
LEX ARTIST

RODO - aktualności

[03.01.2024]

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 Aplikacja mobilna zgodna z RODO - czyli jaka?

- Poniżej kilka istotnych reguł, które niewątpliwie będą pomocne przy tworzeniu aplikacji mobilnych zgodnych z RODO:

1. Pozyskiwanie zgody albo zapewnienie innej przesłanki uprawniającej do przetwarzania danych. Zgoda na przetwarzanie danych nie zawsze będzie potrzebna (przy aplikacjach mobilnych bardzo często dochodzi do zawarcia umowy o świadczenie usług drogą elektroniczną), ale nie jest wykluczone, że pewne funkcjonalności będą jej wymagały np. zgoda na geolokalizację.
2. Minimalizacja danych. Należy ograniczyć ilość zbieranych danych do niezbędnego minimum.
3. Transparentność procesu gromadzenia danych osobowych. Należy pamiętać o obowiązku informacyjnym, czyli o klauzuli, w której dostarczamy użytkownikom jasne informacje na temat tego, kto będzie przetwarzał ich dane, jakie dane, w jaki sposób będą przetwarzane i do jakich celów zostaną wykorzystane.
4. Retencja danych, czyli określenie, jak długo będą przechowywane dane zebrane dla poszczególnych celów, dla których je pozyskujemy. Niektóre dane będzie można przechowywać dłużej, np. dane związane z kwestiami rozliczeniowymi, inne krócej, np. do czasu wycofania zgody, co może nastąpić w dowolnym momencie. Informacje dotyczące retencji danych powinny zostać zamieszczone w obowiązku informacyjnym.
5. Zabezpieczenie danych osobowych. Nie zapominajmy też o regularnych aktualizacjach, zwłaszcza tych, które są krytyczne dla bezpieczeństwa danych. Koniecznie też, zanim aplikacja zadebiutuje na rynku, należy przeprowadzić testy penetracyjne..
6. Sprawny proces obsługi żądań zgłaszanych przez użytkowników aplikacji mobilnej. Już na etapie projektowania całego procesu należy zadbać o dobry kanał komunikacyjny z użytkownikami oraz zatrudnienie kompetentnych osób, które będą obsługiwały takie zgłoszenia.
7. Weryfikacja potencjalnych dostawców usług pod kątem bezpieczeństwa. Należy pamiętać także o tym, by zapewnić odpowiednie i bezpieczne zapisy w umowach powierzenia przetwarzania danych, które trzeba będzie zawrzeć z dostawcami usług.

02 TSUE: podwójne podstawy prawne przetwarzania szczególnych kategorii danych a odpowiedzialność z tytułu RODO

- W orzeczeniu w sprawie C-667/21 TSUE wyjaśnił istotne aspekty ochrony danych związane z przetwarzaniem szczególnych kategorii danych i odpowiedzialnością Administratora wynikającą z RODO;
- MDK North Rhine, spółka publiczna, przetwarza dane dotyczące zdrowia w celu oceny zdolności pracowników do pracy, w tym personelu. Tymi wrażliwymi danymi zajmuje się "jednostka organizacyjna do spraw szczególnych". Pracownik działu IT przebywający na zwolnieniu lekarskim twierdził, że jego dane dotyczące zdrowia były przetwarzane niezgodnie z prawem, gdy jego pracodawca uzyskał je w celu przeprowadzenia badań lekarskich. Zażądał 20 000 euro odszkodowania, czemu MDK Nordrhein odmówiła.
- Art. 9 ust. 2 lit. h) RODO zezwala na przetwarzanie danych dotyczących zdrowia pod pewnymi warunkami. TSUE wyjaśnił, że wyjątek ten ma zastosowanie, gdy organ oceny medycznej przetwarza dane dotyczące zdrowia pracownika nie jako pracodawca, ale jako część służby medycznej w celu oceny jego zdolności do pracy.
- Ponadto, art. 9 ust. 3 RODO nie zobowiązuje administratora do uniemożliwienia współpracownikom dostępu do danych dotyczących zdrowia pracownika. Państwa członkowskie lub przepisy szczególne mogą jednak nakładać takie obowiązki na podstawie art. 9 ust. 4 i innych przepisów RODO.
- Przetwarzanie danych dotyczących zdrowia na podstawie art. 9 ust. 2 lit. h) RODO, aby było zgodne z prawem, musi również spełniać warunki określone w art. 6 ust. 1 RODO.
- TSUE odniósł się także do kwestii odszkodowania wynikającego z RODO. Ma ono na celu pokrycie rzeczywistych szkód i nie ma charakteru represyjnego. Odpowiedzialność zależy od udowodnienia winy po stronie odpowiedzialnej. Jeśli nie można udowodnić braku winy, domniemywa się, że strona ponosi odpowiedzialność. Art. 82 nie wymaga przy tym uwzględniania stopnia winy przy ustalaniu zadośćuczynienia za krzywdę.

