RODO w szkolnej ławce. Przetwarzanie danych biometrycznych

wykład online
28 kwietnia 2021 r.

Urząd Ochrony Danych Osobowych

Przetwarzanie danych biometrycznych w szkole

Natalia Holland, Departament Skarg

1. Czym są dane biometryczne – definicja.
2. Podstawy prawne dopuszczalności przetwarzania danych biometrycznych na gruncie przepisów RODO.
3. Wymogi dla wykorzystywania danych biometrycznych (ocena proporcjonalności, adekwatności, celowości).
4. Czy szkoły mogą przetwarzać dane biometryczne – odciski palców?
5. Dotychczasowe doświadczenia UODO dotyczące stosowania biometrii w szkole na przykładzie decyzji Prezesa UODO z 18 lutego 2020 r. o sygn. ZSZZS.440.768.2018.
6. Przetwarzanie danych biometrycznych przez szkoły na przykładzie europejskich organów nadzorczych.
7. Wytyczne dla administratorów w związku z przetwarzaniem danych biometrycznych.

Zgodnie z art. 4 pkt 14 RODO dane biometryczne oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

Zgodnie z przywołanym przepisem dane biometryczne to wszystkie dane osobowe dotyczące np. kodu DNA, wizerunku twarzy, układu linii papilarnych, tęczówki oka.

Poprzez specjalne przetwarzanie techniczne należy rozumieć wykorzystanie takich metod i środków, których celem jest dokonanie analizy cech biometrycznych oraz doprowadzenie do identyfikacji osoby fizycznej na podstawie przeprowadzonej analizy.

Przykładem specjalnego przetwarzania technicznego może być skanowanie linii papilarnych czy tęczówki oka.

Dana biometryczna jest szczególną cechą przypisaną do konkretnej osoby fizycznej i nie ulega ona zmianom na przestrzeni czasu. Są to więc dane szczególnie chronione, które należy wykorzystywać tylko w uzasadnionych przypadkach.

Przetwarzanie danych biometrycznych w szkole

Natalia Holland, Departament Skarg

Zgodnie z art. 9 ust. 1 RODO zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, biometryczne, przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

Zgodnie z art. 9 ust. 2 RODO wyżej wymieniony ustęp nie ma zastosowania, gdy zostanie spełniony jeden z wymienionych w tym przepisie warunków.

Katalog wymieniony w art. 9 ust. 2 RODO jest zamknięty. Każda z przesłanek legalizujących proces przetwarzania danych osobowych ma charakter autonomiczny i niezależny. Oznacza to, że spełnienie co najmniej jednej z nich stanowi o zgodnym z prawem przetwarzaniu danych osobowych.

Warunek ten występuje m.in. wtedy, gdy osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach – chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1 (lit. a).

Zgodnie z art. 4 ust. 11 RODO „zgoda” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Aby móc wykorzystać dane biometryczne należy spełnić kilka warunków. Administrator musi ocenić zasadność zastosowania danych biometrycznych.

Aby dokonać takiej oceny, konieczne jest udzielenie odpowiedzi na pytania:

- czy biometria jest niezbędna do osiągnięcia celu, a cel – naprawdę istotny?
- czy istnieją inne mniej inwazyjne rozwiązania? Inne metody, dzięki którym ten cel da się osiągnąć?
- czy można dać osobie, której dane dotyczą, wybór rozwiązania?

Przetwarzanie danych biometrycznych w szkole

Natalia Holland, Departament Skarg

Administrator musi ustalić podstawę prawną wykorzystywania danych biometrycznych.

Analiza tego, czy administrator jest w stanie zapewnić właściwą ochronę w przypadku przetwarzania danych biometrycznych.

Przetwarzanie danych biometrycznych nie może się odbywać z pominięciem zasady minimalizacji określonej w art. 5 ust. 1 lit. c RODO.

Zasada ta wymaga, by proces przetwarzania danych był adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których są przetwarzane.

