejska Rada Ochrony Danych (EROD) przyjęła dwie opinie w sprawie projektów decyzji stwier-

dzających odpowiedni stopień ochrony w Zjednoczonym Królestwie po Brexicie. EROD zwróciła uwagę, że istnieją kluczowe obszary zbieżności między ramami ochrony danych UE i Zjednoczonego Królestwa w zakresie określonych podstawowych przepisów, dotyczących m.in.: podstawy dla zgodnego z prawem i rzetelnego przetwarzania danych osobowych dla prawnie uzasadnionych celów, ograniczenia celu, jakości i proporcjonalności danych, zatrzymywania danych, bezpieczeństwa i poufności czy przejrzystości. Jednak w swoich opiniach Rada wskazała także pewne kwestie, które Komisja Europejska powinna poddać dalszej ocenie lub ściśle monitorować.

Spotkania na Teams po wprowadzeniu specjalnego 13-cefrowego identyfikatora

Do końca maja Microsoft ma wprowadzić nowy sposób dołączania do spotkań w aplikacji Teams. Firma wprowadzi 13-cyfrowy kod, dzięki któremu nie będzie konieczności użycia linku. Wszystkie spotkania będą miały identyfikator spotkania, który jest automatycznie przypisywany do użytkownika Microsoft Teams i dodawany do zaproszenia pod linkiem do spotkania. Uczestnicy będą mogli dołączyć do spotkania, wprowadzając wygenerowany identyfikator. Dla wszystkich uczestników spotkania wstępne dołączenie, lobby i zabezpieczenia pozostaną takie same.

Luki w Microsoft Exchange groźne dla wielu firm

Ogłoszone niedawno luki w Microsoft Exchange Server mają realny wpływ na bezpieczeństwo firm na całym świecie. O gigantycznej skali szkód poinformował m.in. KrebsOnSecurity. Exchange Server, będący najpopularniejszym serwerem pocztowym na świecie został zhakowany na początku tego roku, a Microsoft załatał luki w zabezpieczeniach dopiero w marcu. To oznacza, że przestępcy mieli niemal dwa miesiące na przeprowadzenie ataków. Eksperci Check Point zwracają uwagę, że każda organizacja, która nie wdrożyła poprawek lub nie posiada zaawansowanych systemów ochronnych, może być cały czas poważnie narażona na ataki.

**BDO spółka z ograniczoną odpowiedzialnością sp.k., ul. Postępu 12, 02-676 Warszawa;
tel.: +48 22 543 16 00, fax: +48 22 543 16 01, e-mail: office@bdo.pl**