NR 2 - MARZEC 2021

NEWSLETTER RODO

Tematy artykułów:

- Pierwsze kodeksy postępowania pozytywnie zaopiniowane
- Wymagania akredytacji podmiotów monitorujących kodeksy postępowania
- Zadośćuczynienie za naruszenie ochrony danych osobowych
- Projekt decyzji stwierdzającej odpowiedni stopień ochrony w Wielkiej Brytanii
- Mechanizm one-stop-shop
- Najnowsze decyzje Prezesa UODO

Traple Konarski Podrecki & Wspólnicy

TKP

Pierwsze kodeksy postępowania pozytywnie zaopiniowane, ale jeszcze nie zatwierdzone

Prof. INP PAN dr hab. Grzegorz Sibiga, Adwokat

Prezes Urzędu Ochrony Danych Osobowych (UODO) wydał pierwsze pozytywne opinie w sprawie dwóch kodeksów postępowania.

Opinie organu nadzorczego dotyczyły projektów kodeksów postępowania, które zostały złożone do zatwierdzenia przez ten organ, tj.:

1) „Kodeksu postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych", opracowanego i złożonego przez Federację Związków Pracodawców Ochrony Zdrowia „Porozumienie Zielonogórskie";
2) „Kodeksu postępowania dla sektora ochrony zdrowia", opracowanego i złożonego przez Polską Federację Szpitali.

Zgodność z RODO zapewniona, ale z zastrzeżeniem

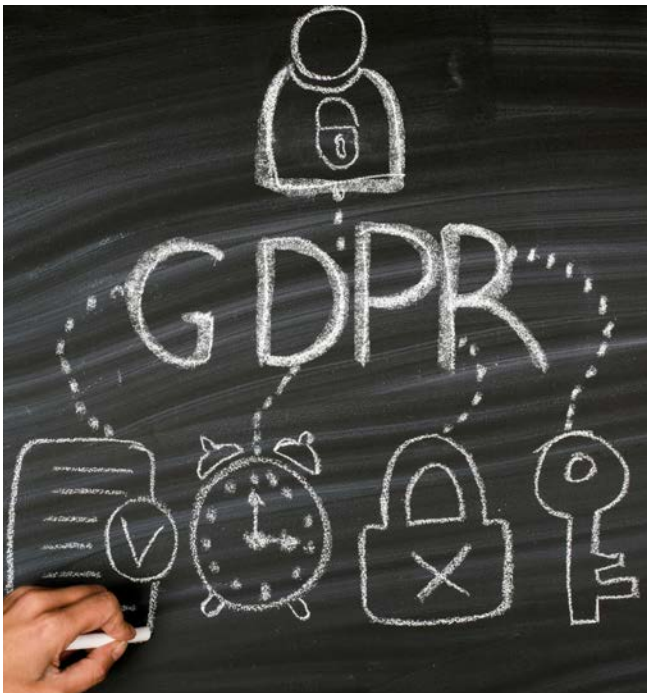
W obu opiniach Prezes UODO pozytywnie ocenił (zaopiniował) projekty kodeksów postępowania, z zastrzeżeniem kwestii monitorowania podmiotów publicznych, która musi zostać doprecyzowana w ostatecznej wersji kodeksów.

Ocena projektów kodeksów została przeprowadzona na podstawie kryteriów przedstawionych w Wytycznych 1/2019 dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679, przyjętych 4 czerwca 2019 r. przez Europejską Radę Ochrony Danych. W wyniku oceny Prezes UODO stwierdził, że oba kodeksy spełniają kryteria ustalone w tych wytycznych, tj. zaspokajają określone potrzeby ustanowienia kodeksu, ułatwiają skuteczne stosowanie RODO[1], doprecyzowują stosowanie RODO oraz zapewniają wystarczające zabezpieczenia. Należy bowiem pamiętać, że celem kodeksu postępowania jest pomoc we właściwym stosowaniu RODO, z uwzględnieniem specyfiki różnych sektorów i szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

Do uzupełnienia: monitorowanie podmiotów publicznych oraz podmiot monitorujący

Z opinii Prezesa UODO wynika jednak, że w niewystarczający sposób ujęto monitorowanie przestrzegania kodeksu przez podmioty sektora publicznego będące członkami kodeksu oraz że brakuje akredytowanego podmiotu monitorującego.

Kodeksy obejmujące podmioty sektora publicznego nie podlegają obowiązkowi wskazania podmiotu monitorującego, ale muszą zawierać skuteczny mechanizm monitorowania. Cel taki można osiągnąć poprzez dostosowanie obowiązujących wymogów w zakresie audytu, tak aby obejmowały one monitorowanie kodeksu. Zdaniem organu nadzorczego przedłożone projekty nie zawierały tego elementu albo zawierały w niewystarczającym stopniu. Te części projektów kodeksów mają jeszcze podlegać uzupełnieniu, co ma stanowić przedmiot dalszego postępowania przed Prezesem UODO.



[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).

Niezależnie od tego, aby kodeks postępowania został zatwierdzony, musi już funkcjonować podmiot monitorujący ten kodeks, tzn. taki podmiot musi zostać akredytowany przez Prezesa UODO jako ten, który jest w stanie skutecznie monitorować kodeks. Ponieważ nie można zatwierdzić kodeksu bez wskazanego, akredytowanego do konkretnego kodeksu podmiotu monitorującego, Prezes UODO wydał opinie właśnie po to, aby umożliwić wystąpienie przez podmiot monitorujący o akredytację. Kodeks postępowania zostanie zatem ostatecznie zatwierdzony dopiero po wydaniu przez Prezesa UODO certyfikatu akredytującego dla podmiotu monitorującego ten konkretny kodeks.

Wymagane zatwierdzenie, a nie tylko opinia

Wydanie przez organ nadzorczy opinii jest przewidziane zarówno w RODO, jak i w ustawie o ochronie danych osobowych[2] i służy ustaleniu zgodności projektu kodeksu postępowania z RODO. Należy jednak zauważyć, że w art. 40 ust. 5 zd. 2 RODO przewiduje się, że organ nadzorczy nie tylko wydaje opinię o tej zgodności, lecz także zatwierdza projekt kodeksu postępowania, jeżeli uzna, że stanowi on odpowiednie zabezpieczenie.

Zatem postępowanie wszczęte wnioskiem organizacji (wystąpieniem o zatwierdzenie kodeksu) do Prezesa UODO zostanie zakończone dopiero w przypadku zatwierdzenia kodeksu postępowania. Ponieważ do postępowania w przedmiocie projektu kodeksu stosuje się przepisy Kodeksu postępowania administracyjnego[3] z odmiennościami określonymi w ustawie o ochronie danych osobowych (tak art. 7 ust. 1 tej ustawy), to wydaje się, że zatwierdzenie powinno nastąpić w drodze decyzji administracyjnej Prezesa UODO. Organ nadzorczy będzie związany treścią decyzji zatwierdzającej od chwili jej doręczenia wnioskującej organizacji. Dla stosowania kodeksu postępowania przez podmioty nim objęte istotna natomiast pozostanie data uprawomocnienia się decyzji zatwierdzającej kodeks. Jednak już obecnie – jak podkreśla Prezes UODO – „podmioty medyczne, chcące zapewnić pacjentom wysoki poziom ochrony ich danych osiągnięty w projekcie kodeksu […], mogą rozpocząć dostosowywanie do ich postanowień", co oznacza możliwość przygotowywania się tych podmiotów do stosowania postanowień projektu kodeksu, który zostanie zatwierdzony w przyszłości, ale zapewne już bez zmian w jego treści oprócz części dotyczącej monitorowania.

[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r., poz. 1781).
[3] Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2020 r., poz. 256 z późn. zm.).

Prezes UODO publikuje wymagania akredytacji podmiotów monitorujących kodeksy postępowania

dr inż. Andrzej Kaczmarek, CISA

Prezes UODO opublikował wymogi akredytacji podmiotów monitorujących kodeksy postępowania, bardzo oczekiwane przez zrzeszenia i inne podmioty reprezentujące administratorów danych i podmioty przetwarzające należące do sektora prywatnego. Publikacja ta umożliwia zainteresowanym podmiotom rozpoczęcie procedury akredytacyjnej w zakresie pełnienia roli podmiotu monitorującego kodeksy i uzyskanie akredytacji, co jest niezbędne do zatwierdzenia przez Prezesa UODO przedłożonych mu kodeksów. Opublikowany dokument zawiera wymogi, jakie musi spełniać podmiot monitorujący w zakresie wykazania swojej niezależności i posiadania wiedzy fachowej w dziedzinie będącej przedmiotem kodeksu, a także wymagania dotyczące procedur, jakimi powinien się wykazać. Pozwoli to Prezesowi UODO na ocenę zdolności kandydatów wnioskujących o akredytację w zakresie realizacji zadań podmiotu monitorującego i ponoszenia wiążącej się z tym odpowiedzialności. Dokument przed publikacją został zaopiniowany przez Europejska Radę Ochrony Danych zgodnie z mechanizmem spójności, o którym mowa w art. 63 RODO.

Wstęp:

Zgodnie z art. 40 ust 5 RODO[1] organ nadzorczy odpowiedzialny w kraju członkowskim za stosowanie RODO może zatwierdzić kodeks postępowania przedłożony przez zrzeszenie lub inne podmioty reprezentujące określone kategorie administratorów lub podmiotów przetwarzających dane osobowe, jeśli uregulowane w nim zostaną mechanizmy pozwalające na monitorowanie jego stosowa-nia przez podmioty, które zobowiązały się do jego przestrzegania, o czym jest mowa w art. 40 ust. 4 RODO. Funkcję podmiotu monitorującego z kolei – zgodnie z art. 41 ust. 1 – może pełnić podmiot, który dysponuje odpowiednim poziomem wiedzy fachowej w dziedzinie będącej przedmiotem kodeksu i został w tym celu akredytowany przez właściwy organ nadzorczy.

Podmiot wnioskujący o akredytację może zostać akredytowany, jeżeli:

w sposób satysfakcjonujący wykazał właściwemu organowi nadzorczemu swoją niezależność i wiedzę fachową w dziedzinie będącej przedmiotem kodeksu;

- dysponuje procedurami, które pozwalają mu ocenić zdolność konkretnych administratorów i podmiotów przetwarzających do stosowania kodeksu, monitorować przestrzeganie przez nich jego przepisów oraz okresowo dokonywać przeglądu jego funkcjonowania;
- dysponuje procedurami i strukturami, które pozwalają rozpatrywać skargi na naruszenie kodeksu przez administratora lub podmiot przetwarzający bądź na sposób wdrożenia lub wdrażania kodeksu przez administratora lub podmiot przetwarzający oraz które umożliwiają zapewnienie przejrzystości tych procedur i struktur dla osób, których dane dotyczą, i opinii publicznej;
- w sposób satysfakcjonujący wykazał właściwemu organowi nadzorczemu, że jego zadania i obowiązki nie powodują konfliktu interesów.

Ponadto – zgodnie z art. 57 ust. 1 lit. p RODO – organ nadzorczy zobowiązany jest do opracowania i publikacji wymogów akredytacji podmiotów monitorujących kodeksy postępowania. Projekt przedmiotowych wymogów został przez Prezesa UODO opracowany i opublikowany[2] 9 czerwca 2020 r. W tym samym dniu rozpoczęły się społeczne konsultacje projektu, które zakończyły się 5 lipca 2020 r. W wyniku zebranych w trakcie konsultacji uwag projekt został zmodyfikowany i jako wersja 2.0 z dnia 24 sierpnia 2020 r. – zgodnie z art. 41 ust. 3 RODO w celu zapewnienia mechanizmu spójności, o którym mowa w art. 63 RODO – przedstawiony Europejskiej Radzie Ochrony Danych (EROD) do zaopiniowania. Opinia EROD w przedmiotowej sprawie[3] została wydana 7 grudnia 2020 r. W dniu 27 stycznia 2021 r. Prezes UODO opublikował ostateczną wersję wymogów akredytacji zatytułowaną „Wymogi akredytacji podmiotów monitorujących kodeksy postępowania.

[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).
[2]Wymogi akredytacji podmiotów monitorujących kodeksy postępowania. Wersja 1.0 z dnia 8 czerwca 2020 r. Zob. załącznik na stronie: https://uodo.gov.pl/pl/138/1559 (dostęp: 2.03.2021).
[3] Opinion 31/2020 on the draft decision of the competent supervisory authority of Poland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR. Zob. https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-312020-draft-decision-competent_en (dostęp: 2.03.2021).

13 stycznia 2021 r. Wersja 3.0" (dalej: „Wymogi")[4] Opublikowanie ww. wymogów akredytacji pozwoliło tym samym na organizacyjne domknięcie modelu, w jakim przewidziane jest funkcjonowanie kodeksów postępowania.

Co nowego?

Przyjęcie i opublikowanie przez Prezesa UODO wymogów akredytacji podmiotów monitorujących umożliwia:

- występowanie przez zainteresowane podmioty z wnioskami o uzyskanie akredytacji w zakresie pełnienia roli podmiotu monitorującego przestrzeganie określonego kodeksu postępowania;
- wskazanie w kodeksie postępowania akredytowanego podmiotu, któremu powierza się monitorowanie jego przestrzegania, co jest warunkiem koniecznym do tego, by Prezes UODO mógł dany kodeks zatwierdzić;
- domknięcie od strony organizacyjnej przez Prezesa UODO procedur niezbędnych do funkcjonowania kodeksów postępowania w pełnym modelu, jaki przewiduje art. 40 i 41 RODO.

