PREZES
URZĘD OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 21 sierpnia 2026 r.

DKN.5101.425.2026.IB
Dot. NRL-ZRP.007.19.2026.WM

Pan
dr n. med. i n. o zdr. Łukasz Jankowski
Prezes
Naczelnej Izby Lekarskiej
ul. Jana III Sobieskiego 110
00-764 Warszawa

Szanowny Panie Prezesie,

w związku z pismem Naczelnej Izby Lekarskiej (dalej też NIL) z 13 sierpnia 2026 r., dotyczącym postępowania lekarzy oraz lekarzy dentystów (dalej też administratorzy) w związku z incydentem, który miał miejsce w organizacji podmiotu przetwarzającego, tj. MyDr Sp. z o.o. (dalej też podmiot przetwarzający lub procesor) uprzejmie informuję, że zgodnie z art. 33 ust. 1 rozporządzenia 2016/679[1], w przypadku naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Zgodnie zaś z ust. 2 ww. artykułu, podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi. W sytuacji zaś, gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwane rozporządzeniem 2016/679; (Dz. Urz. UE L 119 z 4.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35).

bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu (art. 34 ust. 1 rozporządzenia 2016/679).

Z analizy ww. przepisów wynika, że w przypadku gdy do naruszenia ochrony danych osobowych doszło w organizacji podmiotu przetwarzającego, któremu administrator powierzył swoje dane osobowe, **administrator przed przystąpieniem do realizacji obowiązków, o których mowa w art. 33 ust. 1 oraz 34 ust. 1 rozporządzenia 2016/679, powinien otrzymać od ww. podmiotu przetwarzającego informację potwierdzającą, że incydent obejmował również dane administratora.** Niemniej, biorąc pod uwagę fakt, iż to na administratorach spoczywa obowiązek notyfikacji naruszeń ochrony danych osobowych do organu nadzorczego, nieuzasadniony brak kontaktu ze strony podmiotu przetwarzającego, w sytuacji gdy w przestrzeni publicznej pojawiły się informacje o możliwości wystąpienia naruszenia ochrony danych osobowych w organizacji podmiotu przetwarzającego, nie zwalnia administratorów z powinności nadzorowania podmiotu, któremu powierzyli swoje dane. W przypadku wystąpienia takiej sytuacji **administrator ma nie tylko prawo, ale także obowiązek skierować do podmiotu przetwarzającego zapytanie**, czy dane naruszenie ochrony danych osobowych mogło dotyczyć danych osobowych, które powierzył temu podmiotowi do przetwarzania.

Przypominam również uprzejmie, że zgodnie z art. 28 ust. 3 lit. f) rozporządzenia 2016/679, uwzględniając charakter przetwarzania oraz dostępne mu informacje, **podmiot przetwarzający ma obowiązek pomagać administratorowi wywiązać się z obowiązków określonych w art. 32–36**. Oznacza to obowiązek przekazania wszelkich niezbędnych informacji, począwszy od danych osobowych objętych incydentem, liczby osób, kończąc na szczegółowym opisie przebiegu wystąpienia naruszenia ochrony danych osobowych oraz wdrożonych środkach technicznych oraz organizacyjnych w celu ograniczenia ryzyka ponownego wystąpienia naruszenia w przyszłości.

Należy jednak mieć na uwadze, że ww. informacje mają wyłącznie charakter pomocniczy i nie zwalniają administratora od dokonania samodzielnej oceny zaistniałego naruszenia ochrony danych osobowych. W związku z powyższym, z chwilą otrzymania informacji od podmiotu przetwarzającego o stwierdzeniu naruszenia ochrony danych osobowych, każdy administrator jest odpowiedzialny za ich weryfikację oraz ostateczną analizę i kwalifikację incydentu jako naruszenia ochrony danych osobowych. **Dopiero z chwilą stwierdzenia naruszenia ochrony danych osobowych przez administratora biegnie termin, o którym mowa w art. 33 ust. 1 rozporządzenia 2016/679, na dokonanie jego zgłoszenia do organu nadzorczego.**

Biorąc pod uwagę powyższe oraz starając się wyjść na naprzeciw pytaniom NIL zawartym w piśmie z 13 sierpnia 2026 r. informuję, że oświadczenie podmiotu przetwarzającego o braku konieczności dokonywania zgłoszeń nie zwalnia administratorów od dokonania własnej analizy zdarzenia.

To czy określony incydent stanowi naruszenie ochrony danych osobowych, o którym mowa w art. 4 pkt 12 rozporządzenia 2016/679, a jeśli tak, to czy ww. sytuacja obliguje administratorów do podjęcia działań, o których mowa w art. 33 i 34 rozporządzenia 2016/679, należy bowiem do wyłącznych uprawnień poszczególnych administratorów. Wszelka informacja dotycząca incydentu – przekazywana administratorom przez podmiot przetwarzający – może natomiast znacznie pomóc administratorom w podjęciu decyzji o notyfikacji zdarzenia do organu nadzorczego oraz zawiadomieniu osób fizycznych o naruszeniu ochrony ich danych osobowych, ale, jak już wyżej wskazano, nie powinna zastępować własnej analizy administratora. Nie można jednak oczywiście wykluczyć sytuacji, że otrzymana od podmiotu przetwarzającego informacja, że naruszenie dotyczyło danych powierzonych przez konkretnego administratora (z określeniem zakresu danych objętych naruszeniem), może spowodować brak konieczności przeprowadzania analizy zdarzenia przez administratora, gdy informacje przekazane przez podmiot przetwarzający będą wystarczające do stwierdzenia naruszenia. Jak wskazuje EROD w pkt 31 Wytycznych 9/2022 dotyczących zgłaszania naruszenia ochrony danych osobowych na podstawie RODO, Wersja 2.0, „(...) należy uznać, że administrator **»stwierdził«** wystąpienie naruszenia **w momencie, w którym uzyskał dostateczną pewność** co do tego, **że doszło do wystąpienia incydentu** bezpieczeństwa, który **doprowadził do narażenia danych** osobowych".

Odnosząc się do terminu 72 godzin na zgłoszenie naruszenia, w sytuacji gdy administrator, bez uzyskania niezbędnych informacji od procesora, nie jest w stanie stwierdzić naruszenia ochrony danych osobowych, bieg terminu 72 godzin w ogóle nie rozpoczyna się, gdyż może on zacząć biec jedynie z „chwilą stwierdzenia naruszenia". **Administrator** jednak, jak wskazano wyżej, nie może pozostawać bierny, co oznacza, że **w przypadku nieuzasadnionego braku informacji ze strony podmiotu przetwarzającego powinien podjąć kontakt z nim w celu ustalenia, czy incydent dotyczy danych, które jemu powierzył**. Jeżeli natomiast administrator, w określonej dacie, dokonał „stwierdzenia naruszenia ochrony danych osobowych" bieg terminu 72 godzin na zgłoszenie naruszenia organowi nadzorczemu rozpoczyna się, niezależnie od tego, że oczekuje on na dodatkowe informacje na temat incydentu od procesora.

Więcej informacji na temat zgłaszania naruszeń oraz prawidłowego sporządzenia zawiadomienia do osób, których dane dotyczą można znaleźć na stronie internetowej urzędu oraz w zamieszczonym w tej sprawie komunikacie dostępnym pod linkiem: https://uodo.gov.pl/pl/138/4538.

Informuję także, że zastosowane przez podmiot MyDr Sp. z o.o. środki techniczne i organizacyjne, w tym analiza ryzyka, będą przedmiotem kontroli Prezesa Urzędu Ochrony Danych Osobowych, o czym poinformowano w komunikacie z 13 sierpnia 2026 r. (https://uodo.gov.pl/pl/138/4540).

Jednocześnie w celu pomocy w realizacji obowiązku z art. 34 rozporządzenia 2016/679 podmiotom zrzeszonym w ramach Naczelnej Izby Lekarskiej, w załączeniu przekazuję

uprzejmie wzór zawiadomienia podmiotu danych o naruszeniu ochrony jego danych osobowych.

Zał. 1

Łączę wyrazy szacunku

Mirosław Wróblewski

Prezes Urzędu
Ochrony Danych Osobowych

/ - dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem
elektronicznym /

Urzad Ochrony Danych Osobowych
ul. Stanislawa Moniuszki 1A
00-014 WARSZAWA
DKN.5101.425.2026 pismo

REPO PUH9123599418958 54

Umowa nr:582615 Data nadania: 21.08.2026

Naczelna Izba Lekarska
Sobieskiego 110
00-764 WARSZAWA

Potwierdzenie integralności oraz pochodzenia dokumentu elektronicznego od podmiotu publicznego

Niniejszy dokument stanowi integralne odzwierciedlenie treści dokumentu przekazanego w wersji elektronicznej do Poczty Polskiej S.A. za pośrednictwem systemu teleinformatycznego zintegrowanego z systemem teleinformatycznym Poczty Polskiej S.A. zgodnie z art. 58 ust. 4 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. poz. 2320).

Integralność oraz pochodzenie dokumentu elektronicznego od podmiotu publicznego zostały zapewnione z wykorzystaniem środka identyfikacji elektronicznej.

Dokument elektroniczny został przekształcony na wersję papierową zgodnie z art. 46 ust. 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. poz.2320).

Adres Doręczeń Elektronicznych Nadawcy	AE:PL-67085-31860-RWFHC-35
Data i czas nadania	Data: 21.08.2026 Czas: 08:55:55
Liczba kartek	4 + 1 kartka adresowa zawierająca potwierdzenie integralności dokumentu
Autor wydruku	Poczta Polska S.A - Operator Wyznaczony, o którym mowa w art. 3 pkt 13 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2020 r. poz. 1041 i 2320)
Data i czas wydruku	Data: 21.08.2026 Czas: 12:07:15

Zawiadomienie o naruszeniu ochrony danych osobowych

Administrator

Szpital.....

ul. .....

