Podsumowanie miesięcy: lipiec-sierpień 2026 r.

Posted on 2026-09-02

Szanowni Państwo, najważniejszym wydarzeniem związanym z ochroną danych w sierpniu niewątpliwie był cyberatak na aplikację MyDr. Mógł on doprowadzić do największego zapewne w historii naruszenia bezpieczeństwa danych w historii, który – jak informuje sam podmiot przetwarzający – dotyczy blisko 19 milionów pacjentów. Dlatego niezwłocznie podjąłem decyzję o przeprowadzeniu kontroli tej firmy przez UODO. Kontrolerzy UODO sprawdzają zastosowane przez spółkę środki techniczne i organizacyjne. Ustalają również czy te zabezpieczenia były regularnie testowane pod kątem zmieniających się zagrożeń. Przedmiotem kontroli jest też sprawdzenie, czy analiza ryzyka uwzględniała możliwe zagrożenia dla przetwarzanych danych, a jej wyniki zostały zastosowane w praktyce.

Jednocześnie nieustannie przypominamy też administratorom, którzy korzystali usług tego podmiotu przetwarzającego, że również muszą zgłosić naruszenie do UODO. Do końca sierpnia liczba zgłoszeń w tej sprawie wyniosła około tysiąca. Udzieliliśmy także wsparcia administratorom, m.in. współpracując z Naczelną Izbą Lekarską. Infolinia UODO pracuje pełną parą, udzielając informacji administratorom i osobom, których dane dotyczą. Zachęcamy zarazem wszystkich do zapoznania się z odpowiedziami na najczęściej zadawane Prezesowi UODO pytania związane z tym incydentem, a także z innymi komunikatami publikowanymi na stronie UODO.

Ustawa o zarządzaniu danymi, wdrażająca unijny Akt o zarządzaniu danymi – czyli Data Act (DA) – do polskiego porządku prawnego, zaczęła już obowiązywać. Weszła w życie 23 lipca tego roku. Prezes Urzędu Ochrony Danych Osobowych jest od tej pory organem właściwym do spraw:

- usług pośrednictwa danych, o którym mowa w artykule 13 DGA;
- rejestracji organizacji altruizmu danych, o którym mowa w artykule 23 DGA;
- naruszeń obowiązków dotyczących przekazywania danych nieosobowych do państw trzecich, o których mowa w artykule 5 ustęp 14 lub artykule 31 DGA.
  Podstawowym celem Aktu o zarządzaniu danymi jest zwiększenie zaufania do dzielenia się danymi poprzez ustanowienie mechanizmów gwarantujących osobom, których dane dotyczą oraz posiadaczom danych większą kontrolę nad własnymi danymi. Nowe ramy prawne mają sprzyjać powstawaniu europejskich przestrzeni danych (np. w obszarze zdrowia, mobilności czy środowiska), usuwać bariery na rynku wewnętrznym oraz stymulować rozwój konkurencyjnej i bezpiecznej gospodarki opartej na danych, z której korzyści będą czerpać obywatele oraz przedsiębiorstwa, w tym również podmioty z sektora MŚP czy start-upy.

Wnioski, uwagi i postulaty

Przejmując nowe zadania nie ustajemy w działaniach na rzecz budowania nowych kompetencji i dostosowywania prawa do zmian związanych z obrotem danymi osobowymi.

- Uczestniczymy w pracach nad wdrożeniem w Polsce przepisów Aktu o usługach cyfrowych (DSA), które w szczególności mają wprowadzić procedury blokowania treści nielegalnych, jak również nakazywania przywrócenia dostępu do treści usuniętych bezzasadnie przez usługodawcę. Obecnie rządowy projekt ustawy trafił do komisji sejmowej. Nadal konieczne pozostaje rozszerzenie katalogu przestępstw, do których może być stosowana procedura szybkiego usunięcia treści, wprowadzenie możliwości natychmiastowej wykonalności takiej

decyzji w najpoważniejszych wypadkach, a także wzmocnienie ochrony prywatności, szczególnie w kontekście deepfake'ów.

- Zwróciliśmy uwagę, że należy doprecyzować model przechowywania danych biometrycznych funkcjonariuszy i pracowników Policji. Obowiązujące zasady retencji danych wymagają zmiany. Dane genetyczne i biometryczne pobrane od funkcjonariuszy oraz pracowników Policji są obecnie usuwane najpóźniej po pięciu latach od ustania ich stosunku służbowego albo stosunku pracy. Naszym zdaniem przyjęty model nie zapewnia pełnej zgodności z zasadami ochrony danych osobowych i standardami wynikającymi z Konstytucji RP oraz orzecznictwa Trybunału Sprawiedliwości UE. Z odpowiedzi przysłanej w sierpniu przez MSWiA wynika, że resort analizuje obecnie zgłoszone przez nas wątpliwości.
- Wskazaliśmy resortowi pracy na potrzebę uregulowania stosowania systemów sztucznej inteligencji w zatrudnieniu. Dostajemy bowiem coraz więcej sygnałów o stosowaniu w procesach rekrutacyjnych narzędzi opartych na AI. Pozwalają one na przetwarzanie danych osobowych na dużą skalę, w tym nieraz także danych szczególnych, czyli danych wrażliwych.
- Minister Edukacji Narodowej przyjęła w lipcu moją propozycję i uczniowie szkół podstawowych będą uczyli się o zagrożeniach związanych ze zjawiskiem deepfake.
- Wspieramy też media, przypominając, że choć korzystają z tzw. wyjątku dziennikarskiego, przewidzianego w art. 2 ustawy o ochronie danych osobowych, nie są całkowicie zwolnione ze stosowania przepisów RODO. Dlatego promujemy ideę kodeksu postępowania RODO dla mediów: mogłyby się w nim znaleźć zasady anonimizacji danych, archiwizacja materiałów prasowych ze stron internetowych, ochrona danych na nagraniach z dziećmi. Konieczny jest także umiar w ujawnianiu informacji, które mogą ujawnić szczegóły dotyczące osób niepełniących funkcji publicznych.
- Zmiany technologiczne wkraczają wszędzie, dlatego zareagowałem na petycję dotyczącą zmiany przepisów dotyczących wykorzystywania smartfonów na zamkniętych oddziałach szpitali psychiatrycznych. Chociaż organ nadzorczy nie ma inicjatywy ustawodawczej, ze względu na wagę problemu zadeklarowaliśmy Ministrowi Zdrowia gotowość do udzielenia

eksperckiego wsparcia w razie podjęcia przez projektodawcę prac legislacyjnych w tym właśnie obszarze. Chodzi o to, że smartfony służą nie tylko do komunikacji, ale także do nagrywania, publikowania wideo, dokonywania operacji bankowych – konieczne jest więc wskazanie bezpiecznego zakresu tych czynności w przypadku osób w ciężkich kryzysach psychicznych.

- Przekazałem uwagi dotyczące usługi „mojeIKP Junior", usługi przeznaczonej dla młodzieży w wieku od trzynastu do siedemnastu lat jako odpowiedź na potrzeby zdrowotne i systemowe spotykane w tej grupie wiekowej. W związku z faktem, że z usługi będą korzystać osoby małoletnie, wymaga ona szczególnego zapewnienia ochrony danych osobowych, w tym danych dotyczących zdrowia. Komunikacja z osobami małoletnimi musi zostać dostosowana do ich wieku, stopnia dojrzałości oraz poziomu ich świadomości.

Ochrona dzieci i mecz szachowy z WOŚP

W Senacie RP odbyła się pod koniec lipca ważna debata po tytułem „Normy, prawo i prewencja w ochronie dzieci i młodzieży w cyberprzestrzeni", zorganizowana wspólnie z Państwową Komisją do spraw przeciwdziałania wykorzystaniu seksualnemu małoletnich poniżej lat 15. Podczas tego wydarzenia wystąpiłem podkreślając konieczność ochrony danych osób małoletnich w cyberprzestrzeni. Skuteczna ochrona najmłodszych wymaga równoczesnego stosowania odpowiednich regulacji prawnych, bezpiecznych technologii, działań prewencyjnych oraz budowania właściwych norm społecznych.

Na koniec miesiąca, w siedzibie Urzędu, rozegrałem mecz szachowy wylicytowany podczas tegorocznego finału Wielkiej Orkiestry Świątecznej Pomocy. Zwycięzcą aukcji był Pan Piotr Czubaty, na co dzień inspektor ochrony danych. Całość środków zasiliła konto WOŚP. Mecz przebiegał w świetnej atmosferze. Cieszy mnie, że dzięki takim akcjom udaje się połączyć

wsparcie ważnego celu społecznego z przybliżeniem działalności Urzędu i ochrony danych osobowych.

Postępowanie naruszeniowe KE przeciw Polsce

Brak przepisów zapewniających należyty nadzór nad przetwarzaniem danych osobowych w obszarze ochrony porządku publicznego i wymiarze sprawiedliwości stał się powodem zainicjowania przez Komisję Europejską postępowania naruszeniowego przeciw Polsce. Urząd Ochrony Danych Osobowych wielokrotnie zwracał uwagę na ten problem, a ja sam już na początku roku skierowałem kompleksowe wystąpienie do ministrów spraw wewnętrznych i sprawiedliwości, informując ich o konieczności pilnego dostosowania przepisów.

Procedura naruszeniowa składa się z kilku etapów. Pierwszym, nieformalnym krokiem jest wezwanie przez Komisję Europejską do usunięcia uchybienia. Komisja Europejska w specjalnym piśmie wskazuje naruszenia prawa oraz domaga się wyjaśnień tego stanu rzeczy w wyznaczonym terminie.