Nie ma przepisu, który zezwalałby szkołom na pozyskiwanie od uczniów i pracowników odcisków palców w celu zapewnienia kontroli osób wchodzących do budynku. Nie uzasadniają tego nawet względy bezpieczeństwa oraz wyrażenie zgody przez zainteresowane osoby.

To, jakie dane szkoły mogą pozyskiwać od swoich pracowników oraz uczniów, regulują odpowiednio przepisy prawa pracy oraz przepisy sektorowe regulujące funkcjonowanie placówek oświatowych. Żadne z nich nie zezwalają tym podmiotom na przetwarzanie, a więc m.in. pozyskiwanie i gromadzenie odcisków palca uczniów oraz nauczycieli oraz innych pracowników np. w celu kontroli dostępu do budynku.

Prezes UODO, decyzją z 18 lutego 2020 r., nałożył karę na szkołę podstawową w związku z naruszeniem polegającym na przetwarzaniu danych biometrycznych dzieci.

Prezes UODO, po przeprowadzeniu z urzędu postępowania administracyjnego ustalił, że szkoła korzysta z czytnika biometrycznego przy wejściu do stołówki szkolnej, który identyfikuje dzieci w celu weryfikacji uiszczenia opłaty za posiłek.

Przetwarzanie danych biometrycznych w szkole

Natalia Holland, Departament Skarg

W ukaranej szkole podstawowej, zgodnie z zasadami wydawania obiadów, umieszczonymi na stronie internetowej stołówki prowadzonej przez szkołę, uczniowie, którzy nie posiadają identyfikacji biometrycznej, przepuszczają wszystkich i oczekują na końcu kolejki.

Tego typu zasady, zdaniem Prezesa UODO, wprowadzają nierówne traktowanie uczniów i ich bezpodstawne zróżnicowanie, ponieważ wyraźnie promują uczniów posiadających identyfikację biometryczną.

Prezes UODO stwierdził w swojej decyzji, że przetwarzanie danych biometrycznych nie jest niezbędne dla osiągnięcia celu, jakim jest identyfikacja uprawnienia dziecka do odebrania obiadu. Szkoła może przeprowadzić identyfikację za pomocą innych środków, które nie ingerują tak dalece w prywatność dziecka.

W tym przypadku zgoda nie może być przesłanką legalizującą przetwarzanie danych biometrycznych, albowiem udzielona przez rodziców zgoda na przetwarzanie danych biometrycznych ich dzieci nie może być uznana za dobrowolną, skoro jej brak wywoływał negatywne skutki w postaci konieczności przepuszczenia w kolejce po posiłek tych dzieci, których rodzice taką zgodę wyrazili.

Wyrok WSA, który uchylił decyzję Prezesa UODO nakładającą karę na szkołę, przetwarzającą dane biometryczne uczniów jest w opozycji do wcześniejszego orzecznictwa NSA.

WSA uznał, że UODO zbyt rygorystycznie podszedł do zasady minimalizacji danych. Sąd ten stwierdził, że wymóg niezbędności należy odczytywać łącznie z wymogiem adekwatności i stosowności, co powinno pozwolić na uwzględnienie okoliczności oraz dopuszczenie przetwarzania danych, które w istotny sposób mogą pomóc osiągnąć cele przetwarzania.

Przetwarzanie danych biometrycznych w szkole

Natalia Holland, Departament Skarg

UODO nie może się zgodzić z takim stwierdzeniem. Administrator może bowiem przetwarzać tylko te dane, które są mu niezbędne do realizacji określonego celu. Umożliwienie przetwarzania danych, które nie są niezbędne, a jedynie mogą pomóc osiągnąć cel może prowadzić do przetwarzania pod takim pretekstem nieograniczonego zakresu danych. Administrator mógłby wówczas tłumaczyć, że dane nie są niezbędne, ale mogą okazać się przydatne w realizacji danego celu. Takie podejście naruszałoby zasady minimalizacji i adekwatności.

