Kary organów nadzorczych w Unii Europejskiej

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

Data wydania decyzji **18.11.2020 r.**

Podmiot kontrolowany **Carrefour France**

Wysokość kary **2 250 000 EUR**

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Naruszenie Art. 5, Art. 12, Art. 13, Art. 15, Art. 17, Art. 21, Art. 32, Art. 33 RODO.
Nieprzestrzeganie ogólnych zasad przetwarzania danych.

Przedmiot decyzji

Źródło postępowania:

1) Francuski organ nadzorczy od czerwca 2018 r. do kwietnia 2019 r. otrzymał 15 skarg od klientów dotyczących spółek z grupy CARREFOUR.

2) 7 skarg dotyczyło działań handlowych pomimo wyrażenia sprzeciwu wobec przetwarzania danych osobowych.

3) 4 skargi odnosiły się do złożonych wniosków o usunięcie danych, które nie zostały rozpatrzone.

4) 3 skargi wskazywały na brak odpowiedzi na wnioski o dostęp do danych osobowych.

5) 1 skarga dotyczyła rezygnacji z otrzymywania wiadomości e-mailowych, która nie została rozpatrzona.

Opis wydarzeń:

1) Francuski organ nadzorczy w związku z otrzymanymi skargami od kwietnia do czerwca 2019 r. prowadził w CARREFOUR FRANCE czynności kontrolne.

2) Kontrola ujawniła kilka naruszeń przepisów o ochronie danych.

3) Po pierwsze, nie dopełniono obowiązku przechowywania danych osobowych przez okres nie dłuższy niż jest to niezbędne do celów, w których są przetwarzane. Dane klientów będących członkami programu lojalnościowego oraz użytkowników serwisu carrefour.fr były przechowywane w bazie danych przez cztery lata od ich ostatniej aktywności. Na dzień kontroli w bazie danych było ponad 28 milionów klientów, którzy byli członkami programu lojalnościowego oraz byli nieaktywni przez pięć do dziesięciu lat. Wspomniana baza zawierała również dane ponad 750 000 użytkowników serwisu carrefour.fr, którzy ostatni zakup wykonali w okresie od 5 do 10 lat temu oraz 20 000 użytkowników, którzy ostatni zakup wykonali ponad 10 lat temu.

4) Po drugie, Spółka wymagała, aby klienci przedkładali dokumenty tożsamości w celu potwierdzenia tożsamości przy rozpatrywaniu wniosków o realizację praw podmiotów danych. Wspomniane dokumenty były następnie przechowywane przez okres od roku do sześciu lat. Spółka nie dotrzymywała również określonego w RODO czasu udzielania odpowiedzi na wnioski o wykonanie praw podmiotów danych. Czas odpowiedzi na wnioski był różny i zdarzało się, że osoby czekały na odpowiedź nawet dziewięć miesięcy.

5) Po trzecie, informacje dotyczące danych osobowych przekazane przez Spółkę użytkownikom strony internetowej carrefour.fr oraz osobom pragnącym przystąpić do programu lojalnościowego nie były ani łatwo dostępne, ani zrozumiałe.

6) Po czwarte, powyższe informacje były również niekompletne, gdyż Spółka na stronie internetowej carrefour.fr nieprawidłowo zidentyfikowała administratora, nie wskazała podstawy prawnej przetwarzania danych osobowych, nie udzieliła pełnej informacji dotyczącej przekazywania danych do krajów spoza UE oraz czasu przechowywania danych.

7) Po piąte, Spółka nie respektowała prawa dostępu do danych, prawa do usunięcia danych oraz prawa do sprzeciwu przeciwko przetwarzania danych osobowych.

8) Po szóste, Spółka wysyłała informacje handlowe osobom, które nie zgodziły się na otrzymywanie reklam przez SMS lub e-mail.

9) Po siódme, strona internetowa carrefour.fr posiadała lukę, która umożliwiała osobom postronnym dostęp do faktury zapisanej pod stałym adresem URL. Każdy, kto posiadał wskazany adres, mógł uzyskać dostęp do wystawionego dokumentu bez konieczności uwierzytelniania i łączenia się ze swoim kontem klienta.

10) Po ósme, Spółka nie zgłosiła naruszenia bezpieczeństwa danych osobowych, które miało miejsce w lipcu 2019 r. i polegało na ataku hakerskim. Atak ten, wykorzystując usługę uwierzytelniania aplikacji mobilnej grupy, przybrał formę 800 000 prób połączenia z 10 000 adresów IP. Zdarzenie to skutkowało 4000 udanymi uwierzytelnieniami i 275 skutecznymi dostępami do kont klientów.

11) Na koniec Spółka nie informowała użytkowników strony internetowej o plikach cookie oraz nie uzyskała od nich zgody na wykorzystywanie danych przez nie zbieranych.

Przyczyna naruszenia:

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

Decyzja French Data Protection Authority (CNIL):

1) Kara pieniężna w wysokości 2 250 000 euro.

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) Gdy otrzymasz wniosek o skorzystanie z praw podmiotów danych, dotrzymaj terminu odpowiedzi na pismo i nie przechowuj kopii dokumentu tożsamości.

5) 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, unikaj wielokrotnie złożonych zdań i skomplikowanych struktur językowych. Istotne jest również to, aby cele i podstawa prawna przetwarzania danych osobowych były łatwe do zrozumienia.

6) Opracuj i wdróż procedurę zarządzania listami rezygnacji z kampanii marketingowych (tzw. „czarna lista") oraz dokonuj ich cyklicznej weryfikacji.

7) Opracuj i wdróż procedurę zgłaszania naruszeń bezpieczeństwa danych osobowych, które będą uwzględniały kwestie związane ze sprawnym i szybkim stwierdzeniem naruszenia ochrony danych.

8) Wykonaj ocenę naruszenia ochrony danych osobowych pod kątem wystąpienia ryzyka dla praw i wolności osób fizycznych. Dokonując oceny weź pod uwagę:

a) konkretne okoliczności naruszenia, w tym wagę potencjalnego wpływu i prawdopodobieństwo jego wystąpienia,

b) czy naruszenie może prowadzić do uszczerbku fizycznego, albo szkód majątkowych lub niemajątkowych dla osób, których dane zostały naruszone. Przykładami takich szkód są: utrata kontroli nad własnymi danymi osobowymi, nieuprawnione odwrócenie pseudonimizacji, dyskryminacja, kradzież lub sfałszowanie tożsamości, straty finansowe, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.

9) Gdy ocenisz, że naruszenie ochrony danych osobowych może powodować ryzyko dla naruszenia praw lub wolności osób fizycznych, dokonaj zgłoszenia naruszenia ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych. Na zgłoszenie masz 72 godziny od momentu stwierdzenia naruszenia.

10) Jeśli masz wątpliwości co do oceny ryzyka dla naruszenia praw lub wolności osób fizycznych, dokonaj zgłoszenia naruszenia bezpieczeństwa danych osobowych, nawet jeśli taka ostrożność mogłaby się okazać nadmierna.

11) 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.

12) Regularnie testuj, mierz i oceniaj skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

13) 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