
LEX ARTIST

RODO - aktualności

[11.03.2024]

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 TSUE: Informacje o preferencjach internautów to dane osobowe

02 Naruszenie poufności danych pracownika: co powinien zrobić pracodawca

03 NSA: Przekazanie pracodawcy danych pracownika, który użył służbowego maila do celów prywatnych, to naruszenie RODO

04 Ministerstwo Cyfryzacji: Naruszenie danych osobowych pracowników

05 Akt w sprawie AI w kontekście RODO: 10 kluczowych informacji

01 TSUE: Informacje o preferencjach internautów to dane osobowe

- Trybunał Sprawiedliwości Unii Europejskiej zajął się sprawą dotyczącą internetowych aukcji danych osobowych, które są wykorzystywane, aby dopasować reklamy do profilu odbiorcy. TSUE odpowiedział na pytania prejudycjalne sądu w Belgii.
- Chodzi o mechanizm opracowany przez stowarzyszenie branży reklamy cyfrowej IAB Europe, znany jako TCF (z ang. Transparency & Consent Framework). Mamy z nim do czynienia, gdy na odwiedzanej przez nas stronie wyskakuje okienko (tzw. pop-up) z żądaniem zgody na zbieranie danych i przekazywanie ich „zaufanym partnerom IAB Europe". Pozwala to śledzić aktywność internautów w sieci. Zebrane w ten sposób informacje o preferencjach internautów są kodowane i przechowywane po to, aby ostatecznie trafić na specjalne giełdy reklamowe.
- Sprawa toczy się od 2019 r., gdy grupa organizacji – w tym Panoptykon – wniosła do krajowych organów ochrony danych osobowych skargi na IAB Europe, twierdząc, że system TCF narusza RODO.
- Według belgijskiego organu IAB Europe przetwarza dane bez ważnej podstawy prawnej, którą w tym przypadku powinna być zgoda użytkowników. Trudno mówić, by kliknięcie w „okienko zgody" spełniało wymogi w pełni świadomej i dobrowolnej zgody na gruncie RODO, jeśli przeciętny użytkownik nie jest w stanie się zorientować, co właściwie dzieje się z jego danymi. Może mu się wydawać, że dzieli się danymi tylko z administratorem tej strony – podczas gdy w rzeczywistości korzysta z nich ogromna liczba agencji, platform reklamowych, brokerów danych i innych podmiotów – mówi Dorota Głowacka, prawniczka z fundacji Panoptykon.
- TSUE potwierdził, że TC String zawiera informacje dotyczące możliwego do zidentyfikowania użytkownika - a zatem stanowi dane osobowe w rozumieniu RODO. TSUE orzekł także, że IAB Europe należy uznać za „współadministratora" w rozumieniu RODO. Z zastrzeżeniem ustaleń, których dokonanie należy do sądu w Belgii, IAB Europe wpływa na operacje przetwarzania danych przy zapisywaniu informacji w TC String i ustala, wspólnie ze swoimi członkami, cele tych operacji i sposoby ich dokonywania.

Źródło: TSUE orzekł w sprawie śledzenia w sieci. Chodzi o profilowanie - GazetaPrawna.pl; Informacje o preferencjach internautów to dane osobowe. Zapadł wyrok TSUE - GazetaPrawna.pl

