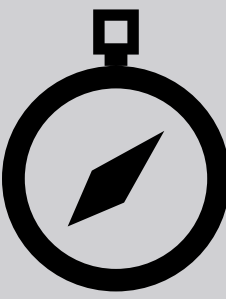


Kary organów nadzorczych w Unii Europejskiej

	Kraj oraz organ nadzorczy	Francja French Data Protection Authority (CNIL)
	Data wydania decyzji	15 kwietnia 2022 r.
	Podmiot kontrolowany	DEDALUS BIOLOGIE
	Wysokość kary	1 500 000 EUR
		

	Rodzaj naruszenia Naruszenie art. 28, art. 29 , art. 32 RODO Niewystarczające środki techniczne i organizacyjne zapewniające bezpieczeństwo informacji.
	Przedmiot decyzji <u>Źródło postępowania:</u> Francuski organ nadzorczy w związku z doniesieniami medialnymi, które odnosiły się do udostępnienia w internecie linku do pobrania pliku zawierającego dane medyczno-administracyjne francuskich pacjentów skradzionych z laboratoriów, dokonał czynności kontrolnych w DEDALUS BIOLOGIE (DEDALUS) – podmiocie, który sprzedaje oprogramowanie dla laboratoriów analiz medycznych. <u>Opis wydarzeń:</u> 1) W trakcie czynności kontrolnych francuski organ nadzorczy ustalił, iż DEDALUS pomimo wcześniejszych zgłoszeń dotyczących problemów z bezpieczeństwem, nie podjął stosownych kroków mających na celu jego poprawę. 2) Powyższe postępowanie sprawiło, że nieupoważnione osoby trzecie miały dostęp do danych medyczno-administracyjnych pacjentów laboratoriów. 3) W wyniku ataku hakerskiego wyciekły dane osobowe najprawdopodobniej ok 500 000 osób. 4) Wykradzione dane obejmowały następujące informacje: a) dane identyfikacyjne: numer PESEL, nazwisko, imiona, płeć, adres pocztowy, numer telefonu, adres e-mail, data ostatniej wizyty lekarskiej, data urodzenia, b) dane dotyczące patologii pacjentów (HIV, nowotwory, choroby genetyczne), stanu ciąży, stosowanych przez pacjentów terapii lekowych oraz danych genetycznych, c) dane identyfikacyjne lekarza przepisującego lek: nazwisko, imię, adres pocztowy, numer telefonu, adres e-mail, d) dane dotyczące próbnika: nazwisko, imię, adres, numer telefonu, e) dane dotyczące ubezpieczenia: numer ubezpieczenia, f) dane uwierzytelniające pacjentów: identyfikator i hasło. 5) Na podstawie zebranego materiału dowodowego francuski organ nadzorczy dopatrył się następujących naruszeń: a) umowy zawarte między DEDALUS a jego klientami nie zawierają zapisów o ochronie danych osobowych spełniających wymogi określone w art. 28 RODO, b) DEDALUS w związku z migracją danych między systemami pozyskiwał większą ilość danych niż było to wymagane współpracą z laboratoriami, c) DEDALUS nie wdrożył odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa danych osobowych, gdyż: - nie wdrożono procedury dla operacji migracji danych, - dane osobowe przechowywane na serwerze FTP MEGABUS nie były zaszyfrowane, - dane osobowe po migracji do innego oprogramowania nie były automatycznie usuwane, - nie zastosowano uwierzytelnienia wymaganego do dostępu przez Internet do strefy publicznej serwera FTP MEGABUS, - kilku pracowników korzystało ze współdzielonych kont użytkowników w odniesieniu do strefy prywatnej serwera FTP MEGABUS, - nie zastosowano nadzoru i raportowania alertów bezpieczeństwa na serwerze.
	<u>Przyczyna naruszenia:</u> DEDALUS nie wdrożył odpowiednich środków technicznych i organizacyjnych, co doprowadziło do wycieku danych osobowych.
	<u>Decyzja Dutch Supervisory Authority for Data Protection (AP):</u> Kara pieniężna w wysokości 1 500 000 EUR.

	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) Wykonaj wdrożenie procedur i systemu powiadamiania o zdarzeniach niepożądanych, w tym monitorowanie ruchu sieciowego. 3) Wykonuj regularne testowanie, mierzenie i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych osobowych. 4) Wykonuj testy podatności systemów informatycznych i aplikacji.
--	---

