
LEX ARTIST

RODO - aktualności

[22.07.2024]

UWAGA!

Tezy przedstawione w artykułach, zamieszczone w niniejszym materiale i niebędące wytycznymi organu nadzorczego albo orzeczeniami sądów lub organów administracji publicznej, stanowią wyłącznie opinię ich autorów i nie są oficjalnym stanowiskiem Lex Artist Sp. z o.o.

01 UODO: Nie każda przerwa w dostępie do danych stanowi naruszenie

02 WSA: Wiadomość o konsekwencjach nieterminowej płatności nie narusza RODO

03 PUODO: Polska powinna zmienić Prawo telekomunikacyjne

04 Ustawa o ochronie sygnalistów wchodzi w życie 25 września 2024 r. (z pewnymi wyjątkami)

05 Rewolucja na rynku. Wspólny certyfikowany podpis biometryczny od Asseco, Samsung i Xtension

01 UODO: Nie każda przerwa w dostępie do danych stanowi naruszenie

- W związku z ujawnioną globalną awarią usług chmurowych UODO przypomina, że nie każda przerwa w dostępie do danych osobowych stanowi naruszenie ochrony danych.
- Awarie powodują duże zamieszanie i kłopoty w wielu branżach, również tych strategicznych, jak transport czy ochrona zdrowia. Wicepremier, minister cyfryzacji Krzysztof Gawkowski poinformował, że zgłaszane są przypadki awarii związanych z przerwą w dostępie do usług chmurowych, lecz nie dotyczą one infrastruktury krytycznej.
- Przerwa w dostępie do usług chmurowych i wynikający z tego brak dostępu do danych, w pewnych sytuacjach może skutkować naruszeniem praw i wolności osób. Jednak nie każde tego typu naruszenie wymaga zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych.
- Administrator każdorazowo powinien przeprowadzić analizę ryzyka i w przypadku stwierdzenia wystąpienia takiego naruszenia skutkującego ryzykiem dla naruszenia praw lub wolności osób zgłosić taki incydent organowi nadzorczemu. Warto podkreślić, że ryzyko będzie występowało w sytuacji prawdopodobieństwa wpływu tej sytuacji na prawa lub wolności jednostki, np. bezpośrednie zagrożenie dla zdrowia czy życia.
- Awaria ta potwierdza, fakt wynikający ze standardów RODO, że inwentaryzowanie zasobów w organizacjach jest bardzo ważne. Istotna jest też konieczność oceny ryzyka w kontekście dostępu do danych i wpływu możliwej awarii na ochronę osób, których dane są przetwarzane.

Źródło: Aktualności - UODO

02 WSA: Wiadomość o konsekwencjach nieterminowej płatności nie narusza RODO

- Prezes Urzędu Ochrony Danych Osobowych udzielił spółce upomnienia za naruszenie polegające na przetwarzaniu, bez podstawy prawnej, danych osobowych klienta (imienia i nazwiska, adresu poczty elektronicznej oraz NIP) w celu przesyłania drogą elektroniczną informacji o nieistniejących zaległościach w płatnościach za karty. Spółka nie zgodziła się z wydaną decyzją, więc wniosła skargę.
- Sprawą zajął się WSA w Warszawie, który wskazał, że klient i spółka byli stronami umowy o wydanie i używanie kart. Nie było też sporne, że klient otrzymywał informacje dotyczące niezaksięgowania płatności pomimo ich regulowania za pomocą złożonego w banku polecenia zapłaty.
- Sąd nie zgodził się z organem i uznał, że przetwarzanie danych osobowych miało podstawę prawną, ponieważ służyło wykonaniu łączącej strony umowy. Zgodnie bowiem z art. 6 ust. 1 lit. b RODO przetwarzanie jest zgodne z prawem, gdy - i w takim zakresie, w jakim - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy.
- Sąd wskazał, że jednym z elementów łączącej strony umowy było zobowiązanie do terminowego regulowania należności. Natomiast działania podejmowane w celu wyegzekwowania zobowiązań umownych, niezależnie od ich racjonalności, mieszczą się w zakresie pojęcia wykonania umowy, o którym mowa w art. 6 ust. 1 lit. b RODO. WSA podkreślił, że przesyłanie klientowi korespondencji dotyczącej ewentualnie nieuregulowanych płatności miało bezpośredni związek z wykonywaniem umowy.
- WSA stwierdził, że w gestii Prezesa UODO nie leży wypowiadanie się w kwestii istnienia albo nieistnienia należności wynikających z umowy cywilnoprawnej. Tymczasem w uzasadnieniu zaskarżonej decyzji organ przesądził, że klient nie zalegał z opłatami za korzystanie z usług spółki. WSA uchylił zaskarżoną decyzję.