00-000.....

tel. .....

adres e-mail .....

Co się stało?

Z przykrością informujemy, że w wyniku cyberataku na systemy naszego podmiotu przetwarzającego, tj. MyDr Sp. z o.o. z siedzibą w Warszawie, mogło dojść do naruszenia poufności Pana/Pani danych osobowych w zakresie imienia, nazwiska, adresu zamieszkania, nr PESEL oraz danych dot. zdrowia.

Z uwagi na fakt, iż ww. incydent może skutkować wysokim ryzykiem naruszenia Pana/Pani praw lub wolności, jesteśmy zobligowani, na podstawie art. 34 rozporządzenia 2016/679[1], poinformować Pana/Panią o potencjalnych ryzykach wykorzystania Pana/Pani danych osobowych oraz przedstawić odpowiednie środki zaradcze, które może Pan/Pani podjąć w celu ochrony swoich praw, dlatego też prosimy Pana/Panią o uważne zapoznanie się z informacjami przedstawionymi w dalszej części pisma.

Gdzie może Pan/Pani uzyskać szczegółowe informacje?

W naszej organizacji wyznaczono inspektora ochrony danych. tj. Pana Jana Kowalskiego. Można się z nim skontaktować pod nr telefonu ..... lub adresem e-mail .....

[w przypadku braku IOD]

Więcej informacji na temat ww. zdarzenia może udzielić Państwu Pan Jan Kowalski. Można się z nim skontaktować pod nr telefonu ..... lub adresem e-mail .....

Jakie zagrożenia zidentyfikowaliśmy w związku z naruszeniem Pana/Pani danych osobowych.

Wśród ujawnionych danych znajdował się Pana/Pani nr PESEL, który w połączeniu z Pana/Pani imieniem i nazwiskiem, w określonych sytuacjach, może posłużyć osobom nieuprawnionym do działań wymierzonych w Pana/Pani prawa, w szczególności do:

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zwane rozporządzeniem 2016/679; (Dz. Urz. UE L 119 z 4.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35).

- wzięcia pożyczki lub kredytu na Pana/Pani dane osobowe;

- uzyskania dostępu do Pana/Pani danych zdrowia w instytucjach medycznych, w których uwierzytelnianie osób następuje przy pomocy nr PESEL;

- zawarcia umów na Pana/Pani dane osobowe.

Naruszenie dotyczyło również danych dotyczących Pana/Pani stanu zdrowia, a więc danych wrażliwych, których nieuprawnione ujawnienie również może naruszać Pana/Pani prawa, w szczególności:

- osoby trzecie mogą spróbować wykorzystać ww. dane do dyskryminacji Pana/Pani osoby w Pana/Pani środowisku zamieszkania;

- osoby trzecie mogą spróbować naruszyć Pana/Pani dobra osobiste;

- osoby trzecie mogą próbować wykorzystać ww. dane w celu dokonania oszustwa, np. kontakt z Panem/Panią lub bliskimi w celu zaoferowania alternatywnych metod leczenia zdiagnozowanych u Pana/Pani chorób.

Jakie działania może Pan/Pani podjąć

W przypadku nr PESEL proponujemy:

- zastrzec swój nr PESEL [od 1 czerwca 2024 r. instytucje finansowe są zobligowane weryfikować, czy nr PESEL jest zastrzeżony przy zawieraniu umów. Może Pan/Pani zastrzec nr PESEL przez Internet lub osobiście w Urzędzie Gminy (Miasta). Zastrzeżenie jest usługą bezpłatną. Należy również pamiętać, iż zastrzeżenie nr PESEL w żaden sposób nie blokuje możliwości rejestracji u lekarza, czy też realizacji recepty, jak też nie stanowi przeszkody w załatwieniu sprawy w urzędzie – więcej informacji znajdzie Pan/Pani pod linkiem: https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie;

- skorzystać z zastrzeżenia kredytowego w portalu BIK;

- poinformować placówki medyczne, w których świadczone są Pana/Pani usługi, iż osoby trzecie mogą chcieć wykorzystać Pana/Pani nr PESEL w celu przejścia procesu autoryzacji w ich jednostkach;

- w przypadku powzięcia wiedzy na temat wykorzystania Pana/Pani danych może Pan/Pani również powiadomić organy ścigania.

W przypadku danych dotyczących zdrowia:

- może Pan/Pani skorzystać z narzędzi ochrony dóbr osobistych, o których mowa w kodeksie cywilnym czy kodeksie postępowania cywilnego;

- może Pan/Pani powiadomić również organy ścigania o bezprawnym wykorzystywaniu Pan/Pani danych osobowych;

- należy uważać na kontakty z nieznanymi osobami, które nie miały prawa znać historii Pana/Pani zdrowia, a które proponują Panu/Pani skorzystanie z oferowanych przez

nie usług medycznych/pseudomedycznych/terapeutycznych. Proszę również uczulić na to Pana/Pani domowników;

- może Pan/Pani skorzystać ze wsparcia psychologicznego w sytuacjach silnego stresu lub niepokoju.