Oświadczenie złożone
przez senatora Adama Szejnfelda
w dniu 19 sierpnia 2026 r.

Oświadczenie skierowane do wiceprezesa Rady Ministrów, ministra cyfryzacji Krzysztofa Gawkowskiego

Szanowny Panie Ministrze!

Z mediów, a także z doniesień pana resortu, dowiedzieliśmy się o gigantycznym cyberataku na systemy medyczne firmy MyDr. Z informacji medialnych wynika, iż w ręce hakerów wpadło nawet 31 milionów indywidualnych rekordów danych, które dotyczyły blisko 19 milionów obywateli Polski (mówiąc ściślej, szacuje się ich liczbę na 18,8 miliona osób). Wyciek dotyczy ok. 12 tysięcy placówek medycznych w całym kraju. Cała skradziona baza danych waży ponad 2 terabajty (TB). Wykradzione rekordy to m.in: dane identyfikacyjne (imiona, nazwiska, daty urodzenia, numery PESEL), dane kontaktowe (numery telefonów) oraz wrażliwe dane medyczne (informacje o wizytach, receptach, przyjmowanych lekach oraz rozpoznaniach chorobowych). Z tych informacji wynika wniosek, iż może to być największy cyberatak w najnowszej historii Polski!

Szczególne zaniepokojenie budzi możliwość objęcia incydentem nie tylko danych identyfikacyjnych i kontaktowych, lecz także informacji związanych z korzystaniem ze świadczeń zdrowotnych, wystawionymi receptami, stosowanymi lekami albo innymi danymi o stanie zdrowia. Dane dotyczące zdrowia należą do szczególnych kategorii danych osobowych w rozumieniu art. 9 RODO. Ich ujawnienie może narazić obywateli na oszustwa, kradzież tożsamości, phishing, szantaż lub niedopuszczalne profilowanie.

Z przekazów publicznych wynika również, że z oprogramowania dostarczanego przez zaatakowaną firmę MyDr korzystało ok. 12 tysięcy podmiotów. Dlatego oceny wymaga nie tylko to, kto dokonał ataku, czy ze swojej inicjatywy, czy też na zlecenie podmiotów trzecich oraz jakie były bezpośrednie przyczyny tego ataku, lecz także to, czy administratorzy i podmioty przetwarzające wypełnili obowiązki wynikające w szczególności z art. 28 RODO (powierzenie przetwarzania), art. 32 RODO (bezpieczeństwo przetwarzania) oraz art. 35 RODO (ocena skutków dla ochrony danych), jeżeli było to wymagane.

Prezes Urzędu Ochrony Danych Osobowych przypomniał podmiotom powierzającym firmie MyDr przetwarzanie danych o potrzebie przeprowadzenia analizy ryzyka oraz ustalenia, czy zachodzi obowiązek zgłoszenia naruszenia i indywidualnego zawiadomienia osób, których dane dotyczą. Obowiązek zgłoszenia naruszenia organowi nadzorczemu, co do zasady w terminie 72 godzin od jego stwierdzenia, wynika z art. 33 RODO, a obowiązek zawiadomienia osób w razie wysokiego ryzyka dla ich praw lub wolności – z art. 34 RODO. Równolegle sprawą zajmują się organy ścigania. Należy jednak wyjaśnić również, czy systemowe mechanizmy prawne, organizacyjne i techniczne zapewniają obywatelom adekwatną ochronę w sytuacji przetwarzania tak rozległego zbioru danych przez dostawcę technologii.

Szanowny Panie Ministrze, w związku z powyższym mam kilka pytań.

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?

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?

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?

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?

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?

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?

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

8. Czy ministerstwo rozważa stworzenie szczególnych standardów cyberbezpieczeństwa dla podmiotów przetwarzających na dużą skalę dane, w tym obowiązkowych i cyklicznych audytów bezpieczeństwa, testów penetracyjnych, wymogów dotyczących szyfrowania i segmentacji danych, zasad ograniczania okresu ich przechowywania oraz procedur szybkiego informowania obywateli o naruszeniach?

Niezależnie od przytoczonego przypadku firmy MyDr chciałbym zaznaczyć, iż obecnie w Polsce niemalże wszystkie instytucje publiczne i prywatne, w tym przedsiębiorcy, zwłaszcza w przypadku świadczenia określonego rodzaju usług (np. usług finansowych, usług zdrowotnych, usług najmu itp.) zbierają dane swoich klientów, i to łącznie z żądaniem podania numeru PESEL. Jest to w Polsce niemalże już normalna praktyka, ale na jakiej podstawie prawnej te dane są potem przekazywane do innych, zwłaszcza prywatnych i centralnych baz danych, i to bez wiedzy oraz zgody zainteresowanych obywateli?

To bardzo ważna kwestia, zwłaszcza, że dane wrażliwe w Polsce zbierane są obecnie już na potęgę. Niestety, poza uprawnionymi podmiotami, jak np. organa administracji publicznej, banki i inne instytucje finansowe, ubezpieczeniowe, zdrowotne, notariusze itp., dane wrażliwe, z numerem PESEL na czele, zbierają niemal wszyscy, także podczas świadczenia innych usług, np. usług hotelowych, najmu mieszkania, wynajmu samochodów, rowerów. Ba, coraz częściej takich danych żądają także aplikacje internetowe, łącznie z żądaniem przesłania zdjęcia czy skanu dowodu osobistego! Co w takim razie daje poufność numeru PESEL, a nawet jego zastrzeżenie? Czy pana resort zamierza tak zmienić przepisy prawa, aby skutecznie uniemożliwić pobieranie w ten sposób danych wrażliwych, łącznie z penalizowaniem takich zachowań?

Z wyrazami szacunku
Adam Szejnfeld
senator RP