Biorąc pod uwagę ryzyka związane z przetwarzaniem danych, zasady określone w RODO, Prezes UODO złożył do Naczelnego Sądu Administracyjnego kasację od wspomnianego wyroku WSA (sygn. akt II SA/Wa 809/20), który uchylił decyzję organu nadzorczego. Zdaniem UODO w sprawie doszło nie tylko do naruszenia zasad określonych w RODO, tj. minimalizacji i adekwatności, dobrowolności wyrażenia zgody, ale i do dyskryminacji niektórych uczniów.

Przetwarzanie danych biometrycznych dzieci z perspektywy europejskich organów nadzorczych

Maria Jęda, Departament Współpracy Międzynarodowej i Edukacji

Przyjrzyjmy się dwóm przykładom przetwarzania danych biometrycznych uczniów szkoły średniej w miejscowości na północy Szwecji oraz dwóch szkół średnich w Nicei oraz Marsylii we Francji. Obie sytuacje są do siebie bardzo podobne.

W obu przypadkach władze lokalne postanowiły zastosować technologię do rozpoznawania twarzy w ramach testu pilotażowego, eksperymentu, w przypadku Szwecji w celu monitorowania obecności grupy uczniów na lekcjach, natomiast we Francji do rozpoznawania twarzy przy wejściu do szkoły. W obu przypadkach twarze uczniów były filmowane i porównywane ze wzorem, który znajdował się w systemie.

W obu przykładach władze lokalne chciały zastosować tę technologię, aby usprawnić, ulepszyć i unowocześnić standardowe procedury szkole.

Również w obu przypadkach administratorzy uznali, że podstawą prawną dla przetwarzania danych biometrycznych uczniów będzie zgoda wyrażona przez dzieci lub ich opiekunów.

Jak do tych sytuacji odniosły się organy nadzorcze?

Szwedzki organ nadzorczy, dowiedziawszy się o sprawie z doniesień medialnych, wszczął postępowanie, w wyniku którego uznał, że:

- przetwarzanie danych biometrycznych było nieproporcjonalne i naruszało zasadę minimalizacji danych, ponieważ obejmowało więcej danych osobowych niż jest to konieczne do celu, jakim było monitorowanie obecności uczniów;
- zgoda na przetwarzanie szczególnej kategorii danych osobowych nie była dobrowolna a wymuszona z uwagi na relację zwierzchnictwa między szkołą a uczniami;
- nie spełniono wymagań dotyczących oceny skutków dla ochrony danych i nie przeprowadzono uprzednich konsultacji ze szwedzkim organem ochrony danych.

W wyniku postępowania organ szwedzki nałożył na szkołę karę.

Przetwarzanie danych biometrycznych dzieci z perspektywy europejskich organów nadzorczych

Maria Jęda, Departament Współpracy Międzynarodowej i Edukacji

W przypadku francuskim, jeszcze przed rozpoczęciem eksperymentu władze lokalne skontaktowały się z organem nadzorczym, który wydał negatywną opinię. Pomimo tego, władze lokalne zdecydowały się na jego wdrożenie. Dokonano też ocenę skutków dla ochrony danych, którą przekazano organowi nadzorczemu i kontynuowano konsultacje w tej sprawie.

Jednakże, organizacje społeczne wyraziły sprzeciw wobec eksperymentu i w lutym 2019 r. skierowały tę sprawę do sądu. W międzyczasie francuski organ nadzorczy wydał drugie stanowisko, w którym ponownie podkreślił, że:

- zastosowanie urządzenia do rozpoznawania twarzy w szkole jest sprzeczne z głównymi zasadami proporcjonalności i minimalizacji danych określonymi w RODO;
- cele polegające na zapewnieniu i usprawnieniu dostępu do szkół średnich można osiągnąć za pomocą środków, które są znacznie mniej inwazyjne pod względem prywatności i swobód, na przykład za pomocą kontroli identyfikatorów;
- urządzenia do rozpoznawania twarzy są szczególnie uciążliwe i stwarzają poważne zagrożenie dla prywatności i wolności osobistych;
- prawdopodobnie stworzą również poczucie wzmocnionego nadzoru.