Źródło: https://www.linkedin.com/posts/mateusz-kupiec-cipp-e-289700121_cjeu-gdpr-privacy-activity-7143553168788955136-s6wW?utm_source=share&utm_medium=member_desktop

03 Tryb incognito to fikcja? Google idzie na ugodę i zapłaci miliardy dolarów

- Alphabet zgodził się na zawarcie ugody w sprawie sądowej, twierdząc, że potajemnie śledził korzystanie z internetu przez miliony ludzi, którzy myśleli, że przeglądają go prywatnie - informuje Reuters.
- Ta głośna sprawa miała swoje początki kilka lat temu. Twierdzono, że analityka, pliki cookie i aplikacje Google pozwalają śledzić aktywność użytkowników, nawet gdy używali trybu incognito w przeglądarce Google Chrome.
- Argumentowano, że Google zamienił się w skarbnicę informacji, pozwalając dowiedzieć się firmie o bardzo prywatnych aspektów z życia użytkowników - przyjaciołach, hobby, ulubionych potrawach, nawykach żywieniowych i "potencjalnie krępujących rzeczach" wyszukiwanych w internecie.
- Spór toczył się o to, czy Google złożył wiążącą obietnicę odnośnie do tego, że nie będzie gromadzić danych swoich użytkowników, gdy przeglądają oni strony internetowe w trybie incognito.
- Złożony w 2020 roku pozew domagał się od firmy co najmniej 5 mld dolarów. Pełne warunki ugody nie zostały ujawnione, ale prawnicy stwierdzili, że zgodzili się na wiążące warunki w drodze mediacji. Formalna ugoda ma zostać przedstawiona sądowi do zatwierdzenia 24 lutego 2024 roku.
- Wiele wskazuje więc na to, że użytkownicy otrzymają niebawem od Google'a pieniądze. Każdy z pozywających użytkowników chce otrzymać co najmniej 5 tys. dolarów w ramach odszkodowania za naruszenie federalnych przepisów Kalifornii dotyczących prywatności.

Źródło: Tryb incognito to fikcja? Google idzie na ugodę i zapłaci miliardy - Bankier.pl

04 Oszustwo na 800+. ZUS ostrzega przed próbami wyłudzenia pieniędzy

- Zakład Ubezpieczeń Społecznych przestrzegł w czwartek przed oszustami, którzy oferują pomoc w wypełnieniu wniosku w sprawie świadczenia 800+.
- "Docierają do nas informacje dotyczące oszustów, którzy w rozmowach telefonicznych oferują pomoc w wypełnieniu wniosku w sprawie świadczenia 800+. Żądają w zamian kilkadziesiąt złotych" – przekazał PAP rzecznik ZUS Paweł Żebrowski.
- "W ostatnich tygodniach w internecie pojawiły się również fałszywe doniesienia dotyczące rzekomego wyrównania świadczenia wychowawczego z kwoty 500 zł do 800 zł za okres od sierpnia 2023 r. do końca bieżącego roku" – dodał rzecznik.
- Przypomniał, że zgodnie z ustawą wysokość świadczenia wychowawczego do końca 2023 r. to 500 zł na każde dziecko do ukończenia przez nie 18 lat. Od 1 stycznia 2024 r. świadczenie wychowawcze 500+ zmieni się w 800+.
- "Podwyżka do 800 zł nastąpi automatycznie bez konieczności składania wniosku. Po nowym roku uprawnieni otrzymają wypłaty w nowej wysokości, a o tym fakcie zostaną poinformowani na Platformie Usług Elektronicznych (PUE) ZUS" – podkreślił Żebrowski.

