
LEX ARTIST

RODO - aktualności

[15.01.2024]

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 Polskie firmy walczą z zegarem w wyścigu o AI – wyniki badania Cisco

02 Konfigurowanie cookiesów analitycznych na urządzeniach użytkowników nie zawsze wymaga ich zgody

03 CNIL opublikowała projekt przewodnika w sprawie oceny skutków transferu danych (TIA)

04 UE: Przyjęto porozumienie w sprawie unijnego aktu dotyczącego cyberodporności (Cyber Resilience Act)

05 Kolejny wyciek danych z placówki ochrony zdrowia

06 Atak na Uniwersytet Zielonogórski. Doszło do wycieku danych?

01 Polskie firmy walczą z zegarem w wyścigu o AI – wyniki badania Cisco

- Najnowsze wyniki badania Cisco AI Readiness Index ujawniają, że tylko 6% polskich organizacji jest w pełni przygotowanych do wdrażania i wykorzystywania sztucznej inteligencji (AI). Tymczasem globalnie, ten odsetek wynosi 14%. Alarmujące jest to, że aż 47% polskich firm obawia się negatywnych konsekwencji dla swojego biznesu, jeśli nie zaczną inwestować w AI w ciągu najbliższego roku.
- Badanie Cisco rozgranicza firmy na cztery kategorie gotowości do AI: Pacesetters (w pełni przygotowani), Chasers (umiarkowanie przygotowani), Followers (ograniczona gotowość) i Laggards (nieprzygotowani). W Polsce tylko 6% firm zalicza się do wspomnianej grupy Pacesetters. Globalnie jest to już 14%. Z kolei aż 64% polskich organizacji znajduje się w dwóch najniższych kategoriach (Laggards i Followers), w porównaniu do 52% na świecie.
- Badanie podkreśla pilność sytuacji: 47% polskich liderów biznesu uważa, że mają maksymalnie rok na wdrożenie strategii AI. Muszą to zrobić zanim ich biznes zacznie ponosić konsekwencje brak wdrożeń. Na świecie, to zdanie podziela 61% ankietowanych.
- Pomimo tych wyzwań, 95% polskich organizacji posiada już strategię AI lub jest w trakcie jej opracowania. To odzwierciedla globalny trend. Priorytetowość wdrożenia AI wzrosła w ostatnich sześciu miesiącach dla 95% firm w Polsce i 97% na świecie. Najwyższym priorytetem dla wdrożeń AI są infrastruktura IT i cyberbezpieczeństwo.
- Wyniki badania Cisco AI Readiness Index są jasnym sygnałem, że polskie firmy muszą przyspieszyć swoje działania w zakresie sztucznej inteligencji. Jest to dla nich konieczne, aby mogły nie zostać w tyle za globalnymi trendami. Stawka jest wysoka – firmy, które nie zdołają dostosować się do szybko zmieniającej się technologicznej rzeczywistości, mogą stracić swoją konkurencyjność na rynku.

Źródło: Polskie firmy walczą z czasem o AI - ccnews.pl

02 Hiszpańska Agencja Ochrony Danych (AEPD): Konfigurowanie cookiesów analitycznych na urządzeniach użytkowników nie zawsze wymaga ich zgody

- Agencia Española de Protección de Datos – Hiszpańska Agencja Ochrony Danych (AEPD) stwierdziła, że czasami konfigurowanie cookiesów analitycznych na urządzeniach użytkowników nie wymaga ich zgody.
- Zgodnie z dyrektywą ePrivacy i przepisami państw członkowskich UE, instalowanie jakichkolwiek informacji na urządzeniu użytkownika lub uzyskiwanie dostępu do danych z urządzenia użytkownika wymaga uprzedniej zgody. Istnieje jednak wyjątek dla "ściśle niezbędnych" plików cookie, które są wymagane do komunikacji lub świadczenia usług na wyraźne żądanie użytkownika.
- Według AEPD instalowanie analitycznych plików cookie, zwykle używanych do śledzenia wizyt na stronie internetowej i zachowań użytkowników, może obejść wymóg uzyskania zgody zgodnie z prawem hiszpańskim. Nie można jednak łączyć pozyskanych danych z innymi procesami, udostępniać ich podmiotom trzecim ani śledzić użytkowników w różnych witrynach lub aplikacjach.
- AEPD zastrzega, że pliki cookie wykorzystywane do następujących celów związanych z zarządzaniem stroną internetową mogą być przechowywane bez zgody (m.in.): analizowanie urządzeń, przeglądarek i rozmiarów ekranów odwiedzających stronę; Gromadzenie statystyk dotyczących czasu ładowania strony i wskaźników zaangażowania (takich jak współczynnik odrzuceń); Zestawienie danych o działaniach użytkowników (kliknięcia, wybory). Przetwarzanie danych wykraczające poza te określone zastosowania wymaga zgody użytkownika, aby można je było uznać za zgodne z prawem.
- Według AEPD, w przypadku plików cookie pozyskiwanych bez zgody, wykorzystywanych do pomiaru oglądalności strony, potrzebne są następujące zabezpieczenia: informowanie użytkowników o tym za pośrednictwem polityki prywatności, ograniczenie żywotności plików cookie do 13 miesięcy bez automatycznego przedłużania przy nowych wizytach na stronie oraz przechowywanie zebranych danych przez maksymalnie 25 miesięcy i regularne sprawdzanie tych okresów retencji, aby upewnić się, że są one absolutnie niezbędne.