Stan dotychczasowy

Tworzenie kodeksów postępowania w celu ułatwienia stosowania przepisów o ochronie danych osobowych możliwe było również w okresie obowiązywania dyrektywy 95/46/WE o ochronie danych osobowych. Artykuł 27 ww. dyrektywy stanowił, że państwa członkowskie i Komisja zachęcają do opracowywania kodeksów postępowania, których celem będzie usprawnienie procesu prawidłowego wprowadzania krajowych przepisów przyjętych przez państwa członkowskie na mocy dyrektywy, z uwzględnieniem szczególnych cech różnych sektorów. Polska ustawa o ochronie danych osobowych z 29 sierpnia 1997 r. nie wprowadziła jednak implementacji przepisów dyrektywy 95/46/WE dotyczących tworzenia kodeksów postępowania. Dochodziło jednak wówczas do zawierania porozumień między GIODO a rozmaitymi organizacjami i instytucjami, dotyczących dobrych praktyk w zakresie ochrony danych. Oddolne inicjatywy w przedmiocie zawierania tych porozumień świadczyły o dużej potrzebie różnych środowisk rozwiązywania problemów związanych z przetwarzaniem danych osobowych, w szczególności tych charakterystycznych dla danego sektora.

Stan obecny

Przepisy RODO, które wprost znajdują zastosowanie w państwach członkowskich, poświęcają znacznie więcej uwagi kodeksom postępowania (art. 40 i 41 oraz motywy 98 i 99 RODO). Wprowadzony został obowiązek ich zatwierdzania przez organ nadzorczy oraz konsultowania z innymi organami oraz EROD, jeśli projekt kodeksu, zmiany lub rozszerzenia dotyczy czynności przetwarzania prowadzonych w kilku państwach członkowskich. Większa jest również rola takich kodeksów, gdyż ich stosowanie uznawane będzie za potwierdzenie zgodności (compliance) z przepisami o ochronie danych osobowych. Dotyczy to potwierdzenia spełnienia warunków rozporządzenia w zakresie ogólnych obowiązków administratora (art. 24 ust. 3), powierzenia przetwarzania (art. 28 ust. 5), bezpieczeństwa przetwarzania (art. 32 ust. 3), oceny skutków (art. 35 ust. 8), a także przekazywania danych do państw trzecich i organizacji międzynarodowych (art. 46 ust. 2 lit. e). Stąd też duże zainteresowanie różnych podmiotów, gównie stowarzyszeń, związków, izb itp., które już opracowały takie kodeksy i złożyły wnioski o ich zatwierdzenie bądź zadeklarowały inicjatywę ich opracowania. Obecnie (wg stanu na dzień 25 lutego 2021 r.) osiem opracowanych kodeksów postępowania oficjalnie czeka już na zatwierdzenie przez Prezesa UODO, osiem innych zaś zgłoszonych zostało jako inicjatywy będące w trakcie opracowywania lub konsultacji . W odniesieniu do dwóch kodeksów postępowania z listy kodeksów zgłoszonych do zatwierdzenia w dniu 23 lutego 2021 r. Prezes UODO wydał już pozytywną opinię, stwierdzając, że stanowią one odpowiednie zabezpieczenia w zakresie ochrony danych przewidziane w art. 40 ust. 5 RODO[6].

[4] Wymogi akredytacji podmiotów monitorujących kodeksy postępowania. 13 stycznia 2021 r. Wersja 3.0, Urząd Ochrony Danych Osobowych. Zob. https://uodo.gov.pl/pl/138/1861 (dostęp: 2.03.2021).

[5]Lista wniosków złożonych do Prezesa UODO o zatwierdzenie kodeksów postępowania dostępna jest na stronie: https://uodo.gov.pl/pl/426/1109; lista zgłoszonych inicjatyw dotyczących opracowania kodeksów dostępna jest na stronie: https://uodo.gov.pl/pl/426/1108 (dostęp: 2.03.2021).

[6] Zob. komunikat Prezesa UODO o wydaniu pozytywnej opinii dla „Kodeksu postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych" opracowanego przez Federację Związków Pracodawców Ochrony Zdrowia „Porozumienie Zielonogórskie" oraz projektu „Kodeksu postępowania dla sektora ochrony zdrowia" opracowanego przez Polską Federację Szpitali: https://www.uodo.gov.pl/pl/138/1923 (dostęp: 2.03.2021).

Wydanie pozytywnej opinii przez Prezesa UODO o zgodności przedłożonych kodeksów postępowania nie jest jednak tożsame z ich zatwierdzeniem. Brak zatwierdzenia kodeksów postępowania sprawia zaś, że ich stosowanie nie wywołuje skutków, o których mowa wyżej, i nie mogą być one uznane jako skuteczne narzędzia rozliczalności ani dla administratorów, ani dla podmiotów przetwarzających. Jak wskazano w motywie 77 i art. 24 ust. 3 RODO, stosowanie zatwierdzonego kodeksu postępowania przewidziano m.in. jako narzędzie służące wykazaniu przez administratora lub podmiot przetwarzający przestrzegania określonych części rozporządzenia, zasad w nim określonych bądź całości rozporządzenia [7].

Dalsze prace

Przedłożone Prezesowi UODO projekty kodeksów nie mogły być jednak zatwierdzone, gdyż zgodnie z art. 40 ust. 4 RODO wymagane jest, aby wskazany został akredytowany podmiot odpowiedzialny za monitorowanie przestrzegania kodeksu. Jak wskazano w wytycznych 1/2019 EROD[8]: „W projekcie kodeksu, który obejmuje czynności przetwarzania prowadzone przez prywatne, niepubliczne organy lub podmioty, należy również wskazać podmiot monitorujący […]. W tym celu podmiot lub podmioty monitorujące muszą zostać akredytowane przez właściwy organ nadzorczy zgodnie z art. 41 ust. 1 RODO".

Oznacza to, że opublikowane przez Prezesa UODO Wymogi zniosły barierę, która dotychczas uniemożliwiała właściwym podmiotom (wskazywanym w projektach kodeksów jako podmioty monitorujące) wystąpienie do Prezesa UODO z wnioskiem o uzyskanie wymaganej akredytacji.

Opublikowane w dniu 27 stycznia 2021 r. Wymogi uwzględniają większość uwag zgłoszonych przez EROD w opinii 31/2020 z dnia 7 grudnia 2020 r., o której mowa wyżej. Dotyczyły one głównie § 3 projektu dotyczącego szczegółowych wymogów akredytacji podmiotu monitorującego kodeks postępowania w zakresie punktów odnoszących się do wykazania niezależności (organizacyjnej, ekonomicznej, w tym zapewniania ciągłości działania), wiedzy specjalistycznej, przeciwdziałania konfliktom interesów, przejrzystości rozpatrywania skarg, komunikacji z organem nadzorczym, a także procedur okresowego przeglądu monitorowanego kodeksu. W większości przypadków wydana opinia wskazywała na drobne nieścisłości w odniesieniu do określonych punktów, zalecając ich rozszerzenie, wyjaśnienie, doprecyzowanie lub przeredagowanie.

Zaznaczyć należy, że przedstawione w opublikowanym dokumencie wymagania dotyczące akredytacji w większości przypadków nie wskazują konkretnych rozwiązań, jakie mają być zastosowane, aby określone wymogi zostały spełnione, lecz głównie cel, jaki powinien być poprzez ich zastosowanie osiągnięty. Przykładem jest § 3 pkt 1.2.3, który stanowi, że: „Podmiot monitorujący dysponuje procedurami zapewniającymi jego długoterminową stabilność finansową. Utrata jednego lub większej liczby źródeł finansowania nie może mieć wpływu na jego niezależność. Dlatego w przyjętych zasadach finansowania uwzględnia mechanizmy zabezpieczenia finansowego m.in. w przypadku zmniejszenia liczby członków kodeksu lub organizacji twórcy kodeksu lub znaczących opóźnień w uiszczaniu opłat". Wydaje się jednak, że trudno byłoby zaproponować jakieś inne wymagania w zakresie zapewnienia długoterminowej stabilności finansowej w ramach samoregulacji bez rozwiązań administracyjnych, np. w postaci utworzenia funduszu gwarantującego niezbędne zabezpieczenie finansowe.

[7] Zob. w szczególności art. 24 ust. 3, art. 28 ust. 5, art. 32 ust. 3, art. 35 ust. 8, a także art. 46 ust. 2 lit. e RODO.

[8]Wytyczne 1/2019 dotyczące kodeksów postępowania podmiotów monitorujących zgodnie z rozporządzeniem 2016/679. Wersja 2.0, przyjęte przez Europejska Radę Ochrony Danych: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_pl.pdf (dostęp: 2.03.2021).

Opublikowana wersja wymogów akredytacyjnych co do zasady jest zgodna z wytycznymi 1/2019 EROD dotyczącymi kodeksów postępowania i podmiotów monitorujących […], wersja 2.0 z 4 czerwca 2019 r. Niemniej pewne sformułowania mogą dalej budzić wątpliwości interpretacyjne. Tak np. w § 3 pkt 6, który dotyczy komunikacji z właściwym organem nadzorczym, w pkt 6.2.1–6.2.8 szczegółowo wymieniono elementy, jakie powinny się znaleźć w sprawozdaniu podmiotu monitorującego do organu nadzorczego. Wątpliwość dotyczy ograniczenia w sprawozdaniu informacji o audytach jedynie do audytów przeprowadzonych w następstwie stwierdzenia naruszenia, z pominięciem natomiast informacji i wniosków wynikających z pozostałych rodzajów audytów wykonywanych w ramach monitorowania.

Wprowadzone w § 3 pkt 6.2.6 i § 3 pkt 6.2.8 ograniczenie do informacji i wniosków z audytów tylko do tych audytów, które przeprowadzono w następstwie stwierdzenia naruszenia kodeksu, jest również sprzeczne z punktem 78 Wytycznych 1/2019 EROD dotyczących kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem , który brzmi:

„Proponowane ramy podmiotu monitorującego muszą uwzględniać skuteczne przekazywanie informacji właściwemu organowi nadzorczemu i innym organom nadzorczym na temat **wszelkich działań** prowadzonych przez podmiot monitorujący w odniesieniu do kodeksu. Informacje te mogą obejmować decyzje dotyczące działań podejmowanych w przypadku naruszenia kodeksu przez członka, który zobowiązał się do jego stosowania, przedstawianie okresowych sprawozdań dotyczących kodeksu bądź informacje uzyskane w ramach **przeglądu kodeksu lub ustalenia z jego audytu**". W ww. wytycznych nie znajdujemy m.in. ograniczenia do informowania wyłącznie o wynikach audytów przeprowadzonych w następstwie stwierdzonych naruszeń.

Pomimo wymienionych wyżej drobnych usterek i nieścisłości należy oczekiwać, że w najbliższym czasie do Prezesa UODO wpłyną pierwsze wnioski o akredytację podmiotów monitorujących i spełnione zostaną warunki umożliwiające zatwierdzenie pierwszych kodeksów postępowania. To z kolei podniesie na wyższy poziom ochronę danych w przypadku podmiotów, które zobowiążą się do stosowania kodeksu.

[9]Ibidem.

Zadośćuczynienie za naruszenie ochrony danych osobowych (art. 82 RODO) – wyrok sądu

Xawery Konarski, Adwokat

Wstęp

W dniu 6 sierpnia 2020 r. Sąd Okręgowy w Warszawie wydał wyrok zasądzający zadośćuczynienie za naruszenie ochrony danych osobowych (sygn. akt XXV C 2596/19). Podstawą materialnoprawną jego wydania był art. 82 ust. 1 RODO, zgodnie z którym „każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia (tj. RODO), ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę".

Stan faktyczny

Powódka była właścicielką pojazdu, który uczestniczył w kolizji drogowej i który był ubezpieczony w zakresie OC u pozwanego (towarzystwo ubezpieczeń). Podczas kolizji powódka nie była osobą kierującą pojazdem. W trakcie postępowania w przedmiocie likwidacji szkody pracownik pozwanego przesłał do poszkodowanego skany dokumentacji dotyczącej szkody, które nie zostały zanonimizowane, tj. zawierały imię i nazwisko powódki, jej adres zamieszkania, numer PESEL, numer telefonu, a także dane pojazdu. Zakład ubezpieczeń zawiadomił powódkę o powyższym incydencie.
Zgodnie z zawartymi w pozwie twierdzeniami powódki wyżej wymienione zdarzenie naraziło ją na „ciągły stres", ponieważ obawiała się, w jaki sposób jej dane osobowe zostaną wykorzystane. Z tych przyczyn powódka zażądała zasądzenia kwoty 10 tys. zł tytułem zadośćuczynienia za doznaną krzywdę.

