
LEX ARTIST

# RODO - aktualności

[29.01.2024]

# 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 TSUE ogranicza odpowiedzialność administratorów za naruszenie RODO

02 Międzynarodowy Dzień Ochrony Danych Osobowych – firm nie stać na wyzwania związane z ochroną danych

03 Rosyjscy hackerzy zaatakowali pocztę HP i Microsoftu

04 Oddział Amazon we Francji ukarany karą w wysokości 32 milionów euro za nadmierne śledzenie produktywności pracowników

05 EROD uruchamia narzędzie do audytu stron internetowych

# 01 TSUE ogranicza odpowiedzialność administratorów za naruszenie RODO

- Najnowszy wyrok TSUE (z 25 stycznia 2024 r. w sprawie C-687/21) ogranicza w sposób znaczący odpowiedzialność administratora w przypadku utraty kontroli nad danymi osobowymi. Zgodnie z nim sama obawa osoby, której dane trafiły w niepowołane ręce, przed ich bezprawnym wykorzystaniem nie stanowi podstawy do odszkodowania, jeśli nikt z tymi danymi nie mógł się zapoznać.
- Powszechnie znana praktyka polegająca na tym, że po naruszeniu poufności danych, np. przez wysłanie dokumentów niewłaściwej osobie, odbiera się od tej osoby oświadczenie o tym, że nie zapoznała się z tymi danymi i że je usunęła, ma więc praktyczne znaczenie. Dotychczas tego typu działania traktowano jako mało istotne, przynajmniej z punktu widzenia samego naruszenia – bo naruszenie ma charakter obiektywny i nie ma znaczenia, co i kto oświadczył. Najnowszy wyrok tego nie zmienia w kontekście samego naruszenia, ale zmienia w kontekście jego skutków – jeżeli wykażemy, że co prawda do naruszenia doszło, ale z danymi nikt się nie zapoznał, to o odszkodowaniu nie ma mowy - tłumaczy dr Paweł Litwiński,
- Wcześniejsze orzecznictwo z grudnia 2023 r. wiele osób interpretowało w taki sposób, że już sama obawa przed wykorzystaniem danych osobowych daje podstawę do uzyskania odszkodowania. W swoim najnowszym wyroku trybunał potwierdza, że osoba, której dane dotyczą, może, w wyniku tymczasowej utraty kontroli nad danymi osobowymi, ponieść szkodę niematerialną, ale musi przedstawić na to dowody. Samo naruszenie RODO nie jest natomiast wystarczające do uzasadnienia roszczenia.
- Dodatkowo trybunał uznał, że w przypadku gdy żadna osoba trzecia nie zapoznała się z danymi osobowymi, czyli gdy ryzyko niewłaściwego wykorzystania danych przez nieuprawnioną osobę trzecią jest jedynie hipotetyczne, to nie może to prowadzić do odszkodowania.
- Ponadto, zdaniem TSUE nieumyślne naruszenie RODO przez pracownika nie oznacza automatycznie, że środki techniczne i organizacyjne podjęte przez administratora w celu ochrony danych były nieodpowiednie.

Źródło: TSUE ogranicza odpowiedzialność administratorów za naruszenie RODO - GazetaPrawna.pl

