
LEX ARTIST

RODO - aktualności

[29.07.2024]

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 Rozporządzenie DORA od 2025 r. Duże kary dla firm za brak dostosowania

02 Polacy mają dużą świadomość funkcjonowania Urzędu Ochrony Danych Osobowych

03 WSA: firma, która zleciła ochronę danych, nie odpowiada za ich kradzież

04 Pracodawcy chcą nowych wyjaśnień. Co z poradnikiem UODO?

01 Rozporządzenie DORA od 2025 r. Duże kary dla firm za brak dostosowania

- Rozporządzenie DORA (Unijne Rozporządzenie o operacyjnej odporności cyfrowej sektora finansowego) zawiera szereg artykułów poświęconych zagadnieniom kontroli i nadzoru, a także możliwości zastosowania kar administracyjnych i środków naprawczych.
- Środki te będą dotyczyć wszystkich podmiotów rynku finansowego, które mają obowiązek stosować przepisy DORA. Osobną kategorią kar zostaną objęci kluczowi zewnętrzni dostawcy usług ICT. W ich przypadku system nadzoru i kar jest nieodłącznym elementem tzw. ram nadzoru nad kluczowymi zewnętrznymi dostawcami usług ICT – jednego z kluczowych filarów DORA.
- Nad przestrzeganiem zasad zgodności z DORA będzie czuwać organ właściwy dla instytucji płatniczych, kredytowych czy ubezpieczycieli, czyli Komisja Nadzoru Finansowego. Wiadomo, że KNF będzie miał szerokie uprawnienia, jeśli chodzi o możliwość ustalenia potencjalnych naruszeń. Będzie on mógł m. in.: mieć dostęp do wszelkich dokumentów lub danych, które uzna za istotne z punktu widzenia wykonywania swoich obowiązków; przeprowadzać dochodzenia lub kontrole na miejscu, zastosować środki naprawcze w odniesieniu do naruszeń wymogów rozporządzenia DORA.
- Do zestawu narzędzi dostępnych KNF należeć więc będzie m. in. wydanie danemu podmiotowi nakazu zaprzestania działań naruszających rozporządzenie oraz aby powstrzymał się od ponownego podejmowania tego postępowania. Kolejnym jest zakaz pełnienia funkcji członka zarządu, rady nadzorczej albo innej funkcji kierowniczej osobie odpowiedzialnej za naruszenie przez okres od miesiąca do roku. Ostatecznym środkiem, jaki będzie mógł zastosować organ nadzoru w razie notorycznych naruszeń będą kary pieniężne. W przypadku osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej może być to nawet kwota 20 869 500 zł lub 10 proc. przychodów netto z ostatniego roku, a w przypadku osoby fizycznej nawet 3 042 410 zł.

Źródło: Rozporządzenie DORA od 2025 r. Skala zmian podobna do RODO. Duże kary dla firm za brak dostosowania - Infor.pl

02 Polacy mają dużą świadomość funkcjonowania Urzędu Ochrony Danych Osobowych

- W ramach badania Eurobarometr z 2024 r. na temat sprawiedliwości, praw i wartości zapytano respondentów m.in. o ich świadomość na temat istnienia krajowych organów odpowiedzialnych za ochronę danych osobowych. Pod tym względem Polska znalazła się w czołówce państw Unii – aż 75% respondentów zadeklarowało, że słyszało o takiej instytucji. Równie dobry wynik odnotowano w Czechach, Słowenii (75%) oraz Portugalii (74 %). Na pierwszym miejscu uplasowały się Niderlandy z wynikiem 82%.
- Komunikat przedstawiony przez KE, jest streszczeniem najważniejszych wniosków ze sprawozdania na temat stosowania RODO, które w całości zostanie opublikowane w późniejszym terminie. Jest to już drugie sprawozdanie Komisji przyjęte zgodnie z art. 97 RODO (pierwsze przyjęto w dniu 24 czerwca 2020 r.).
- Sprawozdanie zostało opracowane w oparciu o wiele źródeł m.in. stanowiska i ustalenia Rady Unii Europejskiej, uwagi zgłaszane w drodze publicznego zaproszenia oraz informacje otrzymane od organów ochrony danych (wkład Europejskiej Rady Ochrony Danych).
- Wśród podstawowych wniosków płynących ze sprawozdania wymieniono wzmocnienie pozycji obywateli oraz stworzenie warunków działania dla przedsiębiorstw, napędzających transformację cyfrową w UE. Autorzy dokumentu wskazali jednak, że pełne osiągnięcie dwóch celów RODO – tj. silnej ochrony osób fizycznych przy jednoczesnym zapewnieniu swobodnego przepływu danych osobowych w UE oraz bezpiecznego przepływu danych poza UE – wciąż wymaga dalszych działań.