Rozstrzygnięcie Sądu Okręgowego

Sąd Okręgowy stwierdził, że dane personalne (osobowe) powódki, jako właściciela pojazdu uczestniczącego w kolizji drogowej, mogły zostać – co do zasady – udostępnione osobie poszkodowanej w tej kolizji, mimo że powódka nie kierowała pojazdem podczas tego zdarzenia. Podstawę do przekazania przez pozwanego takich danych powódki stanowiły przepisy art. 29 ust. 6 ustawy o działalności ubezpieczeniowej i reasekuracyjnej[1] w związku z art. 44 ust. 12 pkt 4 Prawa o ruchu drogowym[2].

Równocześnie jednak Sąd uznał, że pozwany ubezpieczyciel uprawniony był do przekazania poszkodowanemu tylko danych obejmujących imię i nazwisko powódki oraz jej miejsce zamieszkania, a nie był już uprawniony do przekazania informacji dotyczących numeru PESEL i numeru telefonu powódki. Dane te nie były bowiem niezbędne do dochodzenia roszczeń związanych z doznaną szkodą. Przekazanie tych dodatkowych informacji wykraczało więc poza upoważnienie ustawowe wynikające z przywołanych wyżej przepisów, a zatem było bezprawne. Z uwagi na profesjonalny charakter działania pozwanego towarzystwa ubezpieczeń należało mu również przypisać winę w zakresie nadmiarowego udostępnienia danych – wyżej wymienione akty prawne i wynikający z nich dopuszczalny zakres przekazania danych powinny być bowiem dobrze znane przedstawicielom pozwanego, dokonującym przekazania dokumentacji szkodowej poszkodowanemu w kolizji drogowej.

[1] Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (t.j. Dz. U. z 2020 r., poz. 895, z późn. zm.).
[2] Ustawa z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (t.j. Dz. U. z 2020 r., poz. 110, z późn. zm.).

Stwierdzenie elementu bezprawności i winy nie przesądza jeszcze automatycznie o zasadności roszczenia o zadośćuczynienie. Konieczne jest bowiem dodatkowo uznanie, że doszło do powstania po stronie pozwanej szkody niemajątkowej (krzywdy). Zdaniem Sądu tak było w rozstrzyganej sprawie. Na skutek incydentu z udostępnieniem danych osobowych powódki utraciła ona poczucie bezpieczeństwa, zaczęła odczuwać długotrwały lęk związany z możliwością nieuprawnionego wykorzystania jej danych osobowych przez inne osoby, m.in. poprzez dokonanie w imieniu powódki czynności bankowych lub nawiązywanie z nią niechcianych połączeń telefonicznych. Przeprowadzone postępowanie dowodowe nie wykazało jednak, aby dane osobowe powódki (PESEL, numer telefonu) zostały upublicznione lub wykorzystane w sposób niezgodny z prawem przez osobę niepowołaną. Powódka sama przyznała, że osoba poszkodowana w wypadku, której przekazano dane powódki, nie kontaktowała się z nią telefonicznie. Nie doświadczyła ona również żadnych innych negatywnych konsekwencji związanych z udostępnieniem jej danych osobowych. Oprócz deklarowanych przez powódkę obaw związanych z możliwością bezprawnego posłużenia się jej danymi osobowymi przez osobę trzecią powódki nie spotkały więc żadne dalsze konsekwencje. Z tych przyczyn Sąd uznał, że krzywda wyrządzona powódce na skutek naruszenia jej danych osobowych okazała się zatem niewielka, i ograniczył – w stosunku do żądania pozwu – zasądzone zadośćuczynienie **(1,5 tys. zł w miejsce 10 tys. zł, których domagała się powódka).**

Znaczenie wyroku Sądu Okręgowego

Analizowany wyrok jest jednym z pierwszych (o ile nie pierwszym) orzeczeń wydanych na podstawie art. 82 RODO. To, co w nim najistotniejsze, to uznanie przez Sąd, że przesłanki odpowiedzialności cywilnoprawnej za naruszenie ochrony danych osobowych na gruncie RODO są takie same jak w przypadku naruszenia dóbr osobistych (art. 23 k.c.)[3]. Dotyczy to również warunków przyznania zadośćuczynienia za doznaną w ten sposób krzywdę (art. 448 k.c.). Tym samym osoby dochodzące odpowiedzialności na podstawie art. 82 RODO mogą w pełnym zakresie skorzystać z dorobku orzeczniczego wypracowanego na gruncie spraw, których podstawą były przepisy art. 23 i 448 k.c.

[3] Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j. Dz. U. z 2020 r., poz. 1740, z późn. zm.; dalej: „k.c.").

Komisja Europejska przedstawiła projekt decyzji stwierdzającej odpowiedni stopień ochrony w Wielkiej Brytanii

Katarzyna Syska, Adwokatka

Komisja Europejska opublikowała projekt decyzji stwierdzającej odpowiedni stopień ochrony danych w Wielkiej Brytanii – chodzi tu o decyzję, o której mowa w art. 45 RODO[1]. Jeśli decyzja zostanie przyjęta, administratorzy i podmioty przetwarzające z UE (i z EOG) będą mogli nadal przekazywać dane osobowe podmiotom z Wielkiej Brytanii bez ograniczeń i bez spełniania dodatkowych wymogów. Natomiast jeśli decyzja nie zostanie przyjęta, to przy przekazywaniu danych osobowych do Wielkiej Brytanii trzeba będzie polegać na mechanizmach przekazywania danych określonych w art. 46 RODO, takich jak standardowe klauzule ochrony danych lub wiążące reguły korporacyjne, lub na wyjątkach w szczególnych sytuacjach, określonych w art. 49 ust. 1 RODO.

Komisja Europejska poświęciła około roku na analizę ram prawnych dotyczących ochrony danych w Wielkiej Brytanii i stwierdziła, że system prawny i regulacyjny spełnia unijne wymogi w zakresie ochrony danych. W tym kontekście Komisja Europejska wzięła pod uwagę, że w Wielkiej Brytanii obowiązuje Ogólne Rozporządzenie o Ochronie Danych Wielkiej Brytanii (UK GDPR), które jest zasadniczo zbieżne z RODO.

Jest to pierwszy projekt decyzji stwierdzającej odpowiedni stopień ochrony, który zawiera przepis wymagający ponownego przeglądu adekwatności brytyjskiego systemu prawnego w ciągu czterech lat od przyjęcia decyzji. Jeśli po tym czasie Komisja Europejska nie potwierdzi ponownie odpowiedniości stopnia ochrony w Wielkiej Brytanii, decyzja ta wygaśnie i do Wielkiej Brytanii nie będzie już można przekazywać danych osobowych na tej podstawie.

.

Aktualnie, od 1 stycznia 2021 r. do maksymalnie 30 czerwca 2021 r., trwa okres przejściowy, podczas którego Wielka Brytania jest traktowana jako zapewniająca odpowiedni stopień ochrony, w związku z czym można kontynuować przekazywanie danych do tego państwa bez ograniczeń i dodatkowych warunków. Tymczasowe uznanie odpowiedniości na okres przejściowy wynika z umowy o handlu i współpracy między UE a Wielką Brytanią. Jeżeli decyzja zostanie przyjęta, to tymczasowe uznanie odpowiedniości wygaśnie i zamiast tego będzie miała zastosowanie decyzja stwierdzająca odpowiedni stopień ochrony.

Co do projektu decyzji wypowiedzą się Europejska Rada Ochrony Danych oraz Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) Parlamentu Europejskiego, które wydadzą niewiążące opinie. Decyzja zostanie formalnie przyjęta zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2 RODO, tj. po przyjęciu pozytywnej opinii przez komitet doradczy składający się z przedstawicieli państw członkowskich UE.

[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).

Dopuszczalność zbierania przez pracodawcę informacji o pobycie pracowników za granicą

dr Iga Małobęcka-Szwast, LL. M.

Wstęp

Sąd Okręgowy w Olsztynie w wyroku z dnia 29 stycznia 2021 r. (sygn. akt IV Pa 79/20) potwierdził dopuszczalność zbierania przez pracodawcę informacji o pobycie pracowników za granicą i zobowiązywania ich do przekazywania takich informacji w stanie epidemii SARS-CoV-2. Wyrok jest prawomocny.

Stan faktyczny sprawy

W wyroku sąd oddalił apelację Piotra G., byłego pracownika dużego przedsiębiorstwa z branży spożywczej, który został zwolniony w trybie dyscyplinarnym ze względu na zatajenie przed pracodawcą faktu odbycia podróży zagranicznej w początkowym okresie epidemii wywołanej wirusem SARS-CoV-2. Były pracodawca Piotra G. w drodze zarządzenia zobowiązał wszystkich pracowników do informowania o wyjazdach zagranicznych w celu zapewnienia bezpieczeństwa w zakładzie pracy oraz, w efekcie, ciągłości działania przedsiębiorstwa.

Piotr G. nie zgodził się z decyzją byłego pracodawcy i wystąpił przeciwko niemu z powództwem do Sądu Rejonowego w Bartoszycach. Domagał się najpierw przywrócenia go do pracy, a następnie, po zmodyfikowaniu treści pozwu, odszkodowania za niezgodne z prawem rozwiązanie umowy o pracę. Sąd Rejonowy w Bartoszycach oddalił powództwo Piotra G., wskazując, że pracownik ma obowiązek przestrzegać przepisów, zasad BHP oraz zasad współżycia społecznego w zakładzie pracy. W uzasadnieniu wyroku podkreślono, że w stanie epidemii pracodawcy muszą łączyć prawa i obowiązki przewidziane w przepisach Kodeksu pracy z tymi wynikającymi z Ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych.

Sąd pierwszej instancji wskazał również, że wprawdzie sposób spędzania dni wolnych od pracy jest prywatną sprawą zatrudnionych, ale każdy pracodawca ma obowiązek zapewnić bezpieczeństwo swoim pracownikom. Z tego względu uznał za zasadne pytanie pracownika przez pracodawcę, czy w ostatnim czasie nie przebywał on w miejscu, gdzie występują przypadki zakażenia wirusem SARS-CoV-2. Kłamstwo Piotra G. uniemożliwiło pracodawcy podjęcie działań w celu spełnienia wspomnianego obowiązku.

Sąd stwierdził, że Piotr G., okłamując swojego pracodawcę i nie stosując się do wydanego przez niego zarządzenia, dopuścił się ciężkiego naruszenia podstawowych obowiązków pracowniczych, co uzasadniało rozwiązanie umowy bez wypowiedzenia. Sąd zwrócił uwagę, że kłamstwo Piotra G. miało bezpośredni wpływ na zdrowie i życie wszystkich pracowników oraz uniemożliwiło pracodawcy podjęcie czynności, które by ich zabezpieczały.

Piotr G. odwołał się od tego wyroku do Sądu Okręgowego w Olsztynie, który przychylił się do stanowiska sądu pierwszej instancji i w rezultacie oddalił jego apelację. Sąd drugiej instancji potwierdził jednocześnie, że pracodawca ma prawo wymagać od zatrudnionych dostarczania mu informacji, które mają pomóc w zapewnieniu bezpieczeństwa innych osób znajdujących się na terenie zakładu pracy.

Komentarz

Wyrok Sądu Okręgowego w Olsztynie potwierdza, że pracodawcy w czasie epidemii wywołanej wirusem SARS-CoV-2 mają prawo wymagać od osób zatrudnionych informacji o miejscu ich pobytu podczas urlopu w celu zapewnienia bezpieczeństwa pozostałym pracownikom oraz, w efekcie, ciągłości działania zakładu pracy.

Mechanizm kompleksowej współpracy (one-stop-shop) w świetle opinii rzecznika generalnego w sprawie C-645/19

dr Iga Małobęcka-Szwast, LL.M.

Wstęp

13 stycznia 2021 r. rzecznik generalny M. Bobek wydał opinię w sprawie C-645/19: Facebook Ireland Limited, Facebook Inc., Facebook Belgium BVBA (Facebook) przeciwko Gegevensbeschermingsautoriteit (belgijski organ nadzorczy). Dotyczy ona mechanizmu kompleksowej współpracy (one-stop shop) oraz zakresu kompetencji organu wiodącego i innych organów nadzorczych związanych ze sprawą na gruncie RODO. Kwestia, którą musi rozstrzygnąć jeszcze Trybunał Sprawiedliwości UE (TSUE), ma kluczowe znaczenie dla podmiotów dokonujących transgranicznego przetwarzania danych w ramach UE (art. 4 pkt 23 RODO).

Stan faktyczny sprawy

Sprawa sięga 2015 r., kiedy to belgijski organ nadzorczy wszczął postępowanie sądowe przeciwko Facebookowi. Zwrócił się on do sądu o nakazanie Facebookowi zaprzestania umieszczania plików cookie na urządzeniach użytkowników Internetu bez ich zgody oraz zaprzestania gromadzenia danych w nadmierny sposób, gdy przeglądają oni stronę internetową w domenie Facebook.com lub strony internetowe podmiotów trzecich, w tym za pośrednictwem wtyczek społecznościowych i pikseli Facebooka.

Postępowanie, które toczy się obecnie przed Sądem Apelacyjnym w Brukseli, zostało ograniczone do spółki Facebook Belgium BVBA – we wcześniejszym orzeczeniu Sąd Apelacyjny w Brukseli uznał, że nie jest właściwy do rozpoznania powództw wniesionych przeciwko Facebook Inc. i Facebook Ireland Ltd.

W niniejszej sprawie Facebook stoi na stanowisku, że wraz z rozpoczęciem stosowania RODO, w maju 2018 r., belgijski organ nadzorczy utracił kompetencje umożliwiające kontynuowanie postępowania sądowego w sprawie naruszenia RODO w związku z transgranicznym przetwarzaniem danych przez spółkę. W ocenie spółki jedynym właściwym organem nadzorczym w tym przypadku jest organ nadzorczy głównej jednostki organizacyjnej Facebooka w UE. Główna jednostka organizacyjna administratora w UE znajduje się w Irlandii (Facebook Ireland Ltd.) i z tej przyczyny to organ nadzorczy tego kraju (Irish Data Protection Commission) pełni funkcję organu wiodącego w rozumieniu art. 56 RODO

W kontekście tego sporu Sąd Apelacyjny w Brukseli zawiesił postępowanie i zwrócił się do TSUE z pytaniem, czy RODO i przewidziany w nim mechanizm one-stop-shop uniemożliwia organowi nadzorczemu państwa członkowskiego wszczęcie postępowania przed sądem tego państwa w sprawie domniemanego naruszenia RODO w związku z transgranicznym przetwarzaniem danych, jeżeli ów organ nie jest wiodącym organem nadzorczym w odniesieniu do takiego przetwarzania.

Ogólna właściwość organu wiodącego w przypadku transgranicznego przetwarzania danych

Jak podkreślił w swojej opinii rzecznik generalny, z samego brzmienia RODO (motyw 124, art. 56 ust. 1 i 6 RODO) wynika, że wiodącemu organowi ochrony danych przysługuje **ogólne uprawnienie do wszczynania postępowań sądowych w przed-miocie naruszenia przepisów RODO w przypadku trans-granicznego przetwarzania danych.** Konsekwencją tej ogólnej właściwości organu wiodącego są jednocześnie bardziej ograniczone uprawnienia organów nadzorczych w innych państwach członkowskich.

Odnosząc się do kompetencji organów nadzorczych umożliwiających wszczynanie postępowania sądowego w sprawie ewentualnych naruszeń RODO, które dotyczą ich terytoriów, rzecznik generalny wskazał, że uprawnienie to jest wyraźnie ograniczone w przypadku transgranicznego przetwarzania danych, właśnie po to, aby umożliwić wiodącemu organowi nadzorczemu efektywne wykonywanie powierzonych mu w tym zakresie zadań.

Sens mechanizmu kompleksowej współpracy (one-stop-shop)
Rzecznik generalny podkreślił, że przyczyną wprowadzenia w życie ustanowionego w RODO mechanizmu kompleksowej współpracy (one-stop-shop), w ramach którego ważną rolę powierzono wiodącemu organowi nadzorczemu i zaangażowano w sprawę inne organy ochrony danych, było zaradzenie niektórym niedostatkom wynikającym z wcześniej obowiązujących przepisów krajowych przyjętych na podstawie dyrektywy 95/46/WE. Podmioty gospodarcze dokonujące transgranicznego przetwarzania musiały bowiem przestrzegać często niespójnych przepisów krajowych transponujących dyrektywę 95/46/WE i koordynować swoje działania ze wszystkimi krajowymi organami nadzorczymi. Było to dla nich kosztowne, uciążliwe i czasochłonne, a także prowadziło do niepewności prawnej, po stronie zarówno tych podmiotów, jak i ich klientów.

Mechanizm kompleksowej współpracy a ochrona praw podmiotów danych

Odnosząc się do zagadnienia prawa do wszczęcia postępowania sądowego przysługującego osobom, których dane dotyczą, rzecznik generalny podkreślił, że mogą one bezpośrednio wszcząć postępowanie przeciwko administratorom i podmiotom przetwarzającym dane przed m.in. sądami państwa członkowskiego będącego miejscem zwykłego pobytu osób, których dane dotyczą, lub ich siedzibą.

Ponadto rzecznik generalny podkreślił, że skargi przeciwko organom nadzorczym muszą być wnoszone przez osoby, których dane dotyczą, do sądów państwa członkowskiego, w którym organ nadzorczy ma siedzibę, nawet wówczas gdy organ wiodący jest organem nadzorczym innego państwa członkowskiego. W przypadku odrzucenia lub oddalenia skargi organ nadzorczy, do którego taka osoba wniosła skargę, wydaje decyzję w tym względzie i powiadamia o niej skarżącego, co umożliwia mu wszczęcie postępowania w państwie członkowskim jego zwykłego pobytu lub siedziby.

Kompetencje pozostałych organów nadzorczych

W ocenie rzecznika generalnego wiodący organ nadzorczy nie może być uznawany za jedyny podmiot egzekwujący przepisy RODO w sytuacjach transgranicznych. Zgodnie z zasadami z RODO i w przewidzianych w tym akcie ramach czasowych powinien on ściśle współpracować z innymi organami nadzorczymi, których sprawa dotyczy, i nie może ignorować zgłaszanych przez nie istotnych dla sprawy uwag.

Jeżeli krajowe organy nadzorcze nie działają jako organ wiodący, mogą one w określonych sytuacjach w przypadku transgranicznego przetwarzania danych wszcząć postępowanie przed sądami ich państwa członkowskiego. Dotyczy to w szczególności sytuacji, w których krajowe organy ochrony danych:

- podejmują działania niemieszczące się w zakresie przedmiotowego stosowania RODO;
- badają te same lub podobne czynności transgranicznego przetwarzania danych dokonywane przez organy publiczne w interesie publicznym czy też przez administratorów spoza Unii;
- podejmują działania w trybie pilnym;

lub

- rozpoczynają działania wskutek podjęcia przez organ wiodący decyzji, że nie będzie się on zajmować daną sprawą.

Podsumowując, rzecznik generalny uznał, że RODO pozwala organowi nadzorczemu państwa członkowskiego na wszczęcie przed sądem tego państwa postępowania w sprawie domniemanego naruszenia RODO w przypadku transgranicznego przetwarzania danych, nawet jeżeli nie jest on organem wiodącym, pod warunkiem że działa w ramach procedur określonych w RODO.

Komunikat prasowy znajduje się na stronie: https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-01/cp210001pl.pdf.

Opinia RG M. Bobeka jest dostępna na stronie: http://curia.europa.eu/juris/document/document.jsf?text=&docid=236410&pageIndex=0&doclang=pl&mode=req&dir=&occ=first&part=1&cid=5835681.

Kolejne prace ENISA dotyczące pseudonimizacji danych

Katarzyna Barszczewska-Mazur

W związku z obchodami Dnia Ochrony Danych Osobowych w 2021 r. Agencja UE ds. Cyberbezpieczeństwa (ENISA) przygotowała raport dotyczący użycia technik pseudonimizacji na potrzeby ochrony danych osobowych pt. „Pseudonimizacja danych. Zaawansowane techniki i przykłady użycia".

Uwagi wstępne

Głównym przedmiotem działalności Agencji UE ds. Cyberbezpieczeństwa (ENISA) jest analiza rozwiązań technicznych w zakresie wdrażania RODO, podejścia *privacy* by design oraz bezpieczeństwa danych. Raport „Pseudonimizacja danych. Zaawansowane techniki i przykłady użycia" (ang. „Data Pseudonymisation. Advanced Techniques and Use Cases", dalej: „Raport")[1] powstał z intencją wyposażenia administratorów danych oraz procesorów w dokument zawierający techniczną analizę środków cyberbezpieczeństwa stosowanych w zakresie ochrony danych osobowych i prywatności. Dokument został oparty na wcześniejszych pracach ENISA dotyczących technik pseudonimizacji i najlepszych praktyk (dalej: „Raport 2019") [2], ale uzupełniono go o dalsze, zaawansowane techniki pseudonimizacji i konkretne przykłady ich zastosowania w obszarach takich jak opieka zdrowotna i cyberbezpieczeństwo.

Wzrost znaczenia pseudonimizacji w ochronie danych osobowych

Pojęcie pseudonimizacji rozpowszechniło się wraz z rozpoczęciem stosowania RODO[3]. Termin ten oznacza „przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej" (art. 4 pkt 5 RODO). Rozporządzenie postrzega pseudonimizację jako mechanizm zapewnienia bezpieczeństwa i ochrony danych już w fazie projektowania procesu przetwarzania, a także na etapie samego przetwarzania danych. Zastosowanie jednej z technik pseudonimizacji jest uważane za ważny aspekt wdrażania RODO w organizacji oraz sposobu wykazania zgodności z Rozporządzeniem. Podkreśla się jednak wybór i właściwe stosowanie technik pseudonimizacji, dlatego powinna być ona połączona z dokładną oceną ryzyka w zakresie bezpieczeństwa i ochrony danych. W odpowiedzi na te trudności Raport przedstawia możliwe zaawansowane techniki i przykłady ich użycia.

Techniki i polityki pseudonimizacji

Raport 2019 wymienia i opisuje **podstawowe techniki pseudonimizacji:**

1. *Counter*
2. Generator liczb losowych (ang. *random number generator*, RNG)
3. Kryptograficzna funkcja mieszająca
4. Kod uwierzytelniający wiadomość (ang. *message authentication code*, MAC)
5. Szyfrowanie symetryczne

[1] Zob. https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases/ (dostęp: 2.03.2021).
[2]Zob. https://www.enisa.europa.eu/news/enisa-news/enisa-proposes-best-practices-and-techniques-for-pseudonymisation (dostęp: 2.03.2021).
[3]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); dalej: „RODO", „Rozporządzenie".

Niezależnie od wyboru techniki **polityka pseudonimizacji** – czyli praktyczna implementacja techniki – ma również kluczowe znaczenie dla wdrożenia tego środka bezpieczeństwa. Raport 2019 opisuje trzy polityki pseudonimizaji:

1. **Pseudonimizacja deterministyczna:** we wszystkich bazach danych i za każdym razem, gdy się pojawia *Id*, jest ono zawsze zastępowane tym samym pseudonimem – *pseudo*.
2. **Randomizowana pseudonimizacja dokumentu:** za każdym razem, gdy *Id* pojawia się w bazie danych, jest zastępowane innym pseudonimem (*pseudo*1, *pseudo*2 itd.); jednak *Id* jest zawsze mapowane do tego samego zbioru (*pseudo*1, *pseudo*2) w zbiorze danych *A* i *B***.**
3. **W pełni zrandomizowana pseudonimizacja:** dla każdego wystąpienia *Id* w bazie danych *A* lub *B Id* jest zastępowane innym pseudonimem (*pseudo*1, *pseudo*2).

Zaawansowane techniki pseudonimizacji

Niekiedy dany kontekst przetwarzania jest tak szczególny, że dla pseudonimizacji danych przetwarzanych w jego ramach podstawowe techniki pseudonimizacji nie zawsze będą wystarczające. Możliwe jest jednak tworzenie pseudonimów odnoszących się do bardziej złożonych sytuacji, przy jednoczesnym zminimalizowaniu ryzyka naruszenia ochrony danych osobowych.

Raport omawia niektóre z **zaawansowanych technik pseudonimizacji** opartych na kryptografii i wskazuje, jak można je wykorzystać w praktyce:

1. **Szyfrowanie asymetryczne** – oferuje możliwość zaangażowania dwóch różnych podmiotów w proces pseudonimizacji: pierwszy podmiot może stworzyć pseudonimy z identyfikatorów przy użyciu publicznego klucza pseudonimizacji, podczas gdy inny podmiot jest w stanie połączyć pseudonimy z poszczególnymi identyfikatorami, wykorzystując tajny (prywatny) klucz pseudonimizacji.

Typowym zastosowaniem tej techniki jest udostępnianie grupom badawczym danych dotyczących opieki zdrowotnej. Do takich celów stosuje się w pełni zrandomizowane schematy pseudonimizacji, zapewniając, że identyfikatory (np. numer ubezpieczenia społecznego lub inny identyfikator) danego pacjenta nie są ze sobą powiązane.

2. **Sygnatury pierścieniowe i pseudonimy grupowe** – techniki te wiążą się z podpisem cyfrowym, którego podstawową ideą jest to, że każdy może zweryfikować ważność podpisu, który jest powiązany ze znanym sygnatariuszem.

Jedną z zaawansowanych technik podpisu cyfrowego jest tzw. podpis pierścieniowy. To podpis tworzony przez jednego z członków grupy, a jego właściwość polega na tym, że osoba weryfikująca podpis może sprawdzić, czy rzeczywiście został on utworzony przez członka tej grupy, ale nie może określić, który z nich to zrobił. Podpisy pierścieniowe są od niedawna wykorzystywane do tworzenia anonimowych kryptowalut (np. opensourcowa technologia Cryptonote) jako środek do dokonywania niemożliwych do śledzenia płatności.

Z kolei **grupowe pseudonimy** były używane w wielu protokołach śledzenia kontaktów opracowanych na potrzeby pandemii COVID-19. Za każdym razem, gdy spotykają się dwie osoby, tworzony jest pseudonim z wkładem każdej z nich. Po spotkaniu obie osoby otrzymują ten sam pseudonim. Ponadto każda osoba dysponuje listą pseudonimów grupowych. Jeśli któryś z nich zostanie ujawniony, wszystkie pseudonimy grupowe przypisane do tej osoby są publikowane i wszystkie kontakty tej osoby mogą sprawdzić, czy również zostały ujawnione.

