

Informacja o naruszeniu ochrony danych osobowych pacjentów

Szanowni Państwo,

działając jako administrator danych osobowych naszych pacjentów, informujemy o naruszeniu ochrony danych osobowych. Naruszenie wystąpiło u naszego podmiotu przetwarzającego, który dostarcza system do prowadzenia elektronicznej dokumentacji medycznej. Przekazujemy tę informację zgodnie z art. 34 RODO. Zależy nam, aby mogła Pani/mógł Pan podjąć świadome działania w celu ochrony swoich danych.

1. Opis zdarzenia

Elektroniczną dokumentację medyczną prowadzimy w systemie FELG Dent. Dostarcza go FELG Software sp. z o.o. z siedzibą w Krakowie (ul. Sławkowska 25/9, 31-016 Kraków), która przetwarza dane na nasze zlecenie. Spółka poinformowała nas 7 października 2026 r., że jej infrastruktura padła ofiarą cyberataku. W okresie od 28 sierpnia do 29 września 2026 r. osoba nieuprawniona uzyskiwała dostęp do danych przetwarzanych w systemie. Dostawca opanował incydent i nadal wyjaśnia jego okoliczności.

2. Zakres danych

Naruszenie mogło objąć następujące dane pacjentów zapisane w systemie: imię i nazwisko, datę urodzenia, adres zamieszkania, numer PESEL, adres e-mail, numer telefonu oraz informacje o stanie zdrowia.

3. Możliwe konsekwencje

Ze względu na zakres danych nie można wykluczyć, że ktoś spróbuje wykorzystać je bez Pani/Pana wiedzy, w szczególności:

- do zawarcia umowy kredytu, pożyczki lub innej umowy, w tym sprzedaży ratalnej;
- do uzyskania dostępu do Pani/Pana danych medycznych w innych placówkach, w których tożsamość potwierdza się numerem PESEL;
- w sposób, który mógłby prowadzić do nieuprawnionego ujawnienia informacji o stanie zdrowia, a w konsekwencji do naruszenia Pani/Pana praw;
- do kontaktu, w którym ktoś podszywa się pod placówkę medyczną, bank lub urząd albo oferuje usługi medyczne.

4. Podjęte działania

Niezwłocznie po otrzymaniu informacji zgłosiliśmy naruszenie Prezesowi Urzędu Ochrony Danych Osobowych.

FELG Software sp. z o.o.:

- zamknęła dostęp osobie nieuprawnionej;
- wprowadziła obowiązkowe uwierzytelnianie dwuskładnikowe dla wszystkich użytkowników systemu;

- wzmocniła mechanizmy kontroli dostępu;
- zaangażowała zewnętrznych specjalistów ds. cyberbezpieczeństwa;
- zawiadomiła właściwą prokuraturę;
- współpracuje z CERT Polska oraz z Urzędem Ochrony Danych Osobowych.

Ze swojej strony weryfikujemy zabezpieczenia stosowane przez dostawcę oraz uprawnienia użytkowników systemu w naszej placówce.

5. Zalecenia

Zalecamy podjęcie następujących działań:

- Zastrzeżenie numeru PESEL.** Jest to usługa bezpłatna. PESEL można zastrzec w aplikacji mObywatel, na stronie gov.pl (www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie) lub w urzędzie gminy. Instytucje finansowe mają obowiązek sprawdzić zastrzeżenie przed zawarciem umowy. Zastrzeżenie nie ogranicza korzystania z usług medycznych ani realizacji recept.
- Usługa powiadomień kredytowych.** Można rozważyć usługę powiadamiania o próbach zaciągnięcia zobowiązania, np. alerty BIK.
- Ostrożność wobec nieoczekiwanych wiadomości i telefonów.** Nie prosimy pacjentów o podawanie haseł, kodów ani danych osobowych, nie prosimy też o płatności w wiadomościach e-mail, SMS ani telefonicznie. W razie wątpliwości prosimy o kontakt bezpośrednio z placówką.
- Zgłoszenie nadużycia.** Jeżeli podejrzewa Pani/Pan, że dane zostały wykorzystane niezgodnie z prawem, można zgłosić to Policji (www.gov.pl/web/gov/zglos-przestepstwo).

6. Kontakt

W sprawach związanych z naruszeniem prosimy o kontakt z naszym inspektorem ochrony danych, Panią Kingą Kaniewską: iod@twojlekarz-wawa.pl. Pytania dotyczące samego incydentu można kierować również do FELG Software sp. z o.o.: dane.pacjent@felg.app.

