

Kary organów nadzorczych w Unii Europejskiej



Kraj oraz organ nadzorczy

Francja

French Data Protection Authority (CNIL)



Data wydania decyzji

10 listopad 2022 r.



Podmiot kontrolowany

DISCORD INC.



Wysokość kary

800 000 EUR

FORSAFE
BEZPIECZENSTWO PONAD WSZYSTKO



Rodzaj naruszenia

Art. 5 (1) e) RODO, Art. 13 RODO, Art. 25 (2) RODO, Art. 32 RODO, Art. 35 RODO.
Nieprzestrzeganie ogólnych zasad przetwarzania danych.



Przedmiot decyzji

Źródło postępowania:

Francuski organ nadzorczy dokonał czynności kontrolnych w DISCORD INC. (DISCORD), Frima ta oferuje oprogramowanie Voice over IP, umożliwiające komunikowanie z osobami o podobnych zainteresowaniach.

Opis wydarzeń:

1) Przedmiotem kontroli była weryfikacja oprogramowania dostępnego z poziomu przeglądarki internetowej oraz możliwego do zainstalowania jako aplikacja na urządzeniu.

2) W trakcie czynności kontrolnych francuski organ nadzorczy dopatrzył się następujących naruszeń:

a) zasada przejrzystości – polityka prywatności była dostępna jedynie w języku angielskim,

b) zasada przejrzystości – obowiązek informacyjny dla użytkowników nie zawierał precyzyjnego wyjaśnienia okresów przechowywania danych osobowych,

c) zasada ograniczenia przechowywania – DISCORD nie opracował polityki retencji danych, a rejestr czynności przetwarzania nie zawierał okresów przechowywania danych osobowych; na dzień kontroli w bazie danych DISCORD znajdowało się 2 474 000 kont francuskich użytkowników, którzy nie korzystali ze swojego konta przez ponad trzy lata oraz 58 000 kont, które nie były używane przez ponad pięć lat,

d) domyślna ochrona danych – użytkownik musi wykonać kilka czynności, aby zamknąć aplikację DISCORD, gdyż aplikacja jest tak skonfigurowana, że wybranie ikony „X” nie zamyka aplikacji, a jedynie ją minimalizuje. W związku z tym aplikacja pozostaje cały czas aktywna, a tym samym dane osobowe użytkownika mogą być przekazywane osobom trzecim bez jego wiedzy,

e) bezpieczeństwo przetwarzania – hasło do konta DISCORD składało się z sześciu znaków, w tym liter i cyfr,

f) brak przeprowadzenia oceny skutków dla ochrony danych.

3) Na dzień wydania decyzji część naruszeń została skorygowana:

a) udostępniono politykę prywatności w języku francuskim,

b) opracowano politykę retencji danych,

c) opracowano obowiązek informacyjny zawierający precyzyjne określenie okresów przechowywania danych osobowych,

d) wdrożono wyskakujące okienko, które po zamknięciu okna aplikacji po raz pierwszy powiadomi użytkownika, że aplikacja DISCORD jest nadal aktywna,

e) dokonano zmian w zakresie długości i złożoności hasła.

Przyczyna naruszenia:

DISCORD nie dopełnił obowiązku realizacji podstawowych zasad ochrony danych osobowych.

Decyzja:

Kara pieniężna w wysokości 800 000 EUR.

Źródło:

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046562676?init=true&page=1&query=discord%20inc&searchField=ALL&tab_selection=all



Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

1) Opracuj politykę prywatności i obowiązek informacyjny, które w sposób jasny i precyzyjny będą informowały osoby, których dane dotyczą, o przetwarzaniu ich danych osobowych. Staraj się używać prostego języka, unikać zdań i skomplikowanych struktur językowych. Istotne jest również to, aby cele i podstawa prawna przetwarzania danych osobowych były łatwe do zrozumienia. Nie zapomnij o tym, że dokumentu muszą być przetłumaczone na język używany przez użytkowników strony internetowej.

2) Opracuj i wdróż procedurę retencji danych oraz regularnie weryfikuj procesy przetwarzania danych osobowych w aspekcie czasu przetwarzania danych osobowych.

3) Opracuj politykę uwzględniającą używanie skomplikowanych i silnych haseł dostępu.

4) Wykonaj ocenę skutków dla ochrony danych, gdy:

a) przetwarzanie danych osobowych z dużym prawdopodobieństwem może powodować wysokie naruszenie praw lub wolności osób fizycznych,

b) przetwarzanie danych osobowych opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu,

c) dane osobowe szczególnej kategorii oraz dane dotyczące wyroków sądowych i czynów zabronionych są przetwarzane na dużą skalę,

d) operacje przetwarzania danych osobowych zawarte są w wykazie upublicznionym przez organ nadzorczy.