3. **Tryb łączenia (*chaining mode*)** – polega na podejściu warstwowym: tymczasowo generowanych jest kilka pośrednich pseudonimów, aby ostatecznie uzyskać pseudonim, który jest wynikiem ostatniej funkcji mieszającej (ang. *hash function*). Każda warstwa jest obliczana przez inny podmiot i każdy podmiot ma wyłączną informację, jak został przez niego uzyskany pośredni pseudonim.

Przykładowe wykorzystanie tego schematu może polegać na tym, że odbiorca ostatecznego (lub nawet pośredniego) pseudonimu przeprowadza analizę statystyczną lub naukową danych spseudonimizowanych, bez możliwości przyporządkowania pseudonimów do identyfikatorów pierwotnych użytkowników.

4. **Pseudonimy oparte na wielu identyfikatorach lub atrybutach** – do utworzenia pseudonimu może prowadzić przetwarzanie kilku identyfikatorów (mapowanie wiele do jednego, ang. *many-to-one*).

Identyfikatory zaś mogą być jednorodne, gdy mają ten sam typ (np. stanowią numer telefonu osoby, której dane dotyczą) i są powiązane z różnymi osobami. Identyfikatory mogą być także niejednorodne, gdy pasują do różnych atrybutów jednego podmiotu danych (np. numeru ubezpieczenia społecznego, numeru telefonu, imienia i nazwiska).

5. **Pseudonimy z dowodem własności** – stanowią odpowiedź na problem związany z pseudonimizacją, której zastosowanie może w niektórych przypadkach kolidować z wykonywaniem praw przysługujących podmiotom danych na podstawie RODO. Do takiej sytuacji dochodzi np. wtedy, gdy administrator danych ma dostęp jedynie do pseudonimów, a nie do oryginalnych identyfikatorów.

Do takich przypadków mogą zostać wykorzystane **pseudonimy z dowodem własności**. Pseudonim P jest tworzony przez osobę, której dane dotyczą, na podstawie podanego identyfikatora, a następnie przesyłany do administratora danych. Administrator nie jest w stanie odzyskać żadnych informacji z pseudonimu P (właściwość ukrywająca, ang. *hiding property*). Jednocześnie nie jest możliwe znalezienie innego identyfikatora powiązanego z pseudonimem P (właściwość wiążąca, ang. *binding property*).

W schemacie omówionym w raporcie administrator danych poznaje identyfikator podmiotu danych. Można uniknąć tej sytuacji, stosując **dowód wiedzy zerowej** (ang. *zero-knowledge proof*) na etapie obsługi żądania.

6. Bezpieczne obliczenia wielostronne (*secure multiparty computations*) – techniki te mogą znaleźć zastosowanie w szczególności w przypadkach, które wymagają porównania dwóch różnych list od dwóch administratorów danych w sposób zapewniający, że ujawnione zostaną wyłącznie ich wspólne wpisy. Taka sytuacja zachodzi np. wtedy, gdy dwie firmy ubezpieczeniowe chcą się upewnić, że podmiot danych nie wykupił u nich tego samego ubezpieczenia, lub gdy w celu obliczenia współczynnika konwersji reklam reklamodawca i sprzedawcy chcą porównać listy osób, które widziały reklamę, z tymi, które zrealizowały transakcję.

7. Tajne systemy udostępniania (*secret sharing schemes*) – mogą być postrzegane jako rodzaj protokołów omówionych w pkt 6 powyżej. Schemat ten może zostać użyty do podzielenia identyfikatora na odrębne segmenty (będące pseudonimami), po jednym dla każdego innego odbiorcy, aby zapewnić, że odwrócenie pseudonimizacji i poznanie identyfikatora jest możliwe tylko przy spełnieniu określonych warunków, np. znajomości co najmniej kilku takich segmentów.

Przykłady użycia technik pseudonimizacji w dziedzinie ochrony zdrowia i cyberbezpieczeństwa

Przykłady użycia technik pseudonimizacji w dziedzinie zdrowia skupiły się na wymianie danych pomiędzy **pacjentami,** których dane medyczne są przetwarzane, szpitalami przechowującymi dane pacjenta oraz **innymi organizacjami przetwarzającymi dane,** takimi jak np. placówka badawcza. Raport analizuje takie przypadki jak:

1. Porównanie dokumentacji medycznej pacjenta.
2. Pseudonimizacja danych na potrzeby instytucji badawczej.
3. Rozproszone przechowywanie dokumentacji medycznej.

Szczególna uwaga została poświęcona problematyce *data custodianship*. Chociaż nie ma precyzyjnej definicji tego terminu, który oznacza ustanowienie zaufanych pośredników wspierających poufność i ochronę danych, może on obejmować różne funkcje w scenariuszu pseudonimizacji, w zależności od zaangażowania takich podmiotów w proces pseudonimizacji. Raport podkreśla, że zaangażowanie takiego podmiotu można traktować jako organizacyjny środek zabezpieczenia danych.

Wśród przykładów użycia technik pseudonimizacji w cyberbezpieczeństwie omówiono:

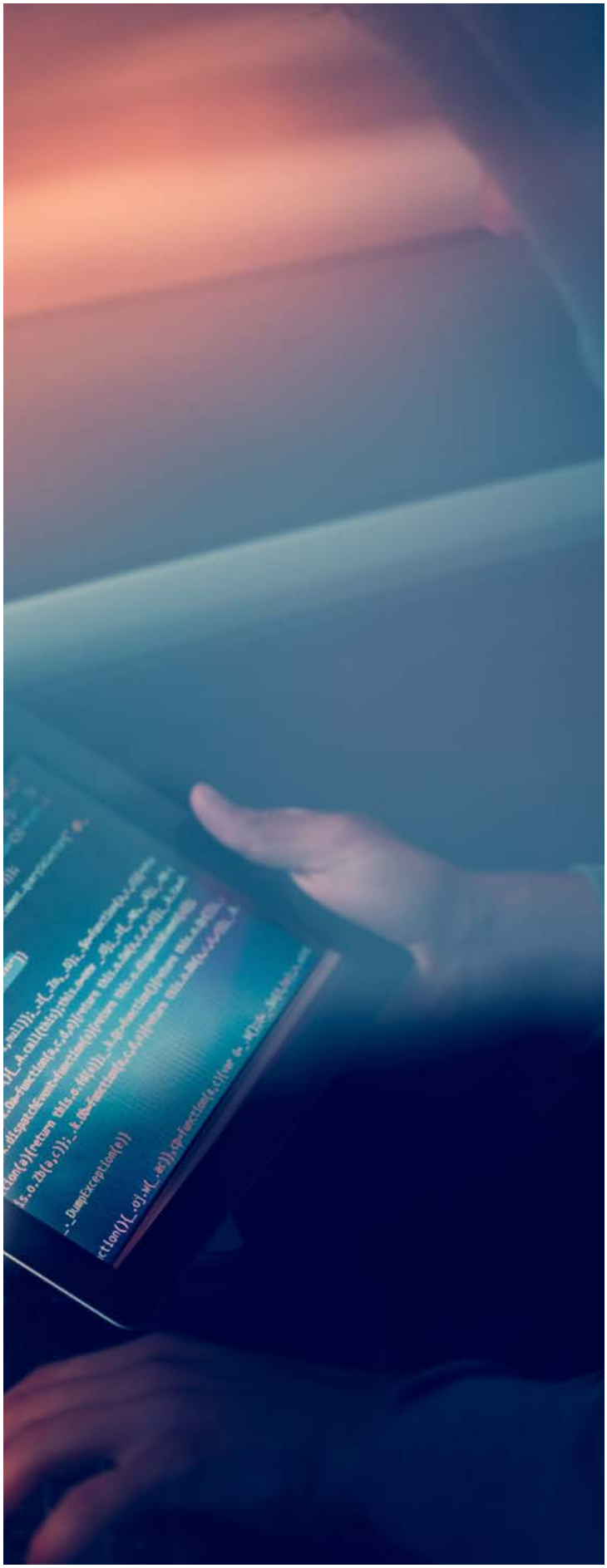
1. Szkolenie systemów Reputation System (RS).
2. Budowanie narzędzi ochrony dopasowanej do użytkownika.
3. Funkcjonowanie Operacyjnego Centrum Bezpieczeństwa (ang. Security Operations Center, SOC) i centrum obsługi klienta.

Komentarz

Raport wyraża przeświadczenie jego autorów, że nie ma jednej techniki pseudonimizacji, która byłaby odpowiednia do wszystkich przypadków i procesów przetwarzania danych osobowych. Wybrana technika powinna ograniczyć zagrożenia, a jednocześnie zachować wydajność przetwarzania danych pseudonimizowanych w różnych scenariuszach.

Połączenie różnych podejść może przynieść korzyści, zapewniając użyteczność danych przy jednoczesnym zachowaniu wysokiego poziomu ich ochrony. Takie rozwiązania wymagają jednak starannego wdrożenia, tak aby te korzyści były zachowane przez cały cykl życia danych. Raport wskazuje, że aby to zrobić, należy zebrać informacje i dokładnie przeanalizować pełny „kontekst" danego procesu przetwarzania danych osobowych, w ramach którego miałoby dojść do pseudonimizacji, a także ogólną specyfikę przetwarzania danych osobowych w organizacji.

Nie ma wątpliwości co do tego, że zastępowanie danych identyfikacyjnych pseudonimami może przyczynić się do zmniejszenia zagrożeń dla ochrony danych. Raport został przygotowany w duchu podejścia *privacy by design* i świadomego budowania systemu bezpieczeństwa ochrony danych osobowych, a także stanowi dobry materiał, który z uwagi na dość techniczny charakter analizy powinien stać się podstawową lekturą przede wszystkim dla funkcjonujących w organizacji działów IT.



Rozpoznawanie twarzy – wytyczne Komitetu Konsultacyjnego Konwencji 108

Katarzyna Barszczewska-Mazur

W dniu 28 stycznia 2021 r. Komitet Konsultacyjny ds. Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Konwencji 108) opublikował wytyczne dotyczące rozpoznawania twarzy (ang. Guidelines on Facial Recognition, dalej: „Wytyczne"[1]). Dokument omawia kryteria, które należy uwzględnić w działalności rządów, producentów, dostawców usług oraz deweloperów pracujących nad technologiami rozpoznawania twarzy, a także podmiotów z nich korzystających. Stosowanie takich technologii nie może bowiem prowadzić do naruszenia godności, praw ani podstawowych wolności człowieka, w tym prawa do ochrony danych osobowych.

Uwagi wstępne

Rozpoznawanie twarzy polega na automatycznym przetwarzaniu cyfrowych obrazów zawierających twarze osób w celu identyfikacji tych osób lub weryfikacji ich tożsamości za pomocą ustalonych wzorców twarzy. Technologia ta może być stosowana na różne sposoby, a niektóre z nich mogą poważnie naruszać prawa osób, których dane dotyczą. Takim przykładem będzie integracja technologii rozpoznawania twarzy z istniejącymi systemami nadzoru. Poważne zagrożenie dla prawa do prywatności i ochrony danych osobowych, a także dla innych praw podstawowych, wynika z tego, że stosowanie takich rozwiązań może pozostawać poza wiedzą osób, których dane biometryczne są przetwarzane, gdy do tego celu wykorzystane będą zdjęcia tych osób umieszczone w Internecie.

Wytyczne dotyczą stosowania technologii rozpoznawania twarzy, w tym rozpoznawania twarzy na żywo, w sektorze zarówno prywatnym, jak i publicznym.

Dokument został podzielony na cztery główne rozdziały:

1.Wytyczne dla legislatorów i podejmujących decyzje

W tej części podkreślone zostało znaczenie zasady **zgodności z prawem**. Zgodnie z art. 6 Konwencji 108+ przetwarzanie szczególnych kategorii danych, takich jak dane biometryczne, jest dozwolone tylko wtedy, gdy opiera się ono na odpowiedniej podstawie prawnej, a dodatkowe mechanizmy zabezpieczające są ustanowione w prawie krajowym.

Wytyczne uznają, że niektóre zastosowania tej technologii mogą być ograniczone lub wręcz zakazane na podstawie krajowych regulacji. Całkowicie zabronione powinno być takie przetwarzanie:

- którego wyłącznym celem będzie ustalenie koloru skóry, wyznania lub innych przekonań, płci, rasy, pochodzenia etnicznego, wieku, stanu zdrowia lub warunków społecznych;
- które do celów zatrudniania pracowników, dostępu do ubezpieczenia czy edukacji wykorzystuje dane pochodzące z rozpoznawania afektów, emocji.

2.Wytyczne dla deweloperów, producentów i dostawców usług

W tej części Wytyczne skupiają się na wyzwaniach związanych z fazą rozwoju i produkcji technologii rozpoznawania twarzy. W szczególności deweloperzy lub producenci takich technologii, a także podmioty z nich korzystające, powinni zapewnić prawidłowość danych wykorzystywanych do rozpoznawania twarzy. Prawidłowość może zostać wypracowana za pomocą testowania systemów, identyfikowania i eliminowania rozbieżności, zwłaszcza w odniesieniu do demograficznych różnic w kolorze skóry, wieku i płci, aby tym samym unikać niezamierzonej dyskryminacji.

