Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.166.2026
Warszawa, 07 września 2026 r.

Szanowna Pani
Magdalena Biejat
Wicemarszałek Senatu RP

Dot. pisma z 21 sierpnia 2026 r. w sprawie oświadczenia złożonego przez senatora Adama Szejnfelda w dniu 19 sierpnia 2026 r. (BPS/043-64-1739/26)

Szanowna Pani Marszałek,

poniżej przedstawiam odpowiedzi na złożone przez Senatora oświadczenie.

Ad 1) Kto i jakim prawem zbiera, posiada oraz centralnie przetwarza dane wrażliwe obywateli bez ich wiedzy i zgody? Jeśli jest to zgodne z prawem lub korzysta się w tym zakresie ze stanu nieuregulowanego prawnie, to czy pan minister zamierza legislacyjnie zmienić ten stan?

W niniejszym pytaniu źródłem nakreślonego przez Senatora problemu nie jest braku podstawy prawnej do przetwarzania danych szczególnych kategorii, ponieważ przesłanki do ich przetwarzania zostały uregulowane w art. 9 ust. 2 unijnym rozporządzeniu 2016/679 (dalej jako: „RODO"), lecz konieczność nałożenia na podmioty przetwarzające dane medyczne dodatkowych wymagań z zakresu spełniania standardów bezpieczeństwa.

W związku z czym, zgodnie z zapowiedziami Ministerstwo Cyfryzacji przygotowało „Cyber Piątkę", czyli propozycję zmian legislacyjnych, których celem jest uszczelnienie systemu ochrony danych osobowych, w tym medycznych, a w konsekwencji wzmocnienie bezpieczeństwa danych obywateli. Na „Cyber Piątkę" składają się m.in. propozycje zmian dotyczące:

- określenia minimalnych wymagań technologicznych dla systemów teleinformatycznych wykorzystywanych do przetwarzania danych medycznych;
- wprowadzenia obowiązku informowania pacjentów o powierzeniu przetwarzania ich danych podmiotom zewnętrznym;
- wprowadzenia nowych obowiązków dla podmiotów, które przetwarzają dane na dużą skalę – świadczą usługi przetwarzania danych dla więcej niż 100 administratorów lub przetwarzają dane dotyczące łącznie ponad 100 tys. osób[1].

Ad 2) Czy w dzisiejszych czasach wojen pełnoskalowych, ale i tych hybrydowych, także mających miejsce w cyberprzestrzeni, bezpieczne i rozsądne jest przetrzymywanie danych w bazach centralnych? Uważam, że nie, ale jeśli jest inny pogląd, to czy zamierza się wprowadzić kolejne, dodatkowe zabezpieczenia prawne i faktyczne cyberprzestrzeni, szczególnie jeśli chodzi o centralne bazy danych?

Kluczowe w tym aspekcie jest zapewnienie odpowiedniego poziomu bezpieczeństwa. Podwyższone i mające zastosowanie do znacznie szerszego kręgu podmiotów (docelowo nawet ponad 100 tys. podmiotów w 18 sektorach) wymogi cyberbezpieczeństwa

[1] https://www.gov.pl/web/cyfryzacja/cyber-piatka--ministerstwo-cyfryzacji-proponuje-nowe-zasady-ochrony-danych

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

wprowadzone zostały poprzez nowelizację ustawy o krajowym systemie cyberbezpieczeństwa[2], która weszła w życie 3 kwietnia 2026 r.

Podmioty te, zgodnie z nowymi przepisami, obowiązane są do wdrożenia wymagań z zakresu cyberbezpieczeństwa, w tym w szczególności do wdrożenia systemu zarządzania bezpieczeństwem informacji, który ma zapewniać m.in. prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu, wdrożenie polityki szacowania ryzyka, wdrożenie polityki kontroli dostępu, bezpieczeństwo fizyczne i środowiskowe, bezpieczeństwo zasobów ludzkich, bezpieczeństwo i ciągłość łańcucha dostaw, edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu, plany awaryjne i plany odtworzeniowe. Konieczne jest także stosowanie bezpiecznych środków komunikacji elektronicznej uwzględniających uwierzytelnianie wieloskładnikowe.

Podkreślić należy, że nawet jeśli niektóre podmioty nie zostaną zakwalifikowane jako podmioty kluczowe lub podmioty ważne, a współpracują z tymi podmiotami, w szczególności występują w ich łańcuchu dostaw np. w obszarze połączeń i zależności systemów czy usług, to one również powinny zostać objęte wymaganiami z zakresu cyberbezpieczeństwa. Wynika to z tego, że na podmiotach kluczowych i podmiotach ważnych spoczywa obowiązek zapewnienia bezpiecznego łańcucha dostaw.

