Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy — **Francja**
French Data Protection Authority (CNIL)

Data wydania decyzji — **14 czerwca 2021 r.**

Podmiot kontrolowany — **BRICO PRIVÉ**

Wysokość kary — **500 000 EUR**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie art. 5 (1) e) , art. 13, art. 17, art. 32 RODO.
Nieprzestrzeganie ogólnych zasad przetwarzania danych.

Przedmiot decyzji

Źródło postępowania:

Francuski organ nadzorczy dokonał czynności kontrolnych w BRICO PRIVÉ (BRICO), który sprzedaje artykuły związane z majsterkowaniem, ogrodnictwem i wyposażeniem domu.

Opis wydarzeń:

1) Przedmiotem kontroli była weryfikacja przestrzegania przez BRICO zasad ochrony danych osobowych w szczególności wobec klientów i potencjalnych klientów.

2) Na podstawie zebranego materiału dowodowego francuski organ nadzorczy ustalił, iż BRICO dopuścił się następujących naruszeń:

a) naruszenie zasady ograniczenia przechowywania – BRICO nie wdrożył procedury retencji danych i przechowywał dane klientów i potencjalnych klientów bez ograniczenia czasowego; BRICO przechowywał dane ponad 16 000 klientów, którzy nie złożyli zamówienia w ciągu ostatnich pięciu lat oraz dane ponad 130 000 osób, które nie logowały się na swoje konta klientów przez pięć lat,

b) naruszenie zasady przejrzystości przetwarzania – obowiązek informacyjny opublikowany w sklepie internetowym nie zawierał informacji o danych kontaktowych inspektora ochrony danych, okresach przechowywania, podstawach prawnych przetwarzania i prawach, które przysługują użytkownikom,

c) brak respektowania prawa do usunięcia danych – BRICO na żądanie użytkownika nie usuwało jego konta a jedynie dokonywało dezaktywacji,

d) brak zapewnienia adekwatnego poziomu bezpieczeństwa:

- uwierzytelnianie przy zakładaniu konta w sklepie internetowym opierało się na haśle składającym się tylko z sześciu cyfr,
- uwierzytelnianie pracowników w bazach danych opierało się na haśle składającym się tylko z ośmiu znaków,
- pracownicy przechowywali hasła dostępowe w postaci zwykłego tekstu, w pliku tekstowym znajdującym się na komputerze firmowym,
- pracownicy wykorzystywali przestarzałą funkcję skrótu używaną do przechowywania haseł użytkowników sklepu internetowego będących pracownikami,
- pracownicy posiadali dostęp do kopii produkcyjnej bazy danych BRICO za pośrednictwem wspólnego konta dla czterech osób,

e) naruszenie zasady przejrzystości – BRICO nie informował użytkowników sklepu internetowego o plikach cookie oraz nie uzyskał od nich zgody na wykorzystywanie danych przez nie zbieranych,

f) brak pozyskania zgody na realizację działań marketingowych – BRICO wysyłał informacje handlowe osobom, które nie zgodziły się na ich otrzymywanie.

3) Ostatecznie BRICO usunęło uchybienia opisane w pkt. 2 a), b), c), d).

Przyczyna naruszenia:

Niedopełnienie podstawowych obowiązków w zakresie przestrzegania zasad ochrony danych osobowych przez BRICO.

Decyzja French Data Protection Authority (CNIL)

1) Kara pieniężna w wysokości 500 000 EUR, w tym:

a) 300 000 EUR za naruszenie zasady ograniczenia przechowywania, naruszenie zasady przejrzystości przetwarzania, brak respektowania prawa do usunięcia danych, brak zapewnienia adekwatnego poziomu bezpieczeństwa,

b) 200 000 EUR za brak pozyskiwania zgody na realizację działań marketingowych.

2) Nakaz:

a) wdrożenia polityki okresów retencji danych osobowych,

b) zaprzestania przechowywania danych osobowych byłych klientów strony internetowej firmy po upływie ustalonego okresu nieaktywności,

c) uszczegółowienia procedury archiwizacji danych osobowych klientów,

d) zaprzestania poszukiwania osób niebędących klientami, które nie wyraziły na to zgody.

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

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

2) Przechowuj dane osobowe w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

3) Opracuj i wdróż procedury realizacji praw podmiotów danych.

4) 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.

5) 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.

6) Zgodnie z rekomendacjami francuskiego organu nadzorczego zalecane jest stosowanie hasła zawierającego co najmniej dwanaście znaków (zawierające co najmniej jedną wielką literę, jedną małą literę, jedną cyfrę i jeden znak specjalny) lub co najmniej osiem znaków (zawierające trzy z tych czterech kategorii znaków) jeśli został uwzględniony dodatkowy środek, taki jak np. opóźnianie dostępu do konta po kilku awariach, wdrożenie mechanizmu zabezpieczającego przed automatycznym i intensywnym przesyłaniem próby i/lub zablokowanie konta po kilku nieudanych próbach uwierzytelnienia.

7) Jeśli na swojej stronie internetowej wykorzystujesz pliki cookie lub inne pliki śledzące, pamiętaj o poinformowaniu o tym użytkownika oraz daj mu możliwość wyboru w zakresie wyrażenia na nie zgody.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak