ALERT BEZPIECZNA FIRMA

BDO

Nr 9-10/2022

Szanowni Państwo,

Szanowni Państwo
Przedstawimy Państwu kolejne wydanie naszego alertu „Bezpieczna Firma", który poświęcony jest omówieniu najbardziej aktualnych i ciekawych naszym zdaniem informacji o przeciwdziałaniu praniu pieniędzy i zwalczaniu terroryzmu (AML) oraz z zakresu cyberbezpieczeństwa i ochrony danych osobowych.
Tym razem przede wszystkie chcielibyśmy zwrócić uwagę na planowane zmiany dotyczące funkcjonowania Centralnego Rejestru Beneficjentów Rzeczywistych (CRBR) oraz planowane przez unijne rozporządzenie, które ma określić zasady wprowadzania do obrotu produktów z elementami cyfrowymi w celu zapewnienia cyberbezpieczeństwa takich produktów. Istotne w tym miejscu jest to, że akt ten ma mieć charakter rozporządzenia, a zatem nie będzie wymagał implementacji, tylko będzie miał zastosowanie bezpośrednio w krajach unijnych, bez konieczności uchwalania przepisów krajowych.
Poza tym jak zawsze, przedstawiamy najciekawsze krótsze informacje dotyczące bezpieczeństwa.
Mamy nadzieję, że kolejna porcja informacji zawarta w naszym alercie okaże się dla Państwa pożyteczna, ułatwiając sprawne poruszanie się po przepisach oraz trendach związanych z cyberbezpieczeństwem, ochroną danych osobowych i AML.
W przypadku, gdyby były Państwu potrzebne dodatkowe, bardziej szczegółowe informacje, zachęcamy do bezpośredniego kontaktu z naszą firmą i ekspertami.

DR ANDRÉ HELIN, Prezes BDO

Podmiot przetwarzający musi dawać gwarancje ochrony osób, których dane dotyczą

Administrator, decydując się na powierzenie przetwarzania danych osobowych innemu podmiotowi, powinien sprawdzić, czy zapewnia on wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych oraz czy przetwarzanie będzie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

Brak weryfikacji podmiotu przetwarzającego oraz jego gwarancji dla przetwarzania zgodnie z przepisami o ochronie danych osobowych może wiązać się z konsekwencjami dla osób fizycznych, których dane osobowe zostały powierzone podmiotowi przetwarzającemu, np. w postaci utraty danych osobowych. Zatem decyzja, komu administrator ma powierzyć przetwarzanie danych osobowych nie może być podejmowana bezpodstawnie. Dopiero po zbadaniu kompetencji i adekwatności wybranego podmiotu przetwarzającego, administrator może przystąpić do zawarcia stosownej umowy powierzenia.

Powierzenie przetwarzania danych osobowych bez zawartej na piśmie umowy powierzenia oraz bez przeprowadzenia weryfikacji, czy podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych, może skutkować nałożeniem przez Urząd Ochrony Danych Osobowych (UODO) administracyjnej kary pieniężnej (czego doświadczył ostatnio Sułkowicki Ośrodek Kultury).

Administrator musi przy tym posiadać dokumenty potwierdzające weryfikację warunków współpracy z podmiotem przetwarzającym.

Na podstawie art. 28 RODO administrator, chcąc przetwarzać dane przy pomocy innego podmiotu, korzysta wyłącznie z usług takich podmiotów, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych. Samo zaś przetwarzanie przez podmiot przetwarzający odbywa się na podstawie pisemnej umowy między administratorem i podmiotem przetwarzającym. Umowa taka określa m.in. przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

Nowe unijne rozporządzenie ma zaostrzyć wymogi cyberbezpieczeństwa

Unia Europejska opublikowała 15 września 2022 r. projekt założeń aktu prawnego, którego głównym celem jest zwiększenie poziomu cyberbezpieczeństwa w państwach członkowskich. Z dokumentu wynika, że producenci, importerzy i dystrybutorzy produktów cyfrowych na rynek europejski będą musieli spełnić wiele zasad, by ich urządzenia mogły być legalnie sprzedawane na terenie państw członkowskich.

Jak czytamy w unijnym dokumencie proponowane rozporządzenie zharmonizowałoby i usprawniło wspólnotowe regulacje poprzez wprowadzenie wymogów w zakresie bezpieczeństwa cybernetycznego dla produktów z elementami cyfrowymi oraz uniknięcie nakładania się wymogów wynikających z różnych aktów prawnych. Stworzyłoby to większą pewność prawną dla operatorów i użytkowników w całej Unii, a także zapewniło lepszą harmonizację jednolitego rynku europejskiego, tworząc bardziej opłacalne warunki dla operatorów zamierzających wejść na rynek UE.

Rozporządzenie miałoby określić: zasady wprowadzania do obrotu produktów z elementami cyfrowymi w celu zapewnienia cyberbezpieczeństwa takich produktów; zasadnicze wymogi dotyczące projektowania, opracowywania i produkcji produktów z elementami cyfrowymi oraz obowiązki podmiotów gospodarczych w odniesieniu do tych produktów w zakresie cyberbezpieczeństwa; zasadnicze wymogi dotyczące procesów obsługi podatności wprowadzonych przez producentów w celu zapewnienia cyberbezpieczeństwa produktów z elementami cyfrowymi w całym cyklu życia oraz obowiązki podmiotów gospodarczych w odniesieniu do tych procesów; przepisy dotyczące nadzoru rynku i egzekwowania wyżej wymienionych przepisów i wymogów.

Zasadnicze wymogi i obowiązki w zakresie bezpieczeństwa cybernetycznego mają przewidywać, że wszystkie produkty z elementami cyfrowymi są udostępniane na rynku tylko wtedy, gdy – w przypadku rzetelnej dostawy, właściwej instalacji, konserwacji i użytkowania zgodnie z przeznaczeniem lub w warunkach, które można racjonalnie przewidzieć – spełniają zasadnicze wymogi w zakresie bezpieczeństwa cybernetycznego określone w nowym rozporządzeniu.

Zasadnicze wymogi i obowiązki nakładałyby na producentów obowiązek uwzględnienia bezpieczeństwa cybernetycznego przy projektowaniu, opracowywaniu i produkcji produktów zawierających elementy cyfrowe, zachowania należytej staranności w odniesieniu do aspektów bezpieczeństwa przy projektowaniu i opracowywaniu produktów, zachowania przejrzystości w odniesieniu do aspektów bezpieczeństwa cybernetycznego, o których należy poinformować klientów, zapewnienia wsparcia w zakresie bezpieczeństwa (aktualizacji) w proporcjonalny sposób oraz przestrzegania wymogów w zakresie obsługi podatności.

W odniesieniu do wprowadzania do obrotu produktów z elementami cyfrowymi ustanowione zostałyby obowiązki dla podmiotów gospodarczych, począwszy od producentów, a skończywszy na dystrybutorach i importerach, odpowiednie do ich roli i obowiązków w łańcuchu dostaw.

Będą zmiany w funkcjonowaniu Centralnego Rejestru Beneficjentów Rzeczywistych

Rząd planuje zmiany w zasadach funkcjonowania Centralnego Rejestru Beneficjentów Rzeczywistych (CRBR). Możliwe ma stać się m.in. wyszukiwanie podmiotów w rejestrze po numerze KRS oraz nazwie podmiotu, a także po numerze, pod którym zarejestrowany jest trust.