W kontekście tych wymogów należy zwrócić uwagę na okres przejściowy związany z nowelizacją ustawy o KSC. Gdy wszystkie przepisy zaczną obowiązywać Państwo Polskie będzie miało większą możliwość oddziaływania na podmioty KSC w celu zapewniania cyberbezpieczeństwa państwa, gospodarki i obywateli.

Jednocześnie Ministerstwo Cyfryzacji analizuje potencjalne uzupełnienie przepisów dotyczących cyberbezpieczeństwa. Przy czym należy mieć na uwadze przedstawione powyżej kwestie związane z okresem dostosowawczym nowelizacji ustawy o KSC uchwalonej w tym roku, która już wprowadziła wysokie wymagania dotyczące cyberbezpieczeństwa.

Należy także zwrócić uwagę, że w zakresie ochrony danych osobowych wymagań nakłada w tym zakresie RODO. Zgodnie z art. 32 RODO administrator oraz podmiot przetwarzający zobowiązani są do wdrożenia odpowiednich środków technicznych i organizacyjnych, w celu zapewnienia stopnia bezpieczeństwa odpowiadającemu danemu ryzyku. Dopasowując odpowiednie środki zabezpieczeń, administrator oraz podmiot przetwarzający muszą wziąć pod uwagę stan wiedzy technicznej, koszt wdrażania oraz charakter, kontekst i cele przetwarzania oraz ryzyko naruszenia prawa lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Ad 3) Czy wobec firmy MyDr oraz podmiotów korzystających z jej oprogramowania uruchomiono działania służące zweryfikowaniu spełnienia wymogów art. 32 RODO, w szczególności w zakresie adekwatności środków technicznych i organizacyjnych, kontroli dostępu, zarządzania podatnościami, zdolności do szybkiego wykrycia incydentu, odtworzenia dostępności danych i zachowania materiału dowodowego? Czy przeprowadzono niezależną ocenę wektora ataku oraz skuteczności działań ograniczających jego skutki?

[2] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 r. poz. 20 z późn. zm.) (ustawa o KSC)

W zakresie przestrzegania przez spółkę MyDr przepisów o ochronie danych osobowych, kontrolę prowadzi Prezes Urzędu Ochrony Danych Osobowych (dalej: Prezes UODO), o czym poinformował w odrębnym komunikacie z dnia 13.08.2026 r. dostępnym na stronie UODO[3].

Kontrola odbywa się na podstawie art. 78 i następnych ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Zgodnie z treścią ww. komunikatu przedmiotem kontroli jest przede wszystkim sprawdzenie zastosowanych przez spółkę MrDr środków technicznych i organizacyjnych, a także ocena czy analiza ryzyka uwzględniała możliwe zagrożenia dla przetwarzanych danych, a jej wyniki zostały zastosowane w praktyce. Kontrolerzy Urzędu weryfikują także, czy zabezpieczenia były regularnie testowane pod kątem zmieniających się zagrożeń.

Niezależnie od tego postępowanie w sprawie prowadzi Centralne Biuro Zwalczania Cyberprzestępczości pod nadzorem Prokuratury Okręgowej w Warszawie, a działania w zakresie wsparcia firmy w obsłudze incydentu realizuje CSIRT NASK, zgodnie z swoim zakresem odpowiedzialności określonym w art. 26 ust. 3 i 6 ustawy o KSC.

Ad 4) Czy ustalono, którzy administratorzy danych oraz podmiot przetwarzający wykonali obowiązki z art. 33 RODO, w tym zgłosili naruszenie prezesowi Urzędu Ochrony Danych Osobowych w terminie przewidzianym w tym przepisie, a także udokumentowali okoliczności naruszenia, jego skutki i działania zaradcze zgodnie z art. 33 ust. 5 RODO? Jeżeli zgłoszenia dokonano po upływie 72 godzin, to czy przedstawiono wymagane wyjaśnienie przyczyn opóźnienia?

Należy wyjaśnić, że Prezes UODO nie jest organem administracji rządowej podległym Radzie Ministrów, lecz niezależnym organem nadzorczym, wobec czego Minister Cyfryzacji nie posiada informacji na temat naruszeń zgłaszanych Prezesowi UODO.