W lutym 2020 r. sąd administracyjny w Marsylii uznał, że decyzja o zainstalowaniu w dwóch szkołach technologii do rozpoznawania twarzy nie była zgodna z RODO, ponieważ uczniowie nie mogli wyrazić zgody na przetwarzanie danych osobowych w sposób dobrowolny i świadomy ze względu na stosunek zwierzchnictwa wiążący uczniów z administracją szkoły.

Ponadto sąd przychylił się do stanowiska francuskiego organu nadzorczego i orzekł, że rozpoznawanie twarzy jest środkiem nieproporcjonalnym do celu, jakim jest kontrola wejść do szkoły, zwłaszcza że istnieją alternatywne środki. Sąd w obrazowy sposób odniósł się do zasady proporcjonalności wskazując, że: „Region używa młota pneumatycznego, aby uderzyć mrówkę”.

Przetwarzanie danych biometrycznych dzieci z perspektywy europejskich organów nadzorczych

Maria Jęda, Departament Współpracy Międzynarodowej i Edukacji

Podsumowując, w obu przykładach organy nadzorcze stwierdziły, że zastosowanie technologii do rozpoznawania twarzy była nieproporcjonalna co do celu, jakim było usprawnienie standardowych procedur szkolnych. Organy nadzorcze zwracają uwagę na to, że istnieją alternatywne, mniej inwazyjne sposoby dla realizacji tych celów. Zwrócono uwagę na złamanie zasady minimalizacji danych i brak ważnej podstawy prawnej, ponieważ zgoda, z uwagi na relacje zwierzchnictwa między szkołą a uczniami, była wymuszona a nie dobrowolna.

Warto zwrócić uwagę na dokument przygotowany przez Europejskiego Inspektora Ochrony Danych przy współpracy z hiszpańskim organem nadzorczym, w którym autorzy próbują zmierzyć się z powszechnymi opiniami na temat skuteczności i niezawodności technologii biometrycznej identyfikacji.

Główne tezy „14 nieporozumień odnośnie identyfikacji i uwierzytelniania biometrycznego”:

Inwazyjność: Dane biometryczne ujawniają więcej informacji na nasz temat niż nam się to wydaje. Dane zebrane do naszej identyfikacji mogą ujawnić informacje o naszej rasie, płci, stanach emocjonalnych, chorobach. Te informacje są zespolone z naszymi danymi biometrycznymi i nie możemy zapobiec ich gromadzeniu. Kto gromadzi nasze dane biometryczne, gromadzi wszystkie informacje, które te dane ujawniają. Co więcej, wykradzione hasło do zalogowania możemy zmienić, ale naszych linii papilarnych już nie.

Niedokładność: Dokładność systemów do biometrycznej identyfikacji zależy od rożnych czynników, to jest: od sprzętu do pobierania danych, warunków pobierania, np. jasność pomieszczenia lub czułość czujnika.

Nieprecyzyjność: Biometryczne podobieństwo między rodzeństwem, szczególnie bliźniakami, i krewnymi może powodować dezorientację systemów biometrycznych.

Przetwarzanie danych biometrycznych dzieci z perspektywy europejskich organów nadzorczych

Maria Jęda, Departament Współpracy Międzynarodowej i Edukacji

Nie jest odpowiednia dla wszystkich: Niektóre osoby nie mogą korzystać z pewnych typów biometrii, ponieważ ich cechy fizyczne, np. niepełnosprawność, nie są rozpoznawane przez system. Dodatkowo, wszelkie urazy, wypadki, stany zdrowia (np. paraliż), czy inne sytuacje również mogą powodować tymczasową niezgodność identyfikacji.