02 Naruszenie poufności danych pracownika: co powinien zrobić pracodawca

- O naruszeniu poufności danych osobowych mówimy w przypadku ich nieautoryzowanego ujawnienia, czyli umożliwienia ich przetwarzania (nawet poprzez sam wgląd) osobie, która nie jest do tego uprawniona.
- Praktyka pokazuje, że dane osobowe w obszarze HR narażone są na takie ujawnienie najczęściej np. poprzez wysłanie pracownikowi listy płac całego działu, wydanie świadectwa pracy lub zaświadczenia o zarobkach (np. na cele kredytowe) nie temu pracownikowi, którego dokument ten dotyczy, uzyskanie dostępu do PUE ZUS pracodawcy jako płatnika przez nieuprawnionego pracownika, co powoduje dostęp do danych ubezpieczeniowych innych osób, lub chociażby ujawnienie danych dotyczących jego zdrowia lub zajęć komorniczych osobom nieuprawnionym.
- Aby zminimalizować ryzyko naruszenia poufności danych zatrudnionych osób, należy działać prewencyjnie. Ważne jest przede wszystkim opracowanie systemu uprawnień do przetwarzania danych, a co za tym idzie – również uprawnień dostępowych do firmowych i zewnętrznych systemów informatycznych. Tak samo bowiem ważny jest adekwatny dostęp do wewnętrznego systemu kadrowego, jak i platformy PUE ZUS lub systemu bankowości, za pośrednictwem którego wypłacane są wynagrodzenia.
- Kluczowe są też stały monitoring takich uprawnień i ich odpowiednia modyfikacja (w tym ograniczenie lub całkowite cofnięcie) stosownie do zmian kadrowych. Jednym z najczęstszych błędów pracodawców w sytuacji rozwiązania umowy o pracę lub zmiany stanowiska jest brak natychmiastowego cofnięcia dostępu do firmowych lub zewnętrznych baz danych.
- Nieuprawnione ujawnienie tych danych rodzi odpowiedzialność przed prezesem UODO. Jeśli stwierdzone ryzyko naruszenia praw lub wolności pracownika jest więcej niż mało prawdopodobne, konieczne jest niezwłoczne zawiadomienie o fakcie naruszenia prezesa Urzędu Ochrony Danych.

Źródło: Naruszenie poufności danych pracownika: co powinien zrobić pracodawca - GazetaPrawna.pl

03 NSA: Przekazanie pracodawcy danych osobowych jego pracownika, który użył służbowego maila do celów prywatnych to naruszenie przepisów RODO

- Spółdzielnia mieszkaniowa wdała się w konflikt z jednym ze swoich członków. Jeden z właścicieli mieszkania korespondował w sprawie rozliczeń finansowych ze spółdzielnią posługując się służbowym adresem e-mail szpitala wojewódzkiego, w którym był zatrudniony. W ten sposób spółdzielnia pozyskała jego dane osobowe tj. imię, nazwisko i adresu zamieszkania.
- Odpowiedź na jedno z pism właściciela mieszkania spółdzielnia przesyłała również do wiadomości jego pracodawcy tj. szpitala. Powodem tego było wykorzystanie przez służbowego adresu e-mail dla celów niezwiązanych z obowiązkami służbowymi. To nie spodobało się głównemu adresatowi, który zażądał od prezesa spółdzielni zaprzestania przetwarzania jego danych osobowych. Gdy ta odmówiła — skutecznie jak się później okazało — poskarżył się do prezesa Urzędu Ochrony Danych Osobowych (UODO).
- Zdaniem UODO, spółdzielnia udostępniając dane osobowe członka spółdzielni szpitalowi wykroczyła poza cel, w którym je pozyskała. Podkreślił, że spółdzielnia nie wskazała podstawy prawnej udostępnienia danych osobowych pracodawcy właściciela mieszkania. W ocenie UODO udostępnienie danych podyktowane "wykorzystaniem służbowego maila dla celów nie związanych z obowiązkami służbowymi" nie mieści się w realizacji pierwotnego celu przetwarzania, a ponadto działanie to nie było niezbędne dla udzielenia odpowiedzi przez spółdzielnie. Sprawa skończyła się na upomnieniu.
- Taki obrót sprawy nie satysfakcjonował spółdzielni.W skardze do WSA w Warszawie spółdzielnia przekonywała, że inicjatorem prowadzenia korespondencji za pośrednictwem służbowej skrzynki e-mail był uczestnik postępowania i to on zaangażował w sprawę swojego pracodawcę. Ta argumentacja nie przekonała jednak WSA, a ostatecznie również sądu kasacyjnego.
- Oddalając skargę kasacyjną spółdzielni NSA zgodził się, że jej działanie stanowiło przetwarzanie danych osobowych poprzez ich "udostępnienie". I nie ma znaczenia, że sporne dane pozostawały już w dyspozycji szpitala, tj. były mu znane jako pracodawcy oraz jako administratorowi adresu e-mail, z którego pracownik korzystał prowadząc korespondencję ze spółdzielnią.