# 02 Międzynarodowy Dzień Ochrony Danych Osobowych – firm nie stać na wyzwania związane z ochroną danych

- W obliczu Międzynarodowego Dnia Ochrony Danych Osobowych, obchodzonego 28 stycznia, nowe badania ISACA (Stowarzyszenie do spraw audytu i kontroli systemów informatycznych) ujawniają znaczące wyzwania, związane ze skuteczną ochroną danych osobowych, do których należą:
  - Niedofinansowanie i braki kadrowe: W Europie aż 41% specjalistów ds. ochrony danych zgłasza niedofinansowanie swoich działów. Co więcej, 56% oczekuje dalszych cięć budżetowych. Ta sytuacja tworzy paradoks, gdzie pomimo rosnącej potrzeby ochrony danych, zasoby finansowe i ludzkie są redukowane.
  - Wyzwania rekrutacyjne: Dwie piąte firm boryka się z utrzymaniem wykwalifikowanych specjalistów. Brak personelu jest odczuwalny, a 53% organizacji przyznaje, że ich zespoły ds. ochrony danych technicznych są niedostatecznie obsadzone.
  - Widmo cyberzagrożeń: Redukcja budżetów i brak umiejętności w obliczu zaawansowanego krajobrazu cybernetycznego może mieć katastrofalne skutki. Warto zauważyć przy tym, że w erze cyfrowej ryzyko naruszeń wciąż rośnie, wraz z przyrostem danych oraz stopniem wykorzystania zaawansowanych technologii przez hakerów.
  - Szkolenia i świadomość: Pomimo wyzwań, 68% specjalistów zgłasza, że ich firmy oferują coroczne szkolenia z zakresu prywatności. Taki wysiłek ma pozytywny wpływ na świadomość prywatności wśród pracowników, co jest kluczowe w budowaniu kultury bezpieczeństwa danych.
  - Luka kwalifikacyjna: Firmy wciąż zmagań się z luką kwalifikacyjną. Braki wiedzy dotyczą przede wszystkim technologii, wiedzy technicznej oraz operacyjnej IT. Ta sytuacja podkreśla potrzebę ciągłego rozwoju umiejętności i adaptacji do szybko zmieniających się technologii.
  - Działania naprawcze: Organizacje podejmują inicjatywy, aby zmniejszyć deficyt umiejętności, w tym szkolenia i korzystanie z usług zewnętrznych. Kluczowe jest zapewnienie odpowiednich zasobów i ustalanie priorytetów w celu skutecznej ochrony danych.



Źródło: Międzynarodowy Dzień Ochrony Danych Osobowych - firm nie stać na wyzwania związane z ochroną danych - Brandsit

# 03 Rosyjscy hackerzy zaatakowali pocztę HP i Microsoftu

- Firma Hewlett Packard Enterprise (HPE) ujawniła, że grupa rosyjskich hackerów znana jako APT29 lub Midnight Blizzard uzyskała dostęp do skrzynek pocztowych pracowników z kilku jej wydziałów, w tym do poczty działu cyberbezpieczeństwa.
- Dnia 12 grudnia 2023 HPE dowiedziała się o podejrzanym działaniu grupy Midnight Blizzard. Początkowo wiedziano, że hackerzy uzyskali dostęp do chmury z systemem pocztowym. Atakujący mogli uzyskać dostęp do danych z małego odsetka skrzynek HPE, które były używane przez osoby z działu cyberbezpieczeństwa i segmentów biznesowych. Ustalono, że atak zaczął się w maju 2023 r. i doszło do wyprowadzenia tych danych poza firmę. Jak dotąd nic nie wskazuje na to, aby atak mógł wywrzeć duży wpływ na działania firmy lub jej finanse.
- Z kolei Microsoft oświadczył, że 12 stycznia tego roku doszło do wykrycia ataku na jego systemy korporacyjne. Firma zdecydowała się na ujawnienie tego faktu, bo zobowiązała się do większej transparentności w ramach akcji Secure Future Initiative.
- Atak na Microsoft zaczął się w listopadzie 2023. Atakujący użyli techniki password spraying, czyli sprawdzali możliwość zalogowania się pewnymi przewidywalnymi hasłami na wielu kontach. Udało im się dostać na stare konto nie używane już na produkcji. Wynikające z tego uprawnienia zostały wykorzystane, by uzyskać dostęp do "małego odsetka kont mailowych" używanych przez: kierowników, pracowników działu cyberbezpieczeństwa i pracowników działu prawnego. Pobrano niektóre wiadomości i załączniki. Co ciekawe, Midnight Blizzard najprawdopodobniej szukał w Microsofcie informacji o sobie samym (tzn. co Microsoft może wiedzieć na temat grupy).
- Atakujący nie uzyskali dostępu do danych klientów, systemów produkcyjnych, kodu źródłowego czy systemów AI. Wiadomo, że atak nie był wynikiem żadnej słabości w produktach czy usługach Microsoftu.

Źródło: » Rosyjscy hackerzy zaatakowali pocztę HP i Microsoftu -- Niebezpiecznik.pl --

# 04 Oddział Amazon we Francji ukarany karą w wysokości 32 milionów euro za nadmierne monitorowanie produktywności pracowników

- Grzywna wymierzona przez francuski organ ochrony danych (CNIL) została nałożona na Amazon France Logistique za wielokrotne zasady minimalizacji danych i niezgodne z prawem przetwarzanie nagrań monitoringu wideo. Amazon stwierdził w oświadczeniu, że "zdecydowanie nie zgadza się" z ustaleniami CNIL i zastrzega sobie prawo do odwołania.
- Każdy pracownik magazynu Amazon otrzymuje skaner do dokumentowania wykonywania określonych zadań przypisanych mu w czasie rzeczywistym (składowanie lub zdejmowanie towaru z półek, odkładanie lub pakowanie itp.). Każde skanowanie skutkuje rejestracją danych, które są przechowywane i wykorzystywane do wyliczania wskaźników dostarczających informacji o jakości, produktywności i okresach bezczynności danego pracownika.
- Odpowiadając na doniesienia medialne i skargi pracowników, CNIL poinformowało, że przeprowadziło wiele dochodzeń we francuskich magazynach Amazona. Zakwestionowano elementy praktyki Amazon dotyczące monitorowania wydajności pracy za pomocą skanera, a w tym:
    - System wymagający od pracowników uzasadnienia każdej przerwy w pracy;
    - Wykorzystywanie systemu do pomiaru produktywności;
    - Nadmiarowe przechowywanie przez Amazon pozyskanych danych;
    - Niedopełnienie obowiązku informacyjnego wobec pracowników;
    - Dostęp do nagrań z monitoringu wizyjnego "nie był wystarczająco zabezpieczony".

Źródło: Jednostka Amazon ukarana grzywną w wysokości 35 mln USD na mocy RODO za śledzenie produktywności pracowników | Krótki opis wiadomości | Tydzień Zgodności (complianceweek.com)

# 05 EROD uruchamia narzędzie do audytu stron internetowych

- EROD uruchomiła narzędzie do audytu stron internetowych, które może być wykorzystywane do oceny ich zgodności z prawem.
- Narzędzie zostało opracowane przez grupę ekspertów wspierających EROD i może być wykorzystywane zarówno przez audytorów prawnych i technicznych w organach ochrony danych, jak i przez administratorów i podmioty przetwarzające, którzy chcą przetestować własne strony internetowe.
- Nowe narzędzie pozwala na przygotowanie, przeprowadzenie audytów bezpośrednio w narzędziu poprzez zwykłą wizytę na danej stronie internetowej. Narzędzie to jest również kompatybilne z innymi narzędziami, takimi jak strona internetowa EIOD i umożliwia audytorom importowanie i ocenę wyników kontroli przeprowadzonych za pomocą tych narzędzi. Narzędzie może też generować raporty.
- Chociaż istnieje już kilka narzędzi do audytu stron internetowych, zwykle wymagają one wiedzy technicznej. W związku z tym EROD postanowiła opracować rozwiązanie, które jest łatwe w użyciu oraz służy ułatwieniu egzekwowania przepisów przez krajowe organy ochrony danych oraz administratorów stron internetowych.
- Narzędzie jest dostępne bezpłatnie do pobrania na stronie: https://code.europa.eu/edpb/website-auditing-tool/-/releases

Źródło: EROD uruchamia narzędzie do audytu stron internetowych | Europejska Rada Ochrony Danych (europa.eu)