Z życia EROD – warto wiedzieć

Podczas 122. posiedzenia plenarnego EROD, które odbyło się 7 lipca 2026 r., EROD przyjęła wytyczne dotyczące anonimizacji oraz wytyczne dotyczące web scrapingu w kontekście generatywnej sztucznej inteligencji. Ponadto EROD przyjęła ostateczną wersję wytycznych dotyczących przetwarzania danych osobowych za pomocą technologii

blockchain.

Kilka słów o naszych decyzjach

Chciałbym zwrócić uwagę na pierwszą decyzję organu nadzorczego o karze pieniężnej związaną z prywatnym monitoringiem. Ponad 26 tysiące zł kary ma zapłacić osoba, która nie wykonała decyzji Prezesa Urzędu Ochrony Danych Osobowych nakazującej zaprzestania przetwarzania danych osobowych za pomocą monitoringu wizyjnego, który obejmuje między innymi drogę publiczną.

Kilka wydanych w czasie letnim decyzji o karach dotyczyło tego, z czym cały czas mamy do czynienia: administratorzy danych nie przeprowadzają odpowiedniej analizy, więc nie wdrażają zabezpieczeń organizacyjnych i technicznych. W efekcie dochodzi do incydentów z danymi. Za każdym razem sprawdzamy wtedy, czy administrator pomyślał o zabezpieczeniach – i czy może pokazać na to dowody.

W lipcu opublikowaliśmy decyzje o karach za brak zabezpieczeń prowadzący do incydentów dla: kancelarii podatkowej, a także starosty i wojewódzkiego biura geodezji. Można się z nimi – i z całą argumentacją – zapoznać w serwisie internetowym UODO.

Działania UODO w sierpniu

Objęliśmy patronatem XXXV Forum Ekonomiczne w Karpaczu. Spotkałem się także z przedstawicielami środowisk ławników. Omówiliśmy możliwą współpracę przy organizacji szkoleń z zakresu ochrony danych osobowych. Pod koniec miesiąca spotkaliśmy się

natomiast z przedstawicielami branży energetycznej, w sprawie inicjatywy opracowania poradnika dla spółek kapitałowych z tego sektora w kwestii przetwarzania danych osobowych oraz możliwości stworzenia kodeksu na podstawie przepisów RODO.

W związku z wejściem w życie nowych przepisów Aktu o Sztucznej Inteligencji, opublikowaliśmy także listy pytań pomocnych przy wdrażaniu narzędzi AI – tak by działały one zgodnie z zasadami RODO. Toczy się wciąż postępowanie przed NSA w sprawie ujawnienia danych osobowych na konferencji Prokuratury Krajowej – zainicjowana skargą kasacyjną Prezesa UODO. Niedawno do postępowania tego przystąpił Rzecznik Praw Obywatelskich – popierając moją skargę.

W sierpniu także złożyłem szereg uwag i postulatów zmian legislacyjnych. Przede wszystkim do projektu nowelizacji ustawy o fundacji rodzinnej. Uważam też, że przepisy dotyczące monitoringu w izbach wytrzeźwień wymagają doprecyzowania. Zwróciłem również uwagę na zagrożenia dla prywatności związane z wykorzystywaniem inteligentnych okularów, które stają się coraz popularniejsze. Interweniowałem również w indywidualnej sprawie mieszkańca Wejherowa, który pytał w trybie dostępie do informacji publicznej o umowy zawarte przez urząd miasta z konkretną firmą. Jednak kopia tego pisma – wraz z danymi pytającego – trafiła do samej spółki – za co upomniałem Prezydenta Wejherowa.

Warto wiedzieć – nowa edycja programów

edukacyjnych UODO

Na koniec pragnę ogłosić, że rozpoczynamy nową – XVII – edycję naszych największych akcji edukacyjnych – „Twoje dane – Twoja sprawa” oraz UODO rusza w kraj. Rekrutacja do pierwszej z nich rozpoczęła się już 1 września, a zakończy z końcem października. Natomiast już na początku września wraz z pracownikami Urzędu odwiedzę Kluczbork, Opole i Śląsk, spotykając się z administratorami, inspektorami ochrony danych oraz innymi specjalistami i ekspertami działającymi w tym obszarze. W związku z początkiem roku szkolnego zachęcam również dzieci i młodzież do korzystania z aplikacji FantomApp, która pomaga bezpieczniej korzystać z internetu i skuteczniej chronić swoje dane. Przypominamy też o trwających konsultacjach w sprawie tzw. dyrektywy policyjnej, prowadzonych przez Komisję Europejską.

O wszystkich swoich działaniach na bieżąco informujemy też na stronie internetowej Urzędu. Łącznie w lipcu opublikowaliśmy 23 komunikaty, zaś w sierpniu – 24: ostatni dotyczył kary dla komornika który sam pełnił w swojej kancelarii funkcję Inspektora Ochrony Danych.