Źródło: Aktualności – UODO; https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=COM:2024:357:FIN

03 WSA: Firma, która zleciła ochronę danych, nie odpowiada za ich kradzież

- Firma, która zapłaciła za to, by administrowane przez nią dane osobowe były właściwie chronione, nie może odpowiadać za ich wyciek w konsekwencji ataku hackerskiego - orzekł w czwartek Wojewódzki Sąd Administracyjny w Warszawie.
- Sprawa rozstrzygnięta w czwartek przez Wojewódzki Sąd Administracyjny dotyczyła odpowiedzialności za wyciek danych, do którego doszło wskutek ataku hackerskiego na przedsiębiorstwo zajmujące się obsługą płacową. Do prezesa Urzędu Ochrony Danych Osobowych (PUODO) wpłynęła skarga podmiotu, którego dane zostały zaszyfrowane i wykradzione. Karę — upomnienie — za wyciek prezes UODO nałożył jednak na firmę będącą klientem zaatakowanego przedsiębiorstwa.
- Jak wyjaśnia Anna Dobiecka — prawniczka z kancelarii Barta Litwiński reprezentującej ukaraną firmę — PUODO uznał bowiem, że to ukarana firma, jako administrator udostępniła dane podmiotowi nieuprawnionemu, czyli hakerowi; tym samym to ona przetwarzała je bez podstawy prawnej, naruszając zasadę legalności.
- Decyzję PUODO uchylił sąd. WSA w większości zgodził się z zarzutami. Podkreślił, że PUODO w swojej decyzji nie wyjaśnił, z czego wywodził, że miało miejsce udostępnienie danych. Sąd uznał, że ich udostępnienie, czyli w istocie przetwarzanie, według przepisów RODO zakłada pewną aktywność po stronie administratora. W przypadku, w którym doszło do ataku hackerskiego nie da się mówić o jakiejkolwiek operacji przetwarzania po stronie naszego klienta, a tym samym o naruszeniu przez niego zasady legalności — tłumaczy Anna Dobiecka.
- Prawniczka precyzuje, że na mocy wyroku sądu PUODO powinien jeszcze raz przeanalizować, czy możliwe jest ukaranie firmy korzystającej z usług zaatakowanego przedsiębiorstwa. Dla przedsiębiorstwa tego – jeśli decyzja prezesa by się uprawomocniła – oznacza to bowiem ryzyko żądania odszkodowania od podmiotu, którego dane wyciekły.

Źródło: Dane wyciekły przez hakera. Kto odpowiada za wyciek danych osobowych w firmie? - rp.pl; *Sygn. akt: II SA/Wa 2430/23*

04 Pracodawcy chcą nowych wyjaśnień. Co z poradnikiem UODO?

- Urząd Ochrony Danych Osobowych zakończył już zbieranie uwag do swojego poradnika dla pracodawców dotyczącego ochrony danych osobowych w miejscu pracy i obecnie trwa ich analiza. Jak dowiedział się DGP, uwag wpłynęło bardzo dużo. Zgłosiło je ponad 40 podmiotów, z czego każdy z nich od kilku do kilkudziesięciu.
- Jednym z zagadnień, które od lat budzą wątpliwości w praktyce, i które – zdaniem komentujących – teraz powinny być wreszcie rozwiane na łamach poradnika, jest kwestia przetwarzania danych osobowych osób trzecich, czyli np. członków rodziny pracownika. Sytuacji, w których trafiają one do pracodawcy, jest wiele. Ma to miejsce w przypadku składania wniosków np. o świadczenia z zakładowego funduszu świadczeń socjalnych (ZFŚS), o opiekę nad dzieckiem do 14. roku życia, o elastyczną organizację pracy czy o urlop opiekuńczy.
- Problem dotyczy zwłaszcza tego, czy wobec tych osób pracodawca powinien realizować obowiązek informacyjny (czyli powiadomić osobę zainteresowaną o przetwarzaniu jej danych osobowych). W dotychczasowym poradniku UODO wskazywał, że nie ma takiego obowiązku, gdy dane członków rodziny są zbierane na potrzeby ZFŚS. Brakuje natomiast takiego stwierdzenia wobec innych przypadków przetwarzania danych os. trzecich.
- Eksperci domagają się także liberalizacji stanowiska UODO w sprawie tzw. background screening czy pre-employment screening. W jej ramach sprawdzana jest przeszłość kandydata do pracy bądź pracownika, np. gdy aplikuje na wyższe stanowisko. W podstawowej wersji obejmuje weryfikację życiorysu zawodowego, czyli poprzedniego zatrudnienia, wykształcenia, uzyskanych certyfikatów i referencji. W zaawansowanej – również np. badanie historii kryminalnej i kredytowej, a także wpisów w mediach społecznościowych.
- Z poradnika UODO wynika obecnie, że rekrutujący nie może kontaktować się z podmiotem, który wystawił referencje. Z kolei dane dotyczące karalności pracodawca może przetwarzać tylko wtedy, gdy wynika to wprost z przepisów prawa.

Źródło: Pracodawcy chcą nowych wyjaśnień. Co z poradnikiem UODO? - GazetaPrawna.pl