W celu zapewnienia zarówno jakości danych, jak i wydajności algorytmów Wytyczne proponują opracowanie algorytmów przy użyciu syntetycznych zbiorów danych, na podstawie dostatecznie zróżnicowanych zdjęć – zarówno mężczyzn, jak i kobiet, osób o różnych kolorach skóry, różnej morfologii, w różnym wieku i w ujęciach z różnych perspektyw.

[1]Zob. https://www.coe.int/en/web/data-protection/-/ensure-that-facial-recognition-does-not-harm-fundamental-rights (dostęp: 2.03.2021).

W tym obszarze podkreślono znaczenie zasad takich jak: **niezawodność używanych narzędzi, budowanie świadomości** podmiotów stosujących technologie rozpoznawania twarzy, **ograniczony czas życia danych** oraz **rozliczalność.** Stosowanie tych zasad w kontekście rozpoznawania twarzy zostało szerzej omówione w Wytycznych.

3.Wytyczne dla podmiotów stosujących technologie rozpoznawania twarzy

Wytyczne zobowiązują podmioty korzystające z technologii rozpoznawania twarzy do wykazania, że wykorzystanie tych technologii jest ściśle niezbędne i zarazem proporcjonalne w kontekście konkretnego procesu przetwarzania, a jednocześnie nie koliduje z prawami podmiotów danych.

Ponieważ technologie rozpoznawania twarzy mogą być stosowane bez wiedzy podmiotu danych lub bez współpracy z podmiotami danych, szczególne znaczenie należy przypisać zasadom **transparentności i uczciwości** przetwarzania. Wytyczne zawierają wskazówki co do tego, jakie informacje powinny się znaleźć w polityce prywatności dotyczącej rozpoznawania twarzy czy w materiałach informacyjnych tej technologii.

Szczególną uwagę Wytyczne poświęcają również zasadom: **prawidłowości danych, ograniczenia celu, minimalizacji danych** oraz **ograniczonego czasu ich przechowywania**. Podkreślono także kwestię bezpieczeństwa danych, które z uwagi na swój charakter danych szczególnych kategorii, co więcej danych biometrycznych, mogą wiązać się z wyjątkowo poważnymi konsekwencjami w razie naruszenia stosowanych środków bezpieczeństwa.

Podmioty korzystające z technologii rozpoznawania twarzy mają obowiązek przeprowadzić **ocenę skutków dla ochrony danych (DPIA)** przed rozpoczęciem takiego przetwarzania. Wytyczne zalecają, aby w tym zakresie konsultować się z grupami interesariuszy, w tym z podmiotami danych, których takie przetwarzanie będzie dotyczyło, aby DPIA uwzględniała perspektywę tych osób. Zalecana jest również publikacja raportu z przeprowadzonej DPIA.

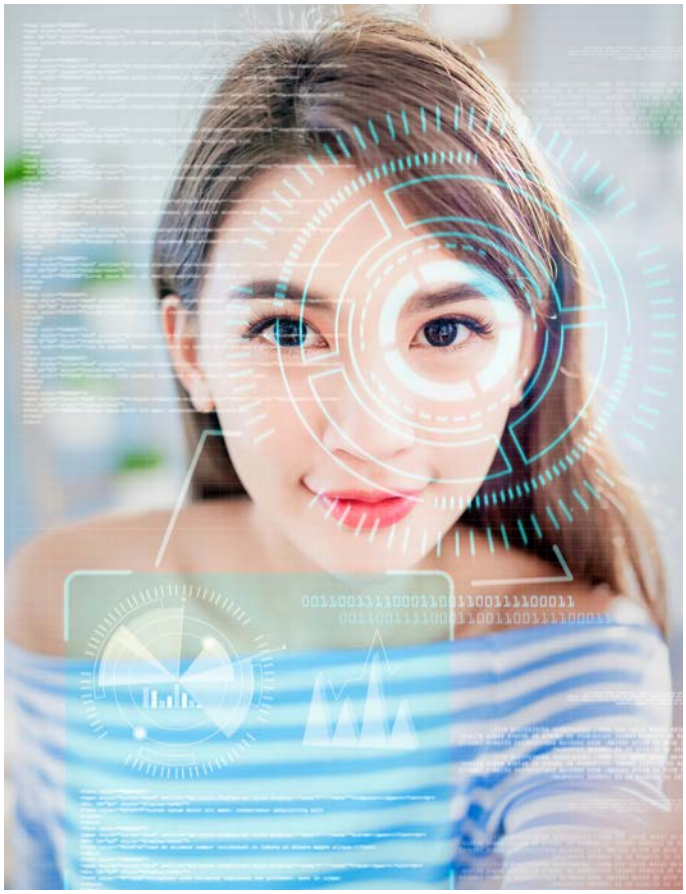
Odrębną uwagę Wytyczne poświęcają etycznym ramom stosowania tej technologii. Etyczne wątki powinny zostać uwzględnione zwłaszcza przy wykorzystywaniu rozpoznawania twarzy w specyficznych sektorach, w których z uwagi na szczególne okoliczności przetwarzania danych osobowych ryzyko związane z tą technologią jest znacznie wyższe.

4. Prawa osoby, której dane dotyczą

Tekst Wytycznych został zamknięty przypomnieniem, że rozpoznawanie twarzy opiera się na przetwarzaniu danych osobowych, zatem wszystkie prawa przewidziane w art. 9 Konwencji 108+ powinny być zagwarantowane osobom, których dotyczą dane przetwarzane w ramach tej technologii, w tym prawo dostępu, prawo do pozyskania informacji o uzasadnieniu, prawo do sprzeciwu oraz prawo do sprostowania. Wątek praw podmiotów danych zostaje szerzej omówiony w Wytycznych w odniesieniu do szczególnych okoliczności przetwarzania.

Komentarz

Dokument ma kierunkowy, dość ogólny charakter. Zalecane byłoby opracowanie bardziej pogłębionej analizy, nie tylko prawnej, lecz także technicznej, przez inne organy zajmujące się ochroną danych osobowych. Najistotniejszy wniosek, jaki płynie z tekstu Wytycznych, sprowadza się do stwierdzenia, że w procesie projektowania i wdrażania technologii rozpoznawania twarzy – w sektorze zarówno publicznym, jak i prywatnym – w centrum tego procesu powinien pozostać człowiek, osoba, której dane dotyczą, a także jego wolności i prawa. Szczególnie zaakcentowane zostaje prawo do ochrony danych osobowych, dyktujące konkretne wymagania, które powinny zostać uwzględnione w stosowanej technologii.



Wytyczne dotyczące ochrony danych dzieci w środowisku edukacyjnym

Mateusz Kupiec

W trakcie 40. posiedzenia plenarnego Komitetu Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzonej w Strasburgu dnia 28 stycznia 1981 r. delegacje państw – stron Konwencji – przyjęły wytyczne dotyczące ochrony danych dzieci w środowisku edukacyjnym (dalej: **Wytyczne**). Dokument ten stanowi drogowskaz dla placówek edukacyjnych, mający na celu wsparcie ich w realizacji podstawowych praw dziecka w kontekście ochrony danych osobowych. W styczniu 2021 r. pracownicy Urzędu Ochrony Danych Osobowych dokonali nieoficjalnego tłumaczenia tekstu Wytycznych na język polski. Przyglądamy się najważniejszym praktycznym elementom tego opracowania.

Wskazówki dla placówek edukacyjnych jako administratorów danych

Chociaż znaczna część Wytycznych poświęcona jest zaleceniom dla ustawodawców i decydentów w zakresie ochrony danych osobowych dzieci, to jej autorzy poświęcili również sporo uwagi zagadnieniom praktycznym dotyczącym **ochrony autonomii informacyjnej dzieci przez placówki oświatowe.** W Wytycznych zauważa się, że:

- zarówno dziecko, jak i jego opiekunowie prawni powinni bezpośrednio otrzymywać informacje dotyczące ich praw jako osób, których dane są przetwarzane. Udzielenie takich informacji opiekunowi prawnemu nie powinno co do zasady zwalniać z obowiązku przekazania ich dziecku;
- placówki edukacyjne powinny zagwarantować odpowiedni poziom alternatywnego świadczenia edukacji, bez uszczerbku dla interesu dziecka, jeżeli rodzina dziecka lub ono samo skorzystają z prawa do sprzeciwu wobec przetwarzania danych za pomocą narzędzi cyfrowych;
- administratorzy danych i podmioty przetwarzające nie mogą udostępniać danych osobowych dzieci pozyskanych w trakcie ich edukacji innym podmiotom, które czerpałyby z nich korzyści ekonomiczne;
- po opuszczeniu placówki edukacyjnej w wyniku np. zakończenia nauki dzieci powinny być (niezależnie od wieku) informowane o tym, które ich dane osobowe nadal będą przechowywane, jaki podmiot będzie je przetwarzał i w jakim celu;
- placówki edukacyjne po zakończeniu przez dziecko procesu kształcenia powinny przechowywać wyłącznie niezbędne informacje pozwalające na jego identyfikację, np. w celu wykazania jego osiągnięć, umożliwienia mu skorzystania z prawa dostępu do danych;
- placówki edukacyjne nie powinny powszechnie przetwarzać danych biometrycznych. Informacje te mogą być przetwarzane jedynie w wyjątkowych okolicznościach, gdy jest to bezwzględnie konieczne.

Ogólne wytyczne dotyczące przetwarzania danych osobowych dzieci w sieci

Autorzy Wytycznych wskazują również, że:

- we wszystkich działaniach dotyczących dziecka w środowisku cyfrowym najważniejszy jest interes dziecka;
- administratorzy danych muszą uznać prawa opiekunów prawnych do działania w imieniu i w najlepszym interesie dziecka, zgodnie z prawem krajowym i międzynarodowym oraz zgodnie z art. 9 Konwencji nr 108;
- należy dołożyć wszelkich starań w celu zaangażowania dziecka w podejmowanie decyzji w zakresie spraw, którego go dotyczą;
- prawo dziecka do bycia wysłuchanym polega na tym, że może ono swobodnie zabierać głos we wszystkich sprawach, które go dotyczą, a wyrażanym przez nie poglądom należy nadawać odpowiednią wagę, stosownie do wieku dziecka i jego dojrzałości (dzieci osiągają poszczególne poziomy dojrzałości w różnym tempie);
- placówki edukacyjne powinny odpowiednio przeszkolić personel w celu zapewnienia pracownikom niezbędnych umiejętności z zakresu uwzględniania prawa dziecka do bycia wysłuchanym;
- profilowanie dzieci powinno być co do zasady zabronione przez ustawodawcę, chyba że takie przetwarzanie danych dotyczących dziecka leży w jego interesie lub istnieje nadrzędny interes publiczny, pod warunkiem że odpowiednie gwarancje są przewidziane przez prawo;
- dane dzieci przetwarzane za pomocą oprogramowania edukacyjnego nie powinny być wykorzystywane w celu wyświetlania im reklam behawioralnych.

Nieoficjalne tłumaczenie Wytycznych na język polski, przygotowane przez pracowników Departamentu Współpracy Międzynarodowej i Edukacji UODO, jest dostępne pod adresem: https://uodo.gov.pl/pl/file/3344

Wymogi AEPD dotyczące audytu czynności przetwarzania danych osobowych z udziałem AI

Mateusz Kupiec

Rozwój sztucznej inteligencji i ochrona danych osobowych są ze sobą powiązane. Podmioty wykorzystujące systemy sztucznej inteligencji w operacjach na danych osobowych muszą bowiem w odpowiedni sposób zagwarantować autonomię informacyjną osób, których dane dotyczą. W styczniu 2021 r. hiszpański organ nadzorczy (AEPD) opublikował anglojęzyczną wersję wymogów dotyczących audytu czynności przetwarzania danych osobowych z udziałem AI. Dokument ten ma na celu przedstawienie działań kontrolnych, które powinny być wykonywane w trakcie audytów procesów przetwarzania danych osobowych wykorzystujących komponenty oparte na sztucznej inteligencji (AI). Jego zakres obejmuje przede wszystkim konkretne wytyczne metodologiczne oraz wykaz mechanizmów kontroli, które można uwzględnić w audycie ochrony danych dotyczącym przetwarzania obejmujące-go komponenty lub rozwiązania oparte na sztucznej inteligencji. Przedstawiamy wybrane elementy opracowania organu.

Wstęp

AEPD wskazuje, że przetwarzanie danych osobowych, w którym sztuczna inteligencja (AI) jest wykorzystywana do przeprowadzania analiz i wnioskowania, wymaga zastosowania dojrzałego modelu organizacji, gwarantującego prywatność osobom fizycznym. Wymaga to od administratorów danych opracowania obiektywnych kryteriów przeprowadzania audytów komponentów AI z punktu widzenia ochrony danych.