Źródło: https://www.linkedin.com/posts/mateusz-kupiec-cipp-e-289700121_analytical-cookies-consent-activity-7152295789753442304-0onw?utm_source=share&utm_medium=member_desktop

03 CNIL opublikował projekt przewodnika w sprawie oceny skutków transferu danych (TIA)

- Przewodnik zawiera metodologię i listę kontrolną, które mają pomóc w przeprowadzeniu TIA, zgodnie z sześcioetapowym procesem zalecanym przez Europejską Radę Ochrony Danych. Jego celem jest ukierunkowanie analizy przekazywania danych z EOG do państwa trzeciego, ze szczególnym uwzględnieniem zgodności z art. 46 RODO. Nie dotyczy to jednak sytuacji, gdy kraj docelowy wydał decyzję Komisji Europejskiej stwierdzającą odpowiedni stopień ochrony lub jeśli przekazanie podlega odstępstwom wynikającym z art. 49 RODO.
- TIA ocenia, czy podmiot odbierający dane jest w stanie wywiązać się z obowiązków, biorąc pod uwagę przepisy i praktyki państwa trzeciego, w szczególności w odniesieniu do dostępu władz lokalnych do danych osobowych. Eksporterzy muszą ocenić poziom ustawodawstwa i praktyki kraju przeznaczenia w odniesieniu do konkretnego transferu. W razie potrzeby TIA powinna określić, czy dodatkowe środki mogą zaradzić niedociągnięciom w zakresie ochrony danych, aby spełnić normy UE.
- Przewodnik jest podzielony na sześć różnych kroków, które należy wykonać, aby przeprowadzić TIA:

1) Poznaj swój transfer danych;
2) Dokumentuj narzędzia wykorzystywane do transferu danych;
3) Oceń przepisy i praktyki w kraju przeznaczenia danych oraz skuteczność narzędzia do przekazywania danych;
4) Wdróż środki uzupełniające i niezbędne procedury;
5) Ponownie oceniaj w odpowiednich odstępach czasu poziom ochrony danych i monitoruj potencjalne zmiany, które mogą mieć wpływ na bezpieczeństwo danych osobowych.

Źródło: Transfer Impact Assessments: the CNIL is seeking public input on TIA guide - Hogan Lovells Engage; Draft practical guide - Transfer impact assessment (cnil.fr)

04 UE: Przyjęto porozumienie w sprawie unijnego aktu dotyczącego cyberodporności (Cyber Resilience Act)

- Rozporządzenie w sprawie cyberodporności jest elementem realizacji unijnej strategii cyberbezpieczeństwa z 2020 roku. Stanowi także działanie spójne z innymi politykami takimi jak projektowana Dyrektywa NIS2 (w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii). Przewiduje się, że regulacja wejdzie w życie w najbliższych miesiącach; na dostosowanie przepisów do nowych wymagań przedsiębiorcy mają mieć 36 miesięcy.
- Zgodnie z Cyber Resilience Act, producenci produktów z elementami cyfrowymi, objętych jego zastosowaniem (w tym producenci oprogramowania) zobowiązani będą do regularnego udostępniania konsumentom aktualizacji zabezpieczeń dotyczących zakupionych przez nich produktów.
- Nowe obowiązki mają dotyczyć nie tylko momentu wprowadzania produktu z elementami cyfrowymi na rynek, lecz całego cyklu jego życia, tak, aby poziom bezpieczeństwa produktu był stały, a konsument miał wiedzę o jego zakresie oraz możliwość korzystania z produktu w sposób bezpieczny przez wiele lat. Spełnienie nowych norm ma być potwierdzone specjalnym certyfikatem CE mającym ułatwić obrót na rynku wewnętrznym.
- Na producentów nałożone zostaną również obowiązki w zakresie zgłaszania cyberincydentów. Zgłoszenia do Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) będzie trzeba dokonać w ciągu 24 godzin od momentu uzyskania informacji o aktywnie wykorzystywanej podatności produktu, czy też incydencie mającym wpływ na jego bezpieczeństwo.
- Rozporządzenie przewiduje kary pieniężne w wysokości do 15 000 000 EUR lub do 2,5 % całkowitego rocznego światowego obrotu przedsiębiorstwa - w przypadku niezgodności z zasadniczymi wymogami cyberbezpieczeństwa bądź obowiązkami producentów wynikającymi z rozporządzenia; Szczegółowa regulacja w zakresie kar nakładanych w przypadku naruszenia rozporządzenia pozostawiona została zasadniczo państwom członkowskim.

Źródło: Legal Alert: Unijny akt dotyczący cyberodporności - KPMG Poland

05 Kolejny wyciek danych z placówki ochrony zdrowia

- Dane osobowe, którymi dysponował Powiatowy Szpital Specjalistyczny w Stalowej Woli, były udostępniane osobie z zewnątrz – przekazywane mailem na adres, na który nie powinny trafić. Sprawę bada policja, prokuratura i Urząd Ochrony Danych Osobowych.
- O stwierdzeniu naruszenia ochrony danych osobowych, polegającym na naruszeniu poufności przetwarzanych danych osobowych, placówka poinformowała w komunikacie na swojej stronie internetowej. Do nieprawidłowości miało dochodzić w okresie w okresie od 19 listopada 2023 r. do 21 grudnia 2023 r. „Nieustalona osoba trzecia" miała otrzymywać dane na swój adres poczty elektronicznej.
- Szpital – jako administrator danych osobowych – powiadomił o sytuacji osoby, których dane trafiły w niepowołane ręce, aby mogły zapobiec ewentualnym szkodom z tego tytułu.
- Szpital zapewnia też w wydanym komunikacie, że „podjął wszelkie możliwe działania mające na celu minimalizację skutków naruszenia, jak również zapewnienia ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną".
- Na razie nie wiadomo, czy dane zostały w ogóle w jakikolwiek sposób wykorzystane i czy osoby trzecie zapoznały się z danymi. Szpital zapewnia, że sprawa minimalizowania skutków zdarzenia jest traktowana priorytetowo oraz że pozostaje w kontakcie z właściwymi służbami w celu szybkiego wyjaśnienia sprawy.
- To kolejna w ostatnim czasie sytuacja, kiedy dane pacjentów dostały się w niepowołane ręce. Jak informowaliśmy, 19 listopada laboratoria ALAB zaobserwowały próbę zmasowanego ataku na swoje serwery. Analiza wykazała, że w wyniku ataku hakerzy uzyskali dostęp do danych osobowych pacjentów, t.j.: imię i nazwisko, numer PESEL, data urodzenia, miejsce zamieszkania oraz wynik badania laboratoryjnego.

Źródło: Cowzdrowiu - Kolejny wyciek danych z placówki ochrony zdrowia

06 Atak na Uniwersytet Zielonogórski. Doszło do wycieku danych?

- Uniwersytet Zielonogórski w ostatni weekend padł ofiarą cyberataku. Ucierpiała m.in. poczta uczelni i system służący do pobierania kluczy do sal wykładowych. Władze placówki miały poinformować studentów o „naruszeniu danych osobowych".
- W wyniku celowanego ataku hackerskiego na Centrum Przetwarzania Danych Uniwersytetu Zielonogórskiego, przeprowadzonego w nocy z dnia 5 na 6 stycznia 2024 r., „zostały zablokowane wszystkie serwisy działające w środowisku wirtualizacji utrzymywanym w Centrum Komputerowym Uniwersytetu Zielonogórskiego".
- Nie funkcjonowały: poczta uczelni (planowo ma zostać przywrócona 10 stycznia br.); System Centralnego Druku; system pobierania kluczy do sal wykładowych; systemy biblioteczne uczelni. Działała natomiast oficjalna strona internetowa placówki, a kilka godzin później przywrócono działanie kilku wewnętrznych systemów.
- Jak podaje zielonogórska „Wyborcza", w środę biuro prasowe uczelni miało wysłać do studentów wiadomość o „naruszeniu ochrony danych osobowych". W następstwie przeprowadzonego w dniu 06.01.2024 r. ataku hakerskiego doszło do czasowego zablokowania możliwości odczytu plików maszyn wirtualnych zawierające dane osobowe pracowników i studentów. Zaszyfrowane pliki zawierały następujące dane osobowe: w odniesieniu do pracowników: imię i nazwisko, numer PESEL, adres e-mail. W odniesieniu do studentów: imię i nazwisko, data urodzenia, adres zamieszkania, adres e-mail, numer PESEL, nr legitymacji studenckiej, nr albumu, nr dowodu osobistego.
- Studenci z którymi rozmawiała „GW" mieli stwierdzić, że uczelnia „się skompromitowała".

Źródło: Atak na Uniwersytet Zielonogórski. Doszło do wycieku danych? | CyberDefence24