Można ją obejść: Istnieją procedury i techniki, które pozwalają obejść systemy uwierzytelniania biometrycznego i przyjąć tożsamość innej osoby.

Wysokie ryzyko naruszenia bezpieczeństwa: Wszelki wyciek danych biometrycznych może powodować poważne szkody, tj. kradzież tożsamości. Nasze dane mogą dostać się w niepowołane ręce, a następnie zostać wykorzystane do dokonania przestępstwa, za które później będziemy odpowiadać.

Zachęcamy również do zapoznania się z dokumentami Europejskiej Rady Ochrony Danych i jej poprzedniczki Grupy Roboczej art. 29. Wszystkie te dokumenty znajdują się w wykazie źródeł na końcu prezentacji.

Biometria w dokumentach Rady Europy

Iwona Piórkowska-Kapica, Departament Współpracy Międzynarodowej i Edukacji

Dlaczego mówimy dziś o Radzie Europy?

Oprócz tego, że jesteśmy jako Polska członkiem Unii Europejskiej i w konsekwencji każdy z nas jest zobowiązany do przestrzegania postanowień ogólnego rozporządzenia o ochronie danych osobowych, potocznie zwanego RODO, Polska jest jednocześnie członkiem Rady Europy, czyli organizacji międzynarodowej, która zajmuje się przede wszystkim promocją i ochroną praw człowieka i demokracji. Rada Europy ma swój odrębny reżim prawny, dotyczący ochrony danych osobowych. Podstawowym dokumentem Rady Europy jest Europejska Konwencja Praw Człowieka, której art. 8 wskazuje, iż każdy z nas ma prawo do poszanowania życia prywatnego i rodzinnego. Dokumentem kluczowym w obszarze ochrony danych osobowych jest Konwencja nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych, podpisana 28 stycznia 1981 r. Dla upamiętnienia tego wydarzenia corocznie obchodzimy w tym dniu Dzień Ochrony Danych Osobowych, w ramach którego, jako uczestnicy programu „Twoje dane – Twoja sprawa", aktywnie biorą Państwo udział. Wrażliwość informacji o charakterze biometrycznym została wyraźnie uznana poprzez włączenie danych jednoznacznie identyfikujących osobę do specjalnych kategorii danych w art. 6 zaktualizowanej Konwencji o ochronie osób w związku z przetwarzaniem danych.

Instytucją w ramach Rady Europy, która zajmuje się wdrażaniem Konwencji 108 jest Komitet Konsultacyjny, czyli T-PD. W ramach prac podczas posiedzeń T-PD, w których UODO, jako reprezentant Polski, bierze udział. W ostatnich miesiącach powstały dwa dokumenty, interesujące w kontekście dzisiejszego webinarium.

W ramach tej części webinarium, zwrócono uwagę na praktyczny aspekt wskazanych dokumentów. Pierwszym z nich są wytyczne dot. ochrony danych dzieci w środowisku edukacyjnym, opublikowane 20 listopada 2020 r. Drugi dokument zaś, to wytyczne dot. rozpoznawania twarzy, opublikowane 28 stycznia br. Zalecenia, które dotyczą dzisiejszego tematu, czyli procesu przetwarzania danych biometrycznych w szkole.

Biometria w dokumentach Rady Europy

Iwona Piórkowska-Kapica, Departament Współpracy Międzynarodowej i Edukacji

Jest to ostatnio bardzo ważny i istotny temat, z uwagi na karę nałożoną przez UODO na jedną ze szkół. Wykorzystanie technologii cyfrowych do celów edukacyjnych prowadzi do przetwarzania danych osobowych dzieci przez różne podmioty (od rządów krajowych, publicznych i prywatnych placówek edukacyjnych po podmioty prywatne, takie jak dostawcy produktów lub usług oraz twórcy oprogramowania, a także osoby takie jak nauczyciele, opiekunowie prawni i rówieśnicy). Przetwarzane dane są dostarczane nie tylko przez dzieci, rodziców lub wychowawców, ale są to także dane, które powstają w wyniku zaangażowania użytkownika lub dane wywnioskowane (np. na podstawie profilowania). Instytucje edukacyjne coraz częściej gromadzą dane szczególnie chronione, takie jak dane biometryczne, a gromadzenie danych może mieć konsekwencje dla dzieci na całe życie. Należy koniecznie przyznać, że edukacja i technologie cyfrowe mają wpływ nie tylko na prawo dziecka do ochrony danych, a także że prawo do prywatności oraz ochrony danych umożliwia ochronę dalszych praw dziecka. Prawo do niedyskryminacji, prawo do rozwoju, prawo do wolności wypowiedzi, prawo do zabawy i prawo do ochrony przed wyzyskiem gospodarczym również mogą być zagrożone. Należy każdorazowo rozważyć implikacji przetwarzania danych dzieci w kontekście edukacji.

Przetwarzając dane biometryczne, warto zapoznać się z wytycznymi dot. ochrony danych dzieci w środowisku edukacyjnym. Zawierają szereg dobrych praktyk, które można zastosować w sektorze oświaty.

Są one następujące:

1) Dane biometryczne nie powinny być rutynowo przetwarzane w placówkach edukacyjnych. Decydując się na przetwarzanie danych biometrycznych, należy pamiętać, że powinno być ono poprzedzone zweryfikowaniem zagrożeń, jakie przetwarzanie danych wrażliwych może stwarzać dla praw i podstawowych wolności dziecka, włączając dyskryminację przez całe życie. Wykorzystanie danych biometrycznych w placówkach edukacyjnych jest dozwolone tylko w wyjątkowych okolicznościach, dlatego warto za każdym razem zastanowić się, czy nie można zastosować mniej inwazyjnej metody, która pozwoli na osiągnięcie tego samego celu przetwarzania.

Biometria w dokumentach Rady Europy

Iwona Piórkowska-Kapica, Departament Współpracy Międzynarodowej i Edukacji

2) Wyjątki dotyczące pomocy dzieciom i personelowi edukacyjnemu z potrzebami dostępności, na przykład śledzenie wzroku na ekranie, dla ich bezpośredniej korzyści i bez dyskryminacji, powinny być przewidziane z odpowiednimi zabezpieczeniami przewidzianymi w prawie.

3) Uznając, że definicja danych biometrycznych w Artykule 6 Konwencji służy do jednoznacznej identyfikacji osoby, należy zwracać uwagę na wrażliwość przetwarzania danych dotyczących ciała i danych behawioralnych dziecka, które może nie służyć weryfikacji tożsamości. Zamiast tego celem takiego przetwarzania danych może być wpływanie na fizyczne lub psychiczne doświadczenia dziecka, na przykład we wciągającej rzeczywistości wirtualnej. Działania te powinny być wykonywane w oparciu o zasadę ostrożności i traktowane jako dane biometryczne są objęte Konwencją 108+, nawet jeśli nie służą do celów jednoznacznej identyfikacji osoby.

4) Należy zwracać szczególną uwagę na korzystanie z oprogramowania do wideokonferencji (w przypadku programów do nauczania na odległość). Pracownicy placówki edukacyjnej muszą wyrazić zgodę na warunki świadczenia usług, które obejmują przetwarzanie i nagrywanie treści, w tym obrazów dzieci i danych głosowych. Jednocześnie, należy zapewnić, by przetwarzanie danych odbywało się na podstawie świadomej i jednoznacznie dobrowolnej zgody wyrażonej przez osobę, której dane dotyczą, czyli dziecko, zgodnie z jego ewoluującymi możliwościami lub ich prawnego opiekuna, a także zgodnie ze wszystkimi innymi zasadami ochrony danych, w tym zasadą ograniczenia celu.

