

Kary organów nadzorczych w Unii Europejskiej



Kraj oraz organ nadzorczy

Norwegia

Norwegian Supervisory Authority (Datatilsynet)



Data wydania decyzji

18 października 2021 r.



Podmiot kontrolowany

Østre Toten Municipality



Wysokość kary

412 000 EUR

FORSAFE
BEZPIECZENSTWO PONAD WSZYSTKO



Rodzaj naruszenia

Naruszenie art. 5 (1) f) RODO, Art. 32 RODO
Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.



Przedmiot decyzji

Źródło postępowania:

Østre Toten Municipality (Gmina) dokonał zgłoszenia do norweskiego organu nadzorczego w związku z przeprowadzonym atakiem ransomware. W jego wyniku dane Gminy zostały zaszyfrowane, a kopie zapasowe zostały usunięte.

Opis wydarzeń:

- 1) W związku z otrzymanym zgłoszeniem norweski organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w Gminie.
- 2) W trakcie czynności kontrolnych norweski organ nadzorczy ustalił, iż:
 - a) Gmina zmagala się z awarią sprzętu,
 - b) cyberprzestępca uzyskał dostęp do infrastruktury Gminy najprawdopodobniej za pośrednictwem zdalnego dostępu lub socjotechniki,
 - c) Gmina utraciła dostęp do systemów informatycznych i kopii zapasowych,
 - d) w wyniku ataku ransomware pobrano ok. 30 000 dokumentów, które zawierały takie informacje jak: pochodzenie etniczne, poglądy polityczne, przekonania religijne, przynależność związkowa, orientacja seksualna, stan zdrowia, data urodzenia a także dane bankowe mieszkańców i pracowników Gminy,
 - e) dane zdobyte podczas ataku zostały opublikowane w dark webie.
- 3) Na podstawie zebranego materiału dowodowego norweski organ nadzorczy dopatrywał się następujących uchybień:
 - a) brak dwuskładnikowego uwierzytelniania przy logowaniu,
 - b) brak odpowiednio zabezpieczonych systemów tworzenia kopii zapasowych,
 - c) brak rejestrowania ważnych zdarzeń w sieci,
 - d) brak scentralizowanego logowania zdarzeń,
 - e) brak odpowiednio skonfigurowanej zapory sieciowej,
 - f) brak dostatecznie dobrze skonfigurowanych serwerów,
 - g) niedociągnięcia w zakresie kontroli wewnętrznej.

Przyczyna naruszenia:

Poważne uchybienia w zakresie bezpieczeństwa i nadzoru nad bezpieczeństwem danych osobowych.

Decyzja:

Kara pieniężna w wysokości 412 000 EUR (4 000 000 NOK).

Źródło:

<https://www.datatilsynet.no/contentassets/4609027cf9504e9aa12c3f05b45bdcf7/varsel-om-vedtak-om-overtredelsesgebyr-og-palegg.pdf>



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) Dokonaj wdrożenia mechanizmu dwuetapowego uwierzytelniania do aplikacji i programów dostępnych z poziomu Internetu, w których przetwarzane są dane osobowe.
- 3) Dokonuj regularnych pomiarów i testów istniejących zabezpieczeń organizacyjnych i technicznych, w szczególności dotyczących poufności, integralności i dostępności, a także możliwości odtwarzania danych po potencjalnej awarii.

Materiał edukacyjny
przygotowany przez FORSAFE



Opracowanie merytoryczne
Katarzyna Cieślak