Ad 5) Czy po przeprowadzeniu analizy ryzyka uruchomiono wobec osób, których dane mogły zostać naruszone, procedurę z art. 34 RODO, tj. indywidualne zawiadomienie bez zbędnej zwłoki, jeżeli naruszenie może powodować wysokie ryzyko dla ich praw lub wolności? Jeżeli którykolwiek z administratorów uznał, że zachodzi wyjątek od tego obowiązku na podstawie art. 34 ust. 3 RODO, to na jakich ustaleniach faktycznych i środkach zabezpieczających oparł tę ocenę?

Należy wyjaśnić, że Prezes UODO nie jest organem administracji rządowej podległym Radzie Ministrów, lecz niezależnym organem nadzorczym, wobec czego Minister Cyfryzacji nie posiada informacji na temat wyników kontroli prowadzonych przez Prezesa UODO w zakresie przestrzegania przez administratorów przepisów o ochronie danych osobowych.

Ad 6) Czy w toku wyjaśnień badane jest, czy umowy powierzenia przetwarzania danych i nadzór administratorów nad podmiotem przetwarzającym odpowiadały art. 28 RODO, a także czy – ze względu na skalę i charakter przetwarzania danych medycznych – sporządzono lub zaktualizowano ocenę skutków dla ochrony danych zgodnie z art. 35 RODO? Jakie mechanizmy koordynacji z prezesem Urzędu Ochrony Danych Osobowych oraz wsparcia dla obywateli zostaną uruchomione, w tym rzetelne informacje o ryzykach i środkach ochrony, z uwzględnieniem prawa do odszkodowania na podstawie art. 82 RODO oraz kompetencji organu nadzorczego do stosowania środków naprawczych i administracyjnych kar pieniężnych, o których mowa w art. 83 RODO?

Na wstępie należy wyjaśnić, że Prezes UODO nie jest organem administracji rządowej podległym Radzie Ministrów, lecz niezależnym organem nadzorczym. Ocena zgodności umów powierzenia przetwarzania oraz nadzoru administratorów nad podmiotem

[3] https://uodo.gov.pl/pl/138/4540

przetwarzającym z art. 28 RODO, jak również ocena wykonania obowiązku z art. 35 RODO, należy do wyłącznej właściwości Prezesa UODO. Minister Cyfryzacji nie posiada informacji o przebiegu i wynikach prowadzonych przez ten organ postępowań kontrolnych.

Ministerstwo Cyfryzacji pozostaje w stałej współpracy z Prezesem UODO. Wnioski płynące z dotychczasowych incydentów znalazły odzwierciedlenie w przygotowanym pakiecie „Cyber Piątka", co zostało już przedstawione w odpowiedzi na pytanie nr 1.

W zakresie wsparcia obywateli należy wskazać, że podstawowym kanałem informacji o naruszeniu pozostaje administrator danych, czyli placówka medyczna, na której zgodnie z art. 34 RODO spoczywa obowiązek zawiadomienia osoby, której dane dotyczą, o naruszeniu powodującym wysokie ryzyko naruszenia jej praw lub wolności. Wyłącznie administrator dysponuje wiedzą o zakresie danych objętych naruszeniem w odniesieniu do konkretnego pacjenta.

Kierując się dobrem obywateli, informacja o wycieku została dodana do portalu bezpiecznedane.gov.pl, co umożliwia każdemu samodzielną weryfikację. Na moment sporządzania niniejszej odpowiedzi służby nie stwierdziły upublicznienia tych danych. Na portalu udostępniono również bazę wiedzy zawierającą podstawowe informacje o incydencie oraz opis rekomendowanych działań ochronnych, w tym zastrzeżenie numeru PESEL za pośrednictwem aplikacji mObywatel, stosowania uwierzytelniania wieloskładnikowego oraz zachowania szczególnej ostrożności wobec prób wyłudzenia danych.

Odnosząc się do kwestii uprawnień przysługujących osobom, których dane dotyczą, należy doprecyzować, że zgodnie z art. 82 RODO każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia przepisów rozporządzenia, ma prawo do odszkodowania od administratora lub podmiotu przetwarzającego. Roszczenie to dochodzone jest w postępowaniu cywilnym przed sądem powszechnym. Z kolei przewidziane w art. 83 RODO administracyjne kary pieniężne oraz środki naprawcze z art. 58 ust. 2 RODO pozostają w wyłącznej kompetencji Prezesa UODO.

Prezes UODO opublikował ponadto odpowiedzi na najczęściej zadawane pytania związane z incydentem bezpieczeństwa MyDr, dostępne na stronie UODO[4]:

Ad 7) Jakie działania systemowe zamierza podjąć Ministerstwo Cyfryzacji, aby ograniczyć ryzyko wystąpienia podobnego zdarzenia w przyszłości?