Integracja technologii rozpoznawania twarzy z istniejącymi systemami nadzoru stwarza poważne zagrożenie dla prawa do prywatności i ochrony danych osobowych, a także dla innych praw podstawowych, ponieważ korzystanie z tych technologii nie zawsze wymaga świadomości lub współpracy osób, których dane biometryczne są przetwarzane, biorąc pod uwagę na przykład możliwość dostępu do cyfrowych obrazów osób w Internecie.

Biometria w dokumentach Rady Europy

Iwona Piórkowska-Kapica, Departament Współpracy Międzynarodowej i Edukacji

Aby zapobiec takim naruszeniom, należy zapewnić, że używanie rozpoznawania twarzy dokonywane będzie z poszanowaniem prawa do prywatności i ochrony danych, wzmacniając w ten sposób prawa człowieka i podstawowe wolności poprzez wdrożenie wskazówek wyszczególnionych w wytycznych dot. rozpoznawania twarzy a są one następujące:

Zgodność z prawem przetwarzania danych i jakość danych

Przetwarzając dane biometryczne przy zastosowaniu technologii rozpoznawania twarzy, należy przestrzegać wszystkich obowiązujących zasad oraz przepisów dotyczących ochrony danych. W przypadku decyzji o zastosowaniu technologii rozpoznawania twarzy, należy wykazać, że takie zastosowanie jest absolutnie niezbędne i proporcjonalne w określonym kontekście ich stosowania oraz że nie koliduje z prawami osób, których dane dotyczą. Dodatkowo, należy zapewnić, że dobrowolne użycie tej technologii nie będzie miało wpływu na osoby, które przypadkowo zetkną się z nią w sposób niezamierzony.

Przejrzystość i rzetelność

Ponieważ technologie rozpoznawania twarzy mogą być wykorzystywane bez żadnego zamiaru lub bez jakiejkolwiek współpracy z osobami, których dane dotyczą, przejrzystość i rzetelność przetwarzania mają ogromne znaczenie i będą musiały zostać należycie rozważone przez podmioty stosujące tę technologię.

Czynniki, które zadecydują o tym, czy zapewniono przejrzystość i rzetelność, obejmują na przykład to, czy informacje są przekazywane osobom fizycznym, jaki jest kontekst zbierania danych, czy oczekiwania co do sposobu wykorzystania danych są rozsądne, czy rozpoznawanie twarzy jest jedynie cechą produktu lub usługi czy raczej integralną częścią samej usługi. Należy również poinformować właściwe osoby o tym, jak może wpłynąć na nie zbieranie, wykorzystywanie lub udostępnianie danych przetwarzanych dotyczących rozpoznawania twarzy, zwłaszcza gdy dotyczą one osób znajdujących się w szczególnie trudnej sytuacji. Przekazane informacje muszą również określać jakie prawa i środki ochrony prawnej przysługują osobom, których dane dotyczą.

Biometria w dokumentach Rady Europy

Iwona Piórkowska-Kapica, Departament Współpracy Międzynarodowej i Edukacji

Ograniczenie celu, minimalizacja danych oraz ograniczenie czasu ich przechowywania

Dane osobowe podlegające przetwarzaniu powinny być zbierane w wyraźnych, konkretnych i prawnie uzasadnionych celach i nie powinny być przetwarzane w sposób niezgodny z tymi celami.

Ponadto, przed jakimkolwiek kolejnym przetwarzaniem podmioty będą musiały rozważyć, czy cele nowego przetwarzania są zgodne z pierwotnie określonymi celami. W przeciwnym razie nowe przetwarzanie będzie wymagało odrębnej podstawy prawnej.

Należy przestrzegać zasady minimalizacji danych, która wymaga, aby przetwarzane były tylko wymagane informacje, a nie wszystkie dostępne informacje.

Należy również ustalić okres zatrzymