



Co powinien zrobić gabinet korzystający z systemu MyDr? Kolejność czynności, terminy, wzory pism i formularze

Przewodnik Naczelnej Izby Lekarskiej dla lekarzy i podmiotów leczniczych występujących w roli administratora danych osobowych. Materiał zawiera również wytyczne dla pacjentów.

Poniższy przewodnik obejmuje wyłącznie stronę praktyczną: co, w jakiej kolejności i w jakim terminie należy zrobić. Nie zawiera opisu przebiegu incydentu ani jego analizy technicznej. Niniejszy przewodnik ma charakter wyłącznie pomocniczy. Stanowi materiał porządkujący kolejność czynności oraz terminy, nie zastępuje natomiast wewnętrznych regulacji obowiązujących u administratora – w szczególności polityki ochrony danych, procedury reagowania na naruszenia ani przyjętej metodyki analizy ryzyka.

Administrator, który dysponuje własną procedurą analizy ryzyka lub oceny skutków dla ochrony danych, przeprowadza ją zgodnie z tą procedurą. Formularze i propozycje sformułowań zawarte w załącznikach mają charakter wzorcowy i wymagają dostosowania do stanu faktycznego oraz do dokumentacji obowiązującej w danej placówce.

Za ocenę zdarzenia, kwalifikację naruszenia, decyzję o zgłoszeniu organowi nadzorcemu oraz o zawiadomieniu osób, których dane dotyczą, a także za sposób i terminowość wykonania tych obowiązków, odpowiada indywidualnie każdy administrator. Odpowiedzialności tej nie wyłącza ani nie ogranicza posłużenie się niniejszym opracowaniem.

Materiał odzwierciedla stan faktyczny i prawny na dzień 12 sierpnia 2026 r. Postępowanie wyjaśniające dostawcy oprogramowania oraz czynności organów nie zostały zakończone; kolejne ustalenia mogą wymagać uzupełnienia zgłoszeń oraz weryfikacji przyjętych ocen. **Opracowanie nie stanowi porady prawnej w indywidualnej sprawie, nie stanowi też podstawy do formułowania przez administratorów dotkniętych naruszeniem pytań o interpretację w indywidualnych przypadkach.**

Jak korzystać z przewodnika?

Punkt wyjścia jest jeden: **administratorem danych pacjentów jest gabinet, praktyka albo przychodnia, a nie dostawca oprogramowania.** Naruszenie wystąpiło w infrastrukturze dostawcy, lecz obowiązki wobec organu nadzorczego i wobec pacjentów obciążają placówkę. Nikt nie wykona ich w jej zastępstwie.

Materiał podzielono na sześć etapów uporządkowanych chronologicznie. Terminy liczone są od dnia stwierdzenia naruszenia, oznaczonego w materiale literą D. Za dzień D przyjmuje się dzień, w którym placówka powzięła wiarygodną informację o incydencie – w praktyce dzień wpływu wiadomości od dostawcy – a nie dzień ustalenia pełnego zakresu zdarzenia.

Zanim przejdą Państwo dalej: należy odszukać w skrzynce pocztowej wiadomość od dostawcy systemu i zapisać jej datę oraz godzinę. Warto sprawdzić także folder wiadomości niechcianych (SPAM).

Od tej daty biegną wszystkie terminy opisane w materiale, a jej ustalenie będzie pierwszą rzeczą, o którą zapyta organ nadzorczy.