Źródło: Informowanie o konsekwencjach nieterminowej płatności nie narusza RODO (prawo.pl)

03 PUODO: Polska powinna zmienić Prawo telekomunikacyjne

- Polska powinna zmienić Prawo telekomunikacyjne w zakresie zasad dostępu „uprawnionych podmiotów" do danych objętych tajemnicą telekomunikacyjną. Obecnie uprawnienia wymiaru sprawiedliwości są zbyt szerokie.
- TSUE orzekł w sprawie C-178/22 Procura della Repubblica presso il Tribunale di Bolzano, że artykuł 15 ust. 1 dyrektywy o prywatności i łączności elektronicznej (2002/58/WE) pozwala sądom krajowym na wydawanie zgody na dostęp do danych telekomunikacyjnych. W tej konkretnej sprawie, uwzględniając włoskie prawodawstwo, zastrzegł jednak, że muszą być tu spełnione następujące warunki: musi chodzić o postępowanie w sprawie przestępstwa zagrożonego karą nie mniejszą niż 3 lata pozbawienia wolności; muszą istnieć wystarczające przesłanki popełnienia takich przestępstw; dane muszą być istotne dla ustalenia okoliczności faktycznych.
- Prawo krajowe nie może pozwalać na dostęp do danych telekomunikacyjnych na zasadach generalnej prewencji. Taki dostęp jest uzasadniony wyłącznie w przypadku zwalczania poważnej przestępczości lub zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego.
- W polskim prawie zasady możliwości pozyskania danych telekomunikacyjnych na potrzeby postępowania karnego zostały uregulowane w art. 218 § 1 Kodeksu postępowania karnego i w art. 180c i art. 180d Prawa telekomunikacyjnego. Dane te mogą być ujawniane, jeżeli mają znaczenie dla toczącego się postępowania. Przepisy nie mówią jednak wprost i precyzyjnie, że dostęp do danych uwarunkowany jest wagą przestępstwa i jego rodzajem. Nie zakładają też, że wniosek organu ścigania o dane osobowe jest poddawany weryfikacji.
- Prezes UODO przypomina jednocześnie, że parlament proceduje już projekt ustawy Prawo komunikacji elektronicznej (druk sejmowy nr 423), w którym zawarte są rozwiązania takie same jak dotychczas , niezgodne z orzecznictwem TSUE.

Źródło: Aktualności - UODO

04 Ustawa o ochronie sygnalistów wchodzi w życie 25 września 2024 r. (z pewnymi wyjątkami)

- Ustawa o ochronie sygnalistów w przeważającej części wchodzi w życie 25 września 2024 roku m.in. z wyjątkiem przepisów o zgłoszeniach zewnętrznych, które wejdą w życie po upływie 6 miesięcy od dnia ogłoszenia.
- Podmioty prawne zobowiązane do posiadania procedury zgłoszeń wewnętrznych można podzielić na dwie grupy:
  - Podmioty prawne, które na dzień 1 stycznia lub 1 lipca danego roku zatrudniają co najmniej 50 osób. Są one zobowiązane do ustalenia procedury zgłoszeń wewnętrznych. Wprowadzenie tej procedury w takich organizacjach jest obowiązkowe.
  - Obowiązek wprowadzenia procedury zgłoszeń wewnętrznych, bez względu na ilość zatrudnianych osób, dotyczy także wszystkich podmiotów prawnych prowadzących działalność w zakresie usług, produktów i rynków finansowych oraz przeciwdziałania praniu pieniędzy i finansowaniu terroryzm, bezpieczeństwa transportu i ochrony środowiska (objętych zakresem stosowania aktów prawnych Unii Europejskiej wymienionych w części I.B i II załącznika do dyrektywy 2019/1937).
- Każdy podmiot prawny, który nie jest do tego ustawowo zobowiązany, powinien rozważyć fakultatywne przyjęcie procedury zgłoszeń wewnętrznych. Wydaje się to korzystnym rozwiązaniem dla podmiotu prawnego, by w przypadku ewentualnych nieprawidłowości, mogły zostać one zgłoszone w ramach organizacji, a nie za pośrednictwem zgłoszenia zewnętrznego.
- Należy pamiętać także o dopełnieniu względem sygnalistów obowiązku informacyjnego spełniającego wymogi RODO. Sygnaliści muszą wiedzieć co dokładnie wydarzy się po zrealizowania przez nich zgłoszenia i dlaczego mogą czuć się bezpiecznie. Ponadto, systemy służące do zgłaszania nieprawidłowości (whistleblowing) zostały wskazane przez UODO jako te, które wymagają wykonania oceny skutków dla ochrony danych osobowych (DPIA), w myśl art. 35 RODO.

Źródło: Procedura zgłoszeń wewnętrznych - KPMG Poland

05 Rewolucja na rynku. Wspólny certyfikowany podpis biometryczny od Asseco, Samsung i Xtension

- BiocertiX to system do składania podpisu własnoręcznego na tablecie Samsung za pomocą rysika. Wykorzystywane w tym celu jest oprogramowanie Xtension - rejestrujące i szyfrujące dane biometryczne. Rozwiązanie to łączy tradycyjny podpis z nowoczesną technologią.
- Natomiast wiarygodność całego procesu zapewniają kwalifikowane usługi Asseco: pieczęć elektroniczna i znacznik czasu oraz sprzętowy moduł depozytu klucza chroniącego dane biometryczne. Dane te są zaszyfrowane i powiązane z konkretnym podpisem. Mogą być ujawnione jedynie biegłemu z zakresu grafologii na podstawie decyzji sądu.
- Artur Miękina, dyrektor sprzedaży Projektowej i Rozwoju e-Biznesu w Asseco Data Systems objaśnia, że rozwiązanie jest na tyle intuicyjne, że nie wymaga znajomości technologii. „biocertiX wpisuje się w ekosystem rozwiązań paperless i uzupełnia paletę narzędzi cyfrowych w procesach on-site. Z perspektywy użytkownika wykorzystanie podpisu biometrycznego jest tożsame z podpisywaniem dokumentów zwykłym długopisem, ale o wiele bezpieczniejsze. Ponadto zachowuje pełną moc prawną i dowodową w przypadku sporów sądowych” – tłumaczy.
- BiocertiX zbiera unikalne dane biometryczne osoby, która składa podpis, takie jak: charakterystyka pisma odręcznego, siła nacisku rysika na ekran czy szybkość pisma. Następnie - poprzez odpowiednie algorytmy kryptograficzne - wiąże te informacje z podpisywaną treścią. Tym samym użytkownik zyskuje pewność, że jego podpis nie będzie przez nikogo podrobiony. Dodatkowo, w podpisanym dokumencie, system umieszcza informacje, które w przyszłości pozwolą potwierdzić tożsamość podpisującego, ale także czas złożenia podpisu i poprawność przeprowadzonego procesu.
- W sytuacjach spornych, organizacja może udostępnić biegłemu grafologowi informacje pozwalające potwierdzić prawdziwość złożonego podpisu.

Źródło: Rewolucja na rynku. Wspólny certyfikowany podpis biometryczny od Asseco, Samsung i Xtension | CyberDefence24