Przepraszamy za tę sytuację i zapewniamy, że ochrona danych naszych pacjentów pozostaje dla nas priorytetem.

Інформація про порушення захисту персональних даних пацієнтів

Шановні пані та панове,

діючи як адміністратор персональних даних наших пацієнтів, повідомляємо про порушення захисту персональних даних. Порушення сталося в компанії, яка за нашим дорученням обробляє персональні дані та надає систему для ведення електронної медичної документації. Ми надаємо цю інформацію відповідно до ст. 34 Загального регламенту про захист даних (GDPR, пол. RODO). Ми хочемо, щоб Ви могли свідомо вжити заходів для захисту своїх даних.

1. Опис події

Електронну медичну документацію ми ведемо в системі FELG Dent. Її постачає компанія FELG Software sp. z o.o. з місцезнаходженням у Кракові (ul. Sławkowska 25/9, 31-016 Kraków), яка обробляє дані за нашим дорученням. 7 жовтня 2026 р. компанія повідомила нам, що її інфраструктура зазнала кібератаки. У період з 28 серпня по 29 вересня 2026 р. стороння особа отримала несанкціонований доступ до даних, що обробляються в системі. Постачальник узяв інцидент під контроль і продовжує з'ясовувати його обставини.

2. Обсяг даних

Порушення могло стосуватися таких даних пацієнтів, збережених у системі: ім'я та прізвище, дата народження, адреса проживання, номер PESEL, адреса електронної пошти, номер телефону, а також інформація про стан здоров'я.

3. Можливі наслідки

З огляду на обсяг даних не можна виключати, що хтось спробує використати їх без Вашого відома, зокрема:

- для укладення договору кредиту, позики чи іншого договору, зокрема купівлі в розстрочку;
- для отримання доступу до Ваших медичних даних в інших медичних закладах, де особу ідентифікують за номером PESEL;
- у спосіб, що може призвести до несанкціонованого розголошення інформації про стан здоров'я, а отже – до порушення Ваших прав;
- для встановлення контакту з Вами, коли хтось видає себе за представника медичного закладу, банку чи державної установи або пропонує медичні послуги.

4. Вжиті заходи

Одразу після отримання інформації ми подали повідомлення про порушення Голові польського Управління із захисту персональних даних (Prezes Urzędu Ochrony Danych Osobowych).

FELG Software sp. z o.o.:

- припинила доступ сторонньої особи;

- запровадила обов'язкову двофакторну автентифікацію для всіх користувачів системи;
- посилила механізми контролю доступу;
- залучила зовнішніх фахівців з кібербезпеки;
- повідомила відповідну прокуратуру;
- співпрацює з CERT Polska та Управлінням захисту персональних даних.

Зі свого боку ми перевіряємо заходи безпеки, які застосовує постачальник, а також права доступу користувачів системи в нашому закладі.

5. Рекомендації

Рекомендуємо вжити таких заходів:

- Обмеження використання номера PESEL.** Ця послуга безкоштовна. Обмежити використання номера PESEL (польською: zastrzeżenie numeru PESEL) можна в застосунку mObywatel, на сайті gov.pl (www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie) або в адміністрації гміни (місцевому органі самоврядування). Фінансові установи зобов'язані перевіряти наявність такого обмеження перед укладенням договору. Це обмеження не перешкоджає користуванню медичними послугами та отриманню ліків за рецептом.
- Сповіщення про кредитні операції.** Варто розглянути послугу сповіщень про спроби оформити зобов'язання на Ваше ім'я, наприклад сповіщення ВІК (Бюро кредитної інформації).
- Обережність щодо неочікуваних повідомлень і дзвінків.** Ми не просимо пацієнтів повідомляти паролі, коди чи персональні дані, а також не звертаємося з проханнями здійснити оплату в електронних листах, SMS-повідомленнях або під час телефонних розмов. У разі сумнівів просимо звертатися безпосередньо до закладу.
- Повідомлення про зловживання.** Якщо Ви підозрюєте, що Ваші дані були використані незаконно, Ви можете повідомити про це поліцію (www.gov.pl/web/gov/zglos-przestepstwo).

6. Контакти

З питань, пов'язаних із порушенням, просимо звертатися до нашого інспектора із захисту даних – пані Кінги Каневської (Kinga Kaniewska): iod@twojlekarz-wawa.pl. Запитання щодо самого інциденту можна також надсилати до FELG Software sp. z o.o.: dane.pacjent@felg.app.

