

Kary organów nadzorczych w Unii Europejskiej



Kraj oraz organ nadzorczy

Francja

French Data Protection Authority (CNIL)



Data wydania decyzji

04 listopad 2021 r.



Podmiot kontrolowany

Régie Autonome des Transports Parisiens



Wysokość kary

400 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO



Rodzaj naruszenia

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



Przedmiot decyzji

Źródło postępowania:

Francuski organ nadzorczy otrzymał od związku zawodowego skargę na Régie Autonome des Transports Parisiens (RATP). Odnosiła się ona do uwzględniania liczby dni strajkowych w dokumentach służących do przygotowania decyzji o awansie zawodowym.

Opis wydarzeń:

1) RATP w tym czasie dokonał również zgłoszenia naruszenia ochrony danych osobowych, które polegało na wykorzystywaniu przez komisję oceniającą awans zawodowy pliku niezgodnego z RODO, co skutkowało utratą poufności danych osobowych.

2) RATP w zgłoszeniu wskazał, iż naruszenie trwało od 9 kwietnia do 11 maja 2020 r. i obejmowało 16 000 osób.

3) W związku z powyższym francuski organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w RATP celem rozpatrzenia przedmiotowej sprawy.

4) Na podstawie zebranego materiału dowodowego francuski organ nadzorczy dopatrył się naruszenia:

a) zasady minimalizacji przetwarzania danych osobowych – komisja oceniająca awans zawodowy przetwarzała dane dotyczące przyczyny nieobecności w pracy, w tym informację o ilość dni, w których osoba strajkowała,

b) zasady ograniczenia przechowywania danych osobowych – dane dotyczące oceny awansu zawodowego były przechowywane w systemie informatycznym po ustaniu celu przetwarzania tych danych,

c) bezpieczeństwa danych osobowych – RATP nie dokonał rozróżnia poziomów uprawnień pracowników, umożliwiając im dostęp do szerszego zakresu danych niż to konieczne.

Przyczyna naruszenia:

RATP nie dopełniło obowiązku wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poziomu ochrony odpowiedniego do ryzyka.

Decyzja:

Kara pieniężna w wysokości 400 000 EUR.

Źródło:

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044286815?init=true&page=1&query=san-2021-019&searchField=ALL&tab_selection=all



Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

1) Dokonując wyboru odpowiednich środków technicznych i organizacyjnych pamiętaj, że jest to proces dwuetapowy. W pierwszej kolejności ważne jest, aby określić poziom ryzyka, jaki wiąże się z przetwarzaniem danych osobowych. Dopiero po wykonaniu tej czynności możemy ustalić, jakie środki techniczne i organizacyjne będą odpowiednie, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

2) Weryfikuj procesy przetwarzania danych osobowych pod kątem realizacji zasady minimalizacji przetwarzania danych osobowych.

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

4) Nadając uprawnienia dostępu do danych osobowych w systemie informatycznym pamiętaj, aby były one skorelowane z zakresem obowiązków przypisanym do danego stanowiska.