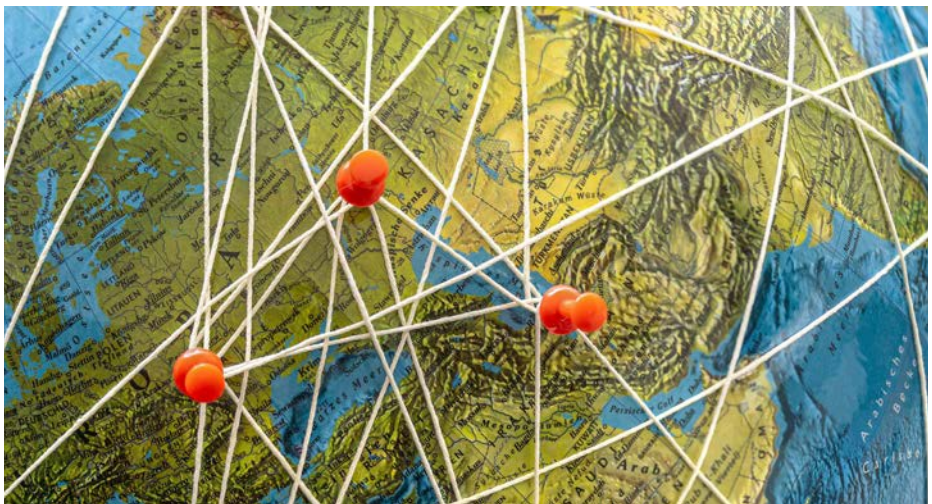
Ministerstwo Finansów przygotowało projekt rozporządzenia zmieniającego rozporządzenie w sprawie wniosków o udostępnienie informacji o beneficjentach rzeczywistych oraz udostępniania tych informacji (druk 554).

Z nowych przepisów wynika, że obok dotychczas stosowanych kryteriów wyszukiwania (numeru PESEL albo numeru NIP albo imienia, nazwiska i daty urodzenia beneficjenta rzeczywistego w przypadku beneficjentów rzeczywistych zgłoszonych do Centralnego Rejestru Beneficjentów Rzeczywistych jako osoby nieposiadające numeru PESEL) możliwe stanie się również wyszukiwanie podmiotów według numeru KRS, a także nazwy (firmy). Od strony technicznej przyjęte rozwiązanie umożliwi użycie części nazwy (firmy) podmiotu jako kryterium wyszukiwania (poprzez podanie co najmniej minimalnej liczby znaków), a w przypadku wyszukania więcej niż jednego wyniku, jako wynik wyszukiwania podana zostanie informacja o pierwszych wynikach (maksymalna liczba znaków) z koniecznością doprecyzowania nazwy podmiotu. Przy czym minimalna i maksymalna liczba znaków będzie możliwa do ustalenia dopiero w trakcie modernizacji systemu.

Dodatkowo, w przypadku podmiotów regulowanych przepisami prawa obcego trustów i podobnych trustom porozumień prawnych, którym nie nadano numeru identyfikacji podatkowej w Polsce, a które dokonały zgłoszenia informacji do CRBR, projekt umożliwia wyszukiwanie w CRBR według mającego techniczny charakter numeru, pod którym trust został zarejestrowany w trakcie procesu zgłaszania informacji do CRBR.

To jednak nie jedyna zmiana w przepisach. Zmiany w rozporządzeniu mają bowiem uwzględnić także to co wynika ze znowelizowanej ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Zmiana ta polegała na rozszerzeniu katalogu podmiotów, które są zobowiązane do zgłaszania informacji o beneficjentach rzeczywistych o trusty, których powiernicy lub osoby zajmujące stanowiska równoważne mają miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej oraz o trusty, których powiernicy lub osoby zajmujące równoważne stanowiska w imieniu lub na rzecz trustu nawiązują stosunki gospodarcze lub nabywają nieruchomość na terytorium Rzeczypospolitej Polskiej. Obowiązkiem tym objęte zostały: spółki partnerskie, europejskie zgrupowania interesów gospodarczych, spółki europejskie, spółdzielnie, spółdzielnie europejskie, stowarzyszenia podlegające wpisowi do Krajowego Rejestru Sądowego oraz fundacje. Tymczasem rozporządzenie odwołuje się obecnie jedynie do spółek.

Nowe rozporządzenie ma wejść w życie 1 stycznia 2023 roku. Obecnie projekt znajduje się na etapie konsultacji.



W SKRÓCIE

Polacy nadal nie wiedzą gdzie zwracać się w sprawie ochrony danych osobowych

Aż 70 proc. Polaków deklaruje, że nie wie, kto powinien zająć się negatywnymi konsekwencjami wycieku danych osobowych, a 1/3 z tych, którzy mają świadomość na ten temat uważa, że musi to zrobić sam poszkodowany. Pozostali wskazują m.in. na policję, UODO oraz inspektorów ochrony danych oraz oczekują od nich przede wszystkim szczegółowej informacji na temat zdarzenia oraz rekomendacji dalszych działań. Tak wynika z badania przeprowadzonego przez serwis ChronPESEL.pl i Krajowy Rejestr Długów pod patronatem UODO.

EROD przyjął oświadczenie w sprawie kodeksu współpracy policyjnej

EROD (Europejska Rada Ochrony Danych) podczas 69. posiedzenia plenarnego przyjęła oświadczenie w sprawie wniosku Komisji Europejskiej dotyczącego unijnego kodeksu współpracy policyjnej oraz wybrała temat drugiego skoordynowanego działania w zakresie egzekwowania prawa, które będzie dotyczyło wyznaczenia i pozycji inspektora ochrony danych. EROD rekomenduje m.in. określenie rodzajów i wagi przestępstw, które mogłyby uzasadniać automatyczne wyszukiwanie w bazach danych innych państw członkowskich oraz wyraźne rozróżnienie między danymi osobowymi różnych kategorii osób, których dane dotyczą, takich jak skazani przestępcy, podejrzani, ofiary lub świadkowie.

Pracownicy zdalni są łatwiejszym celem cyberataków

Pracownicy zdalni, choć często podkreślają, że dzięki temu są bardziej produktywni i łatwiej jest się im skupić w domowej ciszy, są także łatwiejszym celem cyberataków – twierdzi serwis Cyberdefence24.pl. W sumie w Polsce w 2021 roku zanotowano niemal 30 tys. naruszeń bezpieczeństwa (dane CERT Polska), co stanowiło o 182 proc. przypadków więcej w porównaniu do 2020 roku. Nie należy się zatem spodziewać, że 2022 rok będzie pod tym względem lepszy, ze względu na wojnę w Ukrainie i konieczność stałej ochrony w cyberprzestrzeni.

Powstaje sektorowe centrum przeciwdziałania praniu pieniędzy

KIR, ZBP i banki tworzą sektorowe centrum AML. Będą wymienić się infor-

macjami o podejrzanych transakcjach. Sektorowe Centrum Usług AML jest pomyślane jako strukturalna i organizacyjna pomoc dla banków w wypełnianiu licznych obowiązków wynikających z przepisów o praniu pieniędzy. Jak podkreślają pomysłodawcy centrum, z perspektywy pojedynczego banku dostrzeżenie wielu okoliczności wykraczających poza dany bank nie jest możliwe. Dopiero po otrzymaniu informacji z większej liczby banków jest możliwe zidentyfikowanie schematów pewnych zachowań i zależności pomiędzy transakcjami, które świadczą, że mają one charakter przestępczy.

Do blisko 334 mld dolarów wzrosną nakłady na cyberbezpieczeństwo do 2026 roku

Globalne przychody z cyberbezpieczeństwa zwiększą się z 220 mld dol. w 2021 r. do 334 mld USD w 2026 r. – prognozuje GlobalData. Coraz większym wydatkom będzie sprzyjał gwałtowny wzrost liczby i zaawansowania cyberataków, pojawienie się dużej liczby połączonych urządzeń i związanych z nimi zagrożeń oraz priorytetowe traktowanie ochrony cyfrowej w organizacjach, jak i przez konsumentów. Cyberbezpieczeństwo przedsiębiorstw będzie dominować pod względem zapotrzebowania na rynku (ponad 90 proc. udziału w przychodach w 2021 r.).

Revolut został zhakowany, ale dane o kartach i hasła bezpieczne

The Times poinformował że doszło do włamania do Revoluta. Atak dotknął 50144 osób z czego 20687 ofiar to Europejczycy a 379 to Litwini. Włamywacz pozyskał dostęp do: imion i nazwisk, adresów e-mail, adresów zamieszkania, informacji o transakcjach. Hasła oraz dane kart nie zostały skradzione.

Nowe sposoby ataku na niedoświadczone osoby korzystające z kryptowalut

Analityk z rynku cyberbezpieczeństwa – Serpent – opisał na Twitterze, w jaki sposób oszuści obecnie atakują niedoświadczonych użytkowników kryptowalut. Korzystają oni m.in. z fałszywych witryn internetowych, adresów URL, czy zhakowanych zweryfikowanych kont. Według eksperta przestępcy twierdzą, że są programistami blockchaina i wyszukują użytkowników, którzy padli ofiarą niedawnego włamania lub exploita na dużą skalę. Proszą ich o opłatę za wdrożenie smart kontraktu, który może pomóc odzyskać skradzione środki.

Belgia skarży IAB Europe do TSUE za naruszanie przepisów o RODO

Trybunał Sprawiedliwości UE zajmie się sprawą skarg na IAB Europe i jego system śledzącej reklamy, który może być niezgodny z RODO. Belgijski organ ochrony danych osobowych (APD) uznał na początku lutego br., że stworzony przez związek firm branży reklamowej IAB Europe system śledzącej reklamy, z którego korzysta 80 proc. stron internetowych, narusza podstawowe zasady RODO.

Większość firm nie jest w stanie na bieżąco wykrywać cyberzagrożeń

3 na 4 firmy nie są w stanie wykryć bieżących cyberzagrożeń – wynika z badania Dynatrace. Z raportu wynika, że wczesne identyfikowanie problemów, ustalanie priorytetów oraz zmniejszanie skutków potencjalnego ataku nie jest już dodatkową opcją, a koniecznością. Jednak z funkcji zarządzania podatnościami w czasie rzeczywistym korzysta mniej niż 40% przedsiębiorców, a jedynie 1/4 zespołów ds. bezpieczeństwa ma dostęp do dokładnych, stale aktualizowanych raportów.

Hakerzy zyskali dostęp do 140 tysięcy terminali płatniczych z powodu prostych błędów

Fintech Wiseasy został zaatakowany przez hakerów. W efekcie osoby niepowołane zyskały dostęp do 140 tys. terminali płatniczych. O sprawie informuje serwis techcrunch.com, który jednocześnie zwraca uwagę, że włamywacze wykorzystali prosty błąd: brak uwierzytelnienia dwuskładnikowego w systemie poszkodowanej firmy. Co gorsza, z opóźnieniem reagowała ona na ostrzeżenia specjalistów ds. cyberbezpieczeństwa, którzy już kilka tygodni temu informowali o wycieku danych.

BDO to międzynarodowa sieć niezależnych firm audytorsko-doradczych, których współpraca koordynowana jest z centralnego biura w Brukseli. Początki BDO sięgają 1963 roku. W Polsce BDO działa od 1991 roku. Mamy 5 biur, w: Warszawie, Krakowie, Poznaniu, Wrocławiu, Katowicach.

BDO od lat doceniane jest w prestiżowych Rankingach dotyczących działalności m.in. Działów: Audytu oraz Doradztwa Podatkowego. Ostatnie wyróżnienia dla firmy dotyczą Rankingów:

Firm i Doradców Podatkowych Dziennika Gazety Prawnej za 2021 rok:
- **I miejsce** Najlepsza Firma Doradztwa Podatkowego w kategorii firm średnich

Rzeczpospolitej i Parkietu za 2021 rok:
- **Najbardziej Aktywna Firma na Giełdzie** (III miejsce)
- **Najlepsza Firma Audytorska** (IV miejsce)
- **Najlepsza Firma badająca spółki giełdowe** (V miejsce)

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