Просимо вибачення за цю ситуацію та запевняємо, що захист даних наших пацієнтів залишається для нас пріоритетом.

Информация о нарушении защиты персональных данных пациентов

Уважаемые дамы и господа,

действуя в качестве администратора персональных данных наших пациентов, сообщаем о нарушении защиты персональных данных. Нарушение произошло в компании, которая по нашему поручению обрабатывает персональные данные и предоставляет систему для ведения электронной медицинской документации. Мы предоставляем эту информацию в соответствии со ст. 34 Общего регламента по защите данных (GDPR, пол. RODO). Мы хотим, чтобы Вы могли осознанно принять меры для защиты своих данных.

1. Описание события

Электронную медицинскую документацию мы ведём в системе FELG Dent. Её предоставляет компания FELG Software sp. z o.o. с местонахождением в Кракове (ul. Sławkowska 25/9, 31-016 Kraków), которая обрабатывает данные по нашему поручению. 7 октября 2026 г. компания сообщила нам, что её инфраструктура подверглась кибератаке. В период с 28 августа по 29 сентября 2026 г. постороннее лицо получило несанкционированный доступ к данным, обрабатываемым в системе. Поставщик взял инцидент под контроль и продолжает выяснять его обстоятельства.

2. Объём данных

Нарушение могло затронуть следующие данные пациентов, хранящиеся в системе: имя и фамилия, дата рождения, адрес проживания, номер PESEL, адрес электронной почты, номер телефона, а также информация о состоянии здоровья.

3. Возможные последствия

Учитывая объём данных, нельзя исключить, что кто-то попытается использовать их без Вашего ведома, в частности:

- для заключения договора кредита, займа или иного договора, в том числе купли-продажи в рассрочку;
- для получения доступа к Вашим медицинским данным в других медицинских учреждениях, где личность пациента устанавливается по номеру PESEL;
- способом, который может привести к несанкционированному раскрытию информации о состоянии здоровья, а следовательно – к нарушению Ваших прав;
- для установления контакта с Вами, когда кто-либо выдаёт себя за представителя медицинского учреждения, банка или государственного органа либо предлагает медицинские услуги.

4. Принятые меры

Сразу после получения информации мы направили уведомление о нарушении Председателю польского Управления по защите персональных данных (Prezes Urzędu Ochrony Danych Osobowych).

FELG Software sp. z o.o.:

- прекратила доступ постороннего лица;
- ввела обязательную двухфакторную аутентификацию для всех пользователей системы;
- усилила механизмы контроля доступа;
- привлекла внешних специалистов по кибербезопасности;
- уведомила соответствующую прокуратуру;
- сотрудничает с CERT Polska и Управлением по защите персональных данных.

Со своей стороны мы проверяем меры безопасности, применяемые поставщиком, а также права доступа пользователей системы в нашем учреждении.

5. Рекомендации

Рекомендуем принять следующие меры:

- Ограничение использования номера PESEL.** Эта услуга бесплатна. Ограничить использование номера PESEL (по-польски: zastrzeżenie numeru PESEL) можно в приложении mObywatel, на сайте gov.pl (www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie) или в администрации гмины (органе местного самоуправления). Финансовые учреждения обязаны проверять наличие такого ограничения перед заключением договора. Это ограничение не препятствует получению медицинских услуг и лекарств по рецепту.
- Уведомления о кредитных операциях.** Стоит рассмотреть услугу уведомлений о попытках оформить обязательство на Ваше имя, например уведомления ВІК (Бюро кредитной информации).
- Осторожность в отношении неожиданных сообщений и звонков.** Мы не просим пациентов сообщать пароли, коды или персональные данные, а также не обращаемся с просьбами об оплате в электронных письмах, SMS-сообщениях или во время телефонных разговоров. В случае сомнений просим обращаться непосредственно в учреждение.
- Сообщение о злоупотреблении.** Если Вы подозреваете, что Ваши данные были использованы незаконно, Вы можете сообщить об этом в полицию (www.gov.pl/web/gov/zglos-przestepstwo).

6. Контакты

По вопросам, связанным с нарушением, просим обращаться к нашему инспектору по защите данных – г-же Кинге Каневской (Kinga Kaniewska): iod@twojlekarz-wawa.pl. Вопросы, касающиеся самого инцидента, можно также направлять в FELG Software sp. z o.o.: dane.pacjent@felg.app.

Приносим извинения за сложившуюся ситуацию и заверяем, что защита данных наших пациентов остается для нас приоритетом.