Audyt przestrzegania zasady przejrzystości przez komponent AI

W celu określenia, czy w procesie korzystania z systemu AI jest przestrzegana zasada przejrzystości, AEPD zaleca administratorom danych sprawdzenie, czy w ich organizacji:

- należycie udokumentowano źródło wykorzystywanych danych;
- informacje dotyczące metadanych komponentu opartego na sztucznej inteligencji oraz konsekwencji, jakie mogą wynikać z jego zastosowania, są dostępne dla osób, których dane dotyczą;
- możliwe jest prześledzenie zachowania konkretnego komponentu w odniesieniu do zestawów danych wejściowych, wykorzystania danych, danych pośrednich i danych wyjściowych;
- ustanowiono mechanizmy minimalizujące szkody, które może wyrządzić podmiotom danych komponent oparty na AI.

Audyt jakości danych przetwarzanych przez komponent AI

Zgodnie z zasadami dotyczącymi przetwarzania danych osobowych dane te muszą być dokładne i aktualne w odniesieniu do celów, dla których są przetwarzane. AEPD wskazuje, że aby ustalić, czy zasada ta została spełniona w przypadku użycia komponentów opartych na działaniu AI, należy sprawdzić, czy:

- istnieje udokumentowana procedura zarządzania danymi, która gwarantuje dokładność, integralność, prawdziwość, aktualność i adekwatność zbiorów danych wykorzystywanych do szkolenia, testowania i eksploatacji systemu AI oraz pozwala na ich weryfikację;

- zostały przyjęte mechanizmy nadzoru nad procesami gromadzenia, przetwarzania, przechowywania i wykorzystywania danych;

- zostały wprowadzone procedury wykrywania i analizy wszelkich możliwych dysproporcji pomiędzy liczbami danych, które gromadzi komponent AI, mogących prowadzić do odchyleń w działaniu systemu.

Audyt w zakresie przechyłu algorytmicznego (AI bias)

W celu określenia, czy w danej organizacji wprowadzono środki techniczno-organizacyjne mające ograniczyć ryzyko wystąpienia przechyłu (uprzedzenia) algorytmicznego (AI bias), należy:

zweryfikować, czy wdrożono właściwe procedury w celu zidentyfikowania przechyłu algorytmicznego i usunięcia lub przynajmniej ograniczenia tendencyjności danych użytych do trenowania odpowiedniego modelu AI;

sprawdzić, czy w danych treningowych używanych jako dane wejściowe do odpowiedniego modelu nie występują wcześniej stwierdzone uprzedzenia – a jeśli tak, to czy wybrano inne, wolne od uprzedzeń źródło danych;

zastosować właściwe środki, aby ocenić, czy zachodzi konieczność przetwarzania dodatkowych danych w celu poprawy precyzji komponentu AI;

wprowadzić mechanizmy nadzoru w postaci czynnika ludzkiego, których celem jest zapewnienie, że wyniki są wolne od przechyłu (uprzedzenia) algorytmicznego.

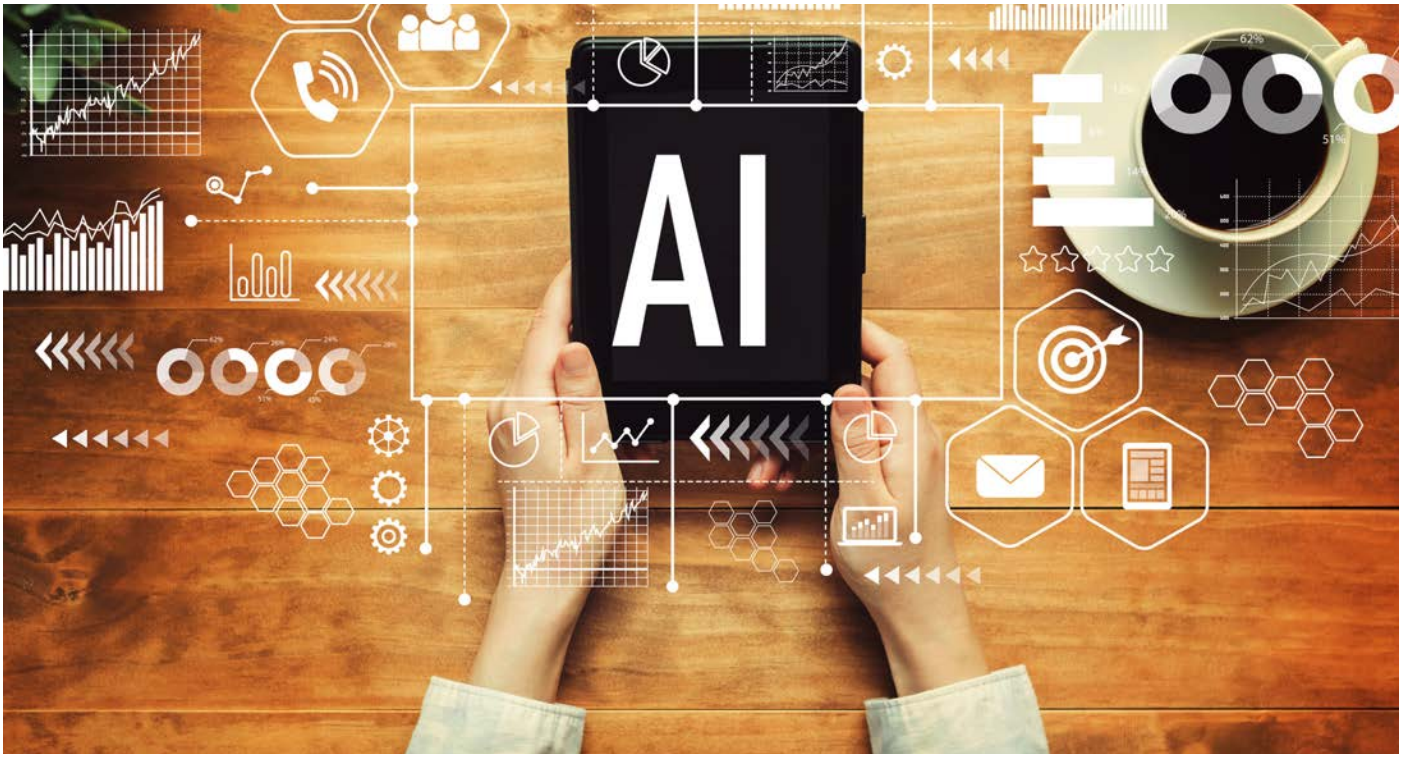
Audyt w zakresie weryfikowalności komponentu AI

W celu sprawdzenia, czy komponent AI wykorzystywany do przetwarzania danych osobowych jest weryfikowalny, należy określić m.in., czy w organizacji:

- istnieje sformalizowana i udokumentowana procedura oceny ryzyka, podlegająca osobnej ocenie w przypadku wystąpienia zmian, które mogą zajść przy wdrażaniu komponentu opartego na AI w całym cyklu jego życia;
- wdrożono odpowiednie mechanizmy monitorowania komponentu opartego na AI, które umożliwiają ocenę jego zachowania w interakcji ze środowiskiem;
- prowadzony jest wykaz wykrytych i naprawionych przypadków nieprawidłowego zachowania komponentu.

Wymogi dotyczące audytu czynności przetwarzania danych osobowych z udziałem AI można znaleźć w języku angielskim pod adresem: https://www.aepd.es/sites/default/files/2021-01/requisitos-auditorias-tratamientos-incluyan-ia-en.pdf.

AEPD wskazuje, że tylko hiszpańska wersja wymogów ma charakter autentyczny. Z wymogami dotyczącymi audytu czynności przetwarzania danych osobowych z udziałem AI w języku hiszpańskim można zapoznać się pod adresem: https://www.aepd.es/sites/default/files/2021-01/requisitos-auditorias-tratamientos-incluyan-ia.pdf.



Niemiecki projekt ustawy o autonomicznej jeździe

Mateusz Kupiec

Tempo rozwoju w dziedzinie zautomatyzowanej, autonomicznej i połączonej jazdy nie słabnie. Niemiecki rząd federalny uznał, że aby umożliwić korzystanie z tych rozwiązań w sposób bezpieczny, konieczne jest poczynienie kroków w celu wprowadzenia odpowiednich regulacji prawnych dotyczących pojazdów silnikowych wyposażonych w funkcję jazdy autonomicznej. 10 lutego 2021 r. przyjął on projekt ustawy o jeździe autonomicznej, która ma dokonać zmian w niemieckiej ustawie o ruchu drogowym oraz w ustawie o ubezpieczeniach obowiązkowych (niem. *Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und des Pflichtversicherungsgesetzes – Gesetz zum autonomen Fahren*, dalej: **Projekt**). Przedstawiamy główne cele i założenia Projektu, ze szczególnym uwzględnieniem zaproponowanych przez projektodawcę rozwiązań dotyczących ochrony danych osobowych.

Cel Projektu

Już na samym wstępie Projektu podkreślono, że wobec braku międzynarodowych standardów oraz zharmonizowanych regulacji na poziomie Unii Europejskiej postępujące w dziedzinie rozwiązań umożliwiających jazdę autonomiczną zagadnienie sposobu eksploatacji pojazdów silnikowych wyposażonych w funkcję jazdy autonomicznej wymaga uregulowania przez prawodawcę krajowego. Z tego względu rząd federalny Niemiec uznał, że konieczne jest wprowadzenie stosownych krajowych ram prawnych, które stworzą odpowiednie warunki do regularnej eksploatacji takich pojazdów do czasu harmonizacji tego obszaru na poziomie UE. W ocenie projektodawców wykorzystanie zautomatyzowanych, autonomicznych i połączonych w sieć pojazdów silnikowych w ruchu publicznym będzie stanowić istotny element przyszłej mobilności.

Definicja pojazdu autonomicznego

W rozumieniu § 1d Projektu pojazdem silnikowym wyposażonym w funkcję jazdy autonomicznej jest pojazd, który może wykonywać zadanie prowadzenia w sposób niezależny w określonym zakresie roboczym bez udziału osoby kierującej oraz jest wyposażony w rozwiązania techniczne określone w § 1e ust. 2 Projektu, np. w systemy umożliwiające samodzielne przestrzeganie przepisów ruchu drogowego skierowanych do kierowcy pojazdu oraz unikanie wypadków.

Przetwarzanie danych na potrzeby jazdy autonomicznej

Przepisy dotyczące przetwarzania danych na potrzeby pracy pojazdów wyposażonych w funkcję jazdy autonomicznej zostały umieszczone w § 1g Projektu. Projektowane regulacje przewidują:

- zobowiązanie właścicieli (niem. *Halter*) pojazdów z funkcją jazdy autonomicznej do gromadzenia określonych danych podczas ich eksploatacji, np. informacji o okresie aktywacji i dezaktywacji funkcji jazdy autonomicznej, z zakresu monitorowania systemu, w tym o stanie oprogramowania, warunkach pogodowych oraz środowiskowych. W uzasadnieniu podkreślono, że wiedza na ten temat jest niezbędna m.in. do kontroli bezpieczeństwa eksploatacji pojazdu (§ 1g ust. 1 Projektu);
- wprowadzenie wyczerpującej listy okoliczności, w których wskazane w § 1g ust. 1 Projektu dane mają być zapisywane, np. w sytuacjach grożących wypadkiem, w przypadku zakłóceń działania pojazdu (§ 1g ust. 2 Projektu);

- zobowiązanie producentów pojazdów z funkcją jazdy autonomicznej do informowania właścicieli pojazdów o możliwości zmiany ustawień dotyczących prywatności i danych, które są przetwarzane, gdy pojazd silnikowy jest używany w trybie jazdy autonomicznej. Odpowiednie oprogramowanie pojazdu (silnikowego) musi umożliwiać właścicielowi dokonanie takich zmian (§ 1g ust. 3 Projektu);
- zobowiązanie producentów pojazdów silnikowych z funkcją jazdy autonomicznej do umożliwienia – technicznie i organizacyjnie – osobom korzystającym z takich pojazdów realizacji suwerenności danych (niem. *Datenhoheit*);
- nadanie właściwym organom krajów związkowych oraz Federalnemu Urzędowi ds. Ruchu Drogowego (niem. *Kraftfahrt-Bundesamt*) prawa dostępu do danych przetwarzanych w związku z eksploatacją pojazdów wyposażonych w funkcję jazdy autonomicznej oraz ich wykorzystania (§ 1g ust. 4 i 6 Projektu);
- uprawnienie Federalnego Urzędu ds. Ruchu Drogowego do przekazania pozyskanych danych nieosobowych dotyczących eksploatacji pojazdów z funkcją jazdy autonomicznej: uniwersytetom, ośrodkom badawczym, władzom federalnym, krajowym i lokalnym, które wykonują zadania w zakresie badań, rozwoju, planowania ruchu lub planowania miejskiego. Celem przekazania danych ma być prowadzenie badań naukowych w dziedzinie cyfryzacji, automatyzacji i tworzenia sieci oraz badań wypadków drogowych (§ 1g ust. 5 Projektu).

Komentarz

Projekt ustawy o jeździe autonomicznej jest obecnie przedmiotem prac w niemieckim parlamencie. Stanowi on ciekawą propozycję uregulowania przepisów dotyczących pojazdów wyposażonych w funkcję jazdy autonomicznej, która może stanowić inspirację dla pozostałych państw członkowskich UE albo do podjęcia działań prawodawczych na poziomie UE.