Źródło: Wniosek na 800 plus to oszustwo. ZUS ostrzega przed próbami wyłudzenia pieniędzy - Bankier.pl

05 Cyberatak na największego operatora aplikacji parkingowych. Tysiące poszkodowanych

- Firma EasyPark Group, będąca właścicielem aplikacji do parkowania RingoGo oraz ParkMobile, poinformowała o dokonanym na nią cyberataku.
- Jak podaje „The Guardian", naruszenie zostało wykryte przez przedsiębiorstwo 10 grudnia br. Kilka dni później mieli się o nim dowiedzieć poszkodowani klienci, a także odpowiednie organy, m.in. brytyjskie Biuro Komisarza ds. Informacji (org. Information Commissioner's Office).
- Z danych podanych przez EasyPark Group wynika, że hakerzy wykradli dane zawierające nazwiska klientów, numery telefoniczne, adresy mailowe itd. Pozyskano także informacje obecne na kartach kredytowych klientów, ale – jak zapewniają przedstawiciele firmy – „żadna kombinacja skradzionych danych nie może być wykorzystana do dokonania płatności przez przestępców".
- W chwili obecnej nie wiadomo, ile osób mogło ucierpieć w wyniku ataku. Jak na razie jedyną liczbą podaną do publicznej wiadomości jest 950 – dane tylu brytyjskich użytkowników RingGo mieli zdobyć hakerzy.
- Poszkodowanych jest jednak prawdopodobnie znacznie więcej. Z informacji podanych przez rzecznika EasyPark Group wynika, że większość klientów zaatakowanej firmy pochodzi z Europy kontynentalnej, a to oznacza naruszenie danych tysięcy użytkowników. Na ten moment nie ma żadnych informacji mówiących o ewentualnym okupie, którego za ukradzione dane żądaliby przestępcy.
- EasyPark zalicza się do grona największych firm oferujących aplikacje parkingowe na Starym Kontynencie. Aplikacje takie jak wspomniany w tekście RingGo czy ParkMobile są używane w ponad 4000 miast w 23 krajach.

Źródło: Cyberatak na największego operatora aplikacji parkingowych. Tysiące poszkodowanych | CyberDefence24

06 Jakie skutki dla płatnika ma informacja o naruszeniu przez ZUS ochrony jego danych osobowych

- Jeżeli administrator danych uznał, że zaistniałe naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, to zgodnie z art. 34 ust. 1 RODO zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
- Zawiadomienie opisuje charakter naruszenia ochrony danych osobowych oraz zawiera informacje i środki, o których mowa w art. 33 ust. 3 lit. b, c i d RODO i obejmuje następujące informacje: opis charakteru naruszenia; imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji; opis możliwych konsekwencji naruszenia ochrony danych osobowych; opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
- Zgodnie z art. 82 ust. 1 RODO każda osoba, która poniosła szkodę majątkową w wyniku naruszenia przepisów RODO, ma prawo uzyskać od administratora odszkodowanie za poniesioną szkodę. Istotne znaczenie ma tutaj ustalenie wystąpienia adekwatnego związku przyczynowego między zaistnieniem naruszenia przepisów o ochronie danych a wystąpieniem szkody.
- Prawo do odszkodowania za poniesioną szkodę ma zatem wyłącznie osoba, która poniosła rzeczywistą szkodę w wyniku naruszenia przez administratora przepisów RODO. Skorzystanie z przykładowych środków zaradczych (także tych wiążących się z poniesieniem dodatkowych kosztów przez płatnika) nie jest tożsame z poniesieniem szkody majątkowej w rozumieniu przepisów prawa, natomiast jest zabezpieczeniem przed skutkiem nieuprawnionego użycia danych osobowych.
- Administrator zawiadamia osobę, której dane dotyczą, o naruszeniu bez zbędnej zwłoki. Zgodnie z wyjaśnieniami prezesa UODO oznacza to, że administrator powinien zrealizować ów obowiązek tak szybko, jak pozwalają na to okoliczności danej sprawy.

Źródło: Jakie skutki dla płatnika ma informacja o naruszeniu przez ZUS ochrony jego danych osobowych [Poradnia ubezpieczeniowa] - GazetaPrawna.pl