Źródło: NSA: Firmowy e-mail a RODO. Kary za naruszenie ochrony danych osobowych - rp.pl

04 Ministerstwo Cyfryzacji: Naruszenie danych osobowych pracowników

- W Ministerstwie Cyfryzacji doszło do naruszenia danych osobowych. Powodem był błąd jednego z pracowników.
- Wyciek miał polegać na udostępnieniu w EZD (system do Elektronicznego Zarządzania Dokumentacją) przez pracownika Biura Budżetowo-Finansowego w resorcie tabeli z wynagrodzeniami byłych i obecnych pracowników Ministerstwa Cyfryzacji za 2024 rok. W ten sposób przekazał to przez pomyłkę pracownikowi Centralnego Ośrodka Informatyki.
- Incydent - jak informuje w piśmie dyrektor generalny MC - był „niezamierzony" i miał wynikać z faktu „zbieżności nazwisk" osób w systemie. „Niemniej jednak w efekcie doszło do naruszenia ochrony danych osobowych, polegającego na utracie poufności" - czytamy w dokumencie.
- Według resortu, ryzyko „nieuprawnionego wykorzystania danych" jest niskie. Natomiast 19 stycznia incydent ten zgłoszono do Prezesa Urzędu Ochrony Danych Osobowych i „podjęto środki zaradcze" w postaci m.in. „zobowiązania pracowników do bezwzględnego weryfikowania danych adresata do którego wysyłana jest korespondencja" oraz „przypomnienia wszystkim pracownikom o zasadach ochrony danych osobowych w korespondencji".
- Pracownicy resortu zostali także poinformowani o prawie do wniesienia skargi do PUODO oraz do skorzystania z ochrony prawnej przed sądem.

Źródło: Ministerstwo Cyfryzacji. Naruszenie danych osobowych pracowników | CyberDefence24

05 Akt w sprawie AI w kontekście RODO: 10 kluczowych informacji

- W preambule Aktu o sztucznej inteligencji wyraźnie podkreślono niezależność reżimów ochrony w „AI Act" i RODO. Ich wzajemnej relacji nie można w związku z tym traktować jako lex generalis i lex specialis (jedno nie uchyla drugiego i odwrotnie).
- Z uwagi na powyżej wskazaną okoliczność, że „AI Act" nie jest lex specialis w stosunku do RODO, dostawcy i użytkownicy rozwiązań sztucznej inteligencji będą musieli łącznie spełnić warunki legalności określone w obydwóch tych aktach prawnych.
- Jedną z istotnych różnic pomiędzy RODO a Aktem w sprawie sztucznej inteligencji jest to, że pierwszy z tych aktów prawnych koncentruje się na ochronie danych osobowych na wszystkich etapach ich przetwarzania, począwszy od ich zbierania (input), podczas gdy nacisk w AI Act położony jest na wynikach wykorzystania sztucznej inteligencji (output).
- Zarówno RODO, jak „AI Act" oparte są na koncepcji „risk based approach", różne jest jednak podejście do tej zasady na gruncie obydwóch tych aktów prawnych. Istotą RODO jest podejście „right based approach", która wyraża się w przyznaniu podmiotom danych szeregu praw (np. prawa do informacji, prawa dostępu do danych, prawa do bycia zapomnianym). Sam AI Act bezpośrednio nie kreuje natomiast praw na rzecz osób fizycznych, których dane są przetwarzane przez systemy sztucznej inteligencji.
- Przepisy RODO poszerzają możliwości ochrony osób, których dane osobowe są wykorzystywane przez sztuczną inteligencję. Przykładem są regulacje dotyczące prawa podmiotów danych (art. 15 RODO), czy możliwość dochodzenia odszkodowań cywilnoprawnych (art. 82 RODO), np. w sytuacjach naruszenia poprzez użycie systemu sztucznej inteligencji zasad określonych w art. 22 RODO (automatyczne decyzje).
- Sankcje administracyjne, w tym kary pieniężne są w obu aktach zbliżone konstrukcyjnie. Overlapping regulacyjny niesie ryzyko „podwójnego" nałożenia kar na administratora oraz dostawcę/użytkownika systemu sztucznej inteligencji, w wyniku jednego zdarzenia (np. wykorzystania systemu SI niezgodnie z warunkami określonymi w art. 22 RODO).