Projekt ustawy o jeździe autonomicznej w języku niemieckim jest dostępny pod adresem: https://www.bmvi.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-19/gesetz-aenderung-strassenverkehrsgesetz-pflichtversicherungsgesetz-autonomes-fahren.pdf?__blob=publicationFile.

Prezes UODO nałożył dwie kolejne administracyjne kary pieniężne za brak współpracy z organem nadzorczym

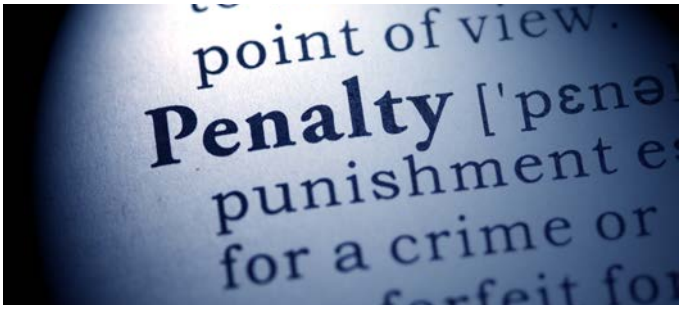
Dominika Nowak, Radczyni prawna

Od grudnia 2020 r. do stycznia 2021 r. Prezes Urzędu Ochrony Danych Osobowych (UODO) wydał kolejne dwie decyzje nakładające administracyjne kary pieniężne za brak współpracy z organem. Warto zapoznać się z okolicznościami nałożenia poszczególnych kar, aby w przypadku wezwania otrzymanego od organu nie narazić się na taki zarzut ani związane z nim konsekwencje.

Wstęp

Na wstępie należy przypomnieć, że zgodnie z art. 31 RODO[1] „administrator i podmiot przetwarzający oraz – gdy ma to zastosowanie – ich przedstawiciele na żądanie współpracują z organem nadzorczym w ramach wykonywania przez niego swoich zadań".

Komplementarne dla tych obowiązków są uprawnienia organu nadzorczego polegające m.in. na uzyskiwaniu od administratora i podmiotu przetwarzającego dostępu do wszelkich danych osobowych i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań oraz uzyskiwaniu dostępu do wszystkich pomieszczeń administratora i podmiotu przetwarzającego, w tym do sprzętu i środków służących do przetwarzania danych, zgodnie z procedurami określonymi w prawie unijnym lub w prawie państwa członkowskiego (art. 58 ust.1 lit. e i f RODO).



Smart Cities sp. z o.o. (znak sprawy: DKE.561.13.2020)

9 grudnia 2020 r. Prezes UODO wydał decyzję w sprawie Smart Cities sp. z o.o. z siedzibą w Warszawie, nakładającą administracyjną karę pieniężną w wysokości 12 838,20 zł.

W ocenie organu adresat decyzji naruszył art. 31 RODO oraz art. 58 ust. 1 lit. e RODO poprzez brak współpracy z Prezesem UODO w ramach wykonywania przez niego jego zadań oraz niezapewnienie dostępu do danych osobowych i innych informacji niezbędnych organowi nadzorczemu do realizacji jego zadań.

Nakładając administracyjną karę pieniężną, Prezes UODO wziął pod uwagę, że spółka nie udzieliła odpowiedzi na pierwsze pismo wzywające do złożenia dodatkowych wyjaśnień ani na ponowne wezwanie do niezwłocznego złożenia wyjaśnień, co utrudniało Prezesowi UODO ustalenie stanu faktycznego w prowadzonym postępowaniu. Spółka nie ustosunkowała się także do pisma informującego o wszczęciu postępowania w przedmiocie nałożenia administracyjnej kary pieniężnej.

Anwara sp. z o.o. (znak sprawy: DKE.561.16.2020)

5 stycznia 2021 r. Prezes UODO wydał decyzję w sprawie Anwara sp. z o.o. z siedzibą w Warszawie, nakładającą administracyjną karę pieniężną w wysokości 21 397 zł.

[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

W ocenie organu adresat decyzji naruszył art. 31 oraz art. 58 ust. 1 lit. a RODO poprzez brak współpracy z Prezesem UODO w ramach wykonywania przez niego jego zadań oraz niedostarczenie wszelkich informacji potrzebnych Prezesowi UODO do realizacji jego zadań, tj. do rozpatrzenia skargi Pana M. K. na nieprawidłowości w procesie przetwarzania jego danych osobowych.

Nakładając administracyjną karę pieniężną, Prezes UODO wziął pod uwagę, że:

- spółka nie złożyła wyjaśnień w sprawie skargi na przetwarzanie przez nią danych osobowych po otrzymaniu wezwania od Prezesa UODO;
- spółka nie udzieliła wyjaśnień również po ponownym wezwaniu, w którym została pouczona, że brak nadesłania wyjaśnień może skutkować nałożeniem administracyjnej kary pieniężnej;
- spółka nie ustosunkowała się także do pisma informującego o wszczęciu postępowania w przedmiocie nałożenia administracyjnej kary pieniężnej.

Komentarz

W obydwu sprawach administracyjna kara pieniężna została nałożona za brak odpowiedzi na pierwotne żądanie Prezesa UODO oraz na ponowne wezwanie do złożenia wyjaśnień, w których to pismach Prezes UODO informował o możliwości nałożenia administracyjnej kary pieniężnej. Wniosek z tych spraw jest następujący: w przypadku wezwania do złożenia wyjaśnień przez Prezesa UODO nie należy takich pism lekceważyć, ponieważ już dwukrotny brak odpowiedzi może skutkować nałożeniem administracyjnej kary pieniężnej za brak współpracy. Ponadto należy zauważyć, że nałożenie kary za brak współpracy nie wyklucza nałożenia kolejnej kary, jeżeli organ w pierwotnym postępowaniu stwierdzi naruszenie przepisów RODO.

Link do pełnej treści decyzji w sprawie Smart Cities sp. z o.o.: https://www.uodo.gov.pl/decyzje/DKE.561.13.2020%20.

Link do pełnej treści decyzji w sprawie Anwara sp. z o.o.: https://uodo.gov.pl/decyzje/DKE.561.16.2020.

Pierwsza kara nałożona przez Prezesa UODO za niewykonanie nakazu

Dominika Nowak, Radczyni prawna

Prezes UODO decyzją z dnia 5 stycznia 2021 r. (DKE.561.11.2020) nałożył na przedsiębiorcę prowadzącego działalność gospodarczą w zakresie ochrony zdrowia administracyjną karę pieniężną w wysokości ponad 85 tys. zł za niewykonanie nakazu wydanego wobec niego w decyzji administracyjnej. Nakaz ten polegał na konieczności zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony danych osobowych zgodnie z art. 34 ust. 1 RODO.

Stan faktyczny

W lipcu 2019 r. administrator zgłosił do Prezesa UODO naruszenie ochrony danych osobowych, które polegało na nieuprawnionym skopiowaniu w kwietniu 2019 r. danych osobowych stu pacjentów z systemu przychodni przez byłego pracownika celem wykorzystania tych informacji do marketingu własnych usług. Naruszenie dotyczyło następujących kategorii danych osobowych pacjentów: numer PESEL, imię i nazwisko, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu oraz numer telefonu. Administrator zrezygnował z zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony danych osobowych, **pomimo że ocenił ryzyko naruszenia praw i wolności osób fizycznych za wysokie.**

W sierpniu 2019 r. Prezes UODO wystąpieniem skierowanym do administratora wezwał go do niezwłocznego zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych oraz przekazania tym osobom zaleceń odnośnie do zminimalizowania potencjalnych negatywnych skutków zaistniałego naruszenia. W wystąpieniu wskazano przykładowe ryzyka związane z tego rodzaju naruszeniem oraz przykładowe zalecenia co do środków, jakie osoby dotknięte naruszeniem mogą podjąć, aby zabezpieczyć się przed jego negatywnymi skutkami.

.W związku z **brakiem reakcji ze strony administratora** Prezes UODO wszczął postępowanie administracyjne w sprawie niezawiadomienia osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych. Decyzją administracyjną Prezes UODO nakazał administratorowi zawiadomienie osób, których dane dotyczą – w terminie trzech dni od dnia, w którym decyzja stanie się ostateczna. Administrator nie wniósł od tej decyzji administracyjnej skargi do Wojewódzkiego Sądu Administracyjnego.

Następnie, w maju 2020 r., **wezwał administratora do złożenia wyjaśnień i przedstawienia wykazu osób, którym przekazano zawiadomienia, o których mowa w nakazie decyzji, a także informacji o sposobie ich przekazania oraz dowodów na ich przekazanie** (kopii dziesięciu przykładowych zawiadomień wraz z potwierdzeniem ich nadania). W odpowiedzi administrator poinformował Prezesa UODO, że: „Niestety mimo naszych chęci nie byliśmy w stanie takiej listy stworzyć, gdyż nie wiemy, których pacjentów dane zebrał lekarz, o którym mowa w zawiadomieniu złożonym przez K. Obecnie w naszych placówkach leczy się ponad […] osób i powiadomienie wszystkich o możliwości naruszenia ich danych osobowych jest awykonalne". W czerwcu 2020 r. Prezes UODO skierował do administratora **upomnienie**. Następnie administrator przedstawił kopie dziesięciu przesłanych listem zawiadomień, które nie zawierały wszystkich informacji wymaganych przez art. 34 ust. 1 RODO. W lipcu 2020 r. Prezes UODO wezwał administratora do uzupełnienia wyjaśnień, które również okazały się niewystarczające.

Rozstrzygnięcie

W związku z tym Prezes UODO wszczął **postępowanie administracyjne w przedmiocie nałożenia na administratora administracyjnej kary pieniężnej za nieprzestrzeganie nakazu orzeczonego przez organ nadzorczy.** W piśmie wskazano, że jeżeli administrator przedstawi dowody na wykonanie w całości nakazu przedmiotowej decyzji Prezesa UODO, okoliczność ta może wpłynąć łagodząco na wymiar administracyjnej kary pieniężnej orzeczonej w niniejszym postępowaniu lub też może spowodować odstąpienie od jej nałożenia.

W trakcie tego postępowania administrator przedstawił listę osób, którym przesłał zawiadomienia o naruszeniu ich danych osobowych. Ponadto do pisma załączone zostały: kopia wystawionej przez Pocztę Polską S.A. na rzecz przedsiębiorcy faktury VAT dokumentującej zakup 37 znaczków pocztowych oraz kopia oświadczenia o treści „Potwierdzamy nadanie przez Pana M. K. listów zwykłych w ilości 37 sztuk". Prezes UODO uznał, że wyjaśnienia są niekompletne i nie dają podstawy do stwierdzenia, że administrator istotnie powiadomił osoby, których dane dotyczą. Administrator został wezwany do uzupełnienia dowodów wykonania nakazu decyzji, tj. do przesłania poprawnego wykazu osób, którym zostały przesłane zawiadomienia, oraz kopii wszystkich zaadresowanych zawiadomień wraz z potwierdzeniem nadania przesyłek poleconych lub zwrotnych potwierdzeń odbioru. W odpowiedzi administrator wskazał, że nie ma obowiązku wysyłania listów poleconych.

Na podstawie powyższych informacji Prezes UODO nałożył na administratora administracyjną karę pieniężną w wysokości 85 588 zł.

Komentarz

Administrator powinien pamiętać o następujących kwestiach, jeżeli zgłasza naruszenie ochrony danych osobowych do Prezesa UODO na podstawie art. 33 ust. 1 RODO:

- jeżeli na podstawie przeprowadzonej analizy ryzyka naruszenia praw lub wolności osób, których dane dotyczą, administrator dojdzie do wniosku, że występuje **wysokie ryzyko,** to zgodnie z art. 34 ust. 1 RODO należy powiadomić o tym osoby objęte naruszeniem;
- zawiadomienie powinno spełniać przesłanki z art. 34 ust. 2 RODO;
- zwolnienie z zawiadomienia osób, których dane dotyczą, może wystąpić wyłącznie wtedy, gdy zostanie spełniona jedna z przesłanek z art. 34 ust. 3 RODO;
- **należy odpowiednio udokumentować zawiadomienie osób, których dane dotyczą.**

Pełna treść decyzji dostępna jest pod adresem: https://www.uodo.gov.pl/decyzje/DKE.561.11.2020.

ZESPÓŁ RODO

Xawery Konarski
Adwokat, Senior Partner
xawery.konarski@traple.pl

Prof. INP PAN dr hab. Grzegorz Sibiga
Adwokat, Partner
grzegorz.sibiga@traple.pl

dr inż. Andrzej Kaczmarek
Of counsel
andrzej.kaczmarek@traple.pl

Katarzyna Syska
Adwokatka, Senior Associate
katarzyna.syska@traple.pl

Dominika Nowak
Radczyni prawna, Senior Associate
dominika.nowak@traple.pl

dr Iga Małobęcka-Szwast LL.M.
Senior Associate
iga.malobecka@traple.pl

Katarzyna Barszczewska-Mazur
Associate
katarzyna.barszczewska@traple.pl

Mateusz Kupiec
Trainee
mateusz.kupiec@traple.pl

Redaktor newslettera:
dr Iga Małobęcka-Szwast

Pytania prosimy kierować na adres:
rodo@traple.pl