Ministerstwo Cyfryzacji analizuje potencjalne uzupełnienie przepisów dotyczących cyberbezpieczeństwa. Jednocześnie na obecnym Ministerstwo Cyfryzacji nie identyfikuje konieczności dokonania istotnych zmian w ustawie o KSC. W tym zakresie należy wskazać na przedstawione w odpowiedzi na pytanie nr 2 kwestie związane z okresem dostosowawczym nowelizacji ustawy o KSC uchwalonej w tym roku, która to ustawa wprowadziła już szczegółowe wymogi w zakresie cyberbezpieczeństwa.

Ministerstwo Cyfryzacji przygotowało „Cyber Piątkę", czyli propozycje zmian legislacyjnych, których celem jest uszczelnienie systemu ochrony danych osobowych, w tym medycznych, a w konsekwencji wzmocnienie bezpieczeństwa danych obywateli, co zostało już przedstawione w odpowiedzi na pytanie nr 1.

Ad 8) Czy ministerstwo rozważa stworzenie szczególnych standardów cyberbezpieczeństwa dla podmiotów przetwarzających na dużą skalę dane, w tym obowiązkowych i cyklicznych audytów bezpieczeństwa, testów penetracyjnych,

[4] https://uodo.gov.pl/pl/615/4550

wymogów dotyczących szyfrowania i segmentacji danych, zasad ograniczania okresu ich przechowywania oraz procedur szybkiego informowania obywateli o naruszeniach?

W tym zakresie obowiązują już szczegółowe wymogi cyberbezpieczeństwa określone w art. 8 ustawy o KSC przedstawione w odpowiedzi na pytanie nr 2. Jednocześnie w tym zakresie należy wskazać na przedstawione również w odpowiedzi na pytanie nr 2 kwestie związane z okresem dostosowawczym nowelizacji ustawy o KSC uchwalonej w tym roku.

Piąty filar opracowanej przez Ministerstwo Cyfryzacji „Cyber Piątki" obejmuje podmioty przetwarzające dane na skalę, której obecny reżim prawny w żaden sposób nie różnicuje: świadczące usługi przetwarzania na rzecz więcej niż 100 administratorów albo przetwarzające dane dotyczące łącznie ponad 100 tysięcy osób. Kryterium ma charakter alternatywny — spełnienie któregokolwiek z progów będzie skutkowało objęciem nowymi obowiązkami, niezależnie od tego, czy dany podmiot występuje formalnie jako administrator, czy wyłącznie jako podmiot przetwarzający.

Pierwszym z projektowanych obowiązków jest niezwłoczne zawiadamianie o naruszeniu, polegające na przekazaniu do CSIRT NASK, za pośrednictwem Policji, danych osób, których bezpieczeństwo zostało naruszone, w celu zasilenia bazy portalu bezpiecznedane.gov.pl. Rozwiązanie to usuwa istotną barierę proceduralną: dotychczas przekazanie takich danych wymagało uprzedniego postanowienia prokuratora, co wydłużało ścieżkę o dodatkowe czynności i czas. Ma to bezpośrednie znaczenie praktyczne, ponieważ wartość ostrzeżenia dla obywatela maleje wraz z upływem czasu od naruszenia — możliwość zastrzeżenia numeru PESEL czy zmiany danych uwierzytelniających jest tym skuteczniejsza, im wcześniej zostanie podjęta.

Drugim obowiązkiem jest przejrzystość wobec administratora. Podmiot przetwarzający ma przekazywać placówkom, które powierzyły mu dane, informacje niezbędne do oceny poziomu ich bezpieczeństwa, w tym wyniki audytów, testów i ocen bezpieczeństwa, których przeprowadzanie stanie się obligatoryjne. Administrator, tj. gabinet lub przychodnia medyczna ma dysponować pełną wiedzą o statusie certyfikacyjnym i zabezpieczeniach dostawcy jeszcze przed zawarciem umowy powierzenia przetwarzania danych osobowych.

Trzecim obowiązkiem jest ocena ryzyka przeprowadzana przed rozpoczęciem przetwarzania, a następnie aktualizowana nie rzadziej niż raz na dwa lata oraz po każdej istotnej zmianie sposobu lub warunków przetwarzania.

Konstrukcja całego filaru sprowadza się zatem do przeniesienia ciężaru z reakcji następczej na obowiązki prewencyjne, bez naruszania dotychczasowego podziału ról między administratora a podmiot przetwarzający.

Z wyrazami szacunku
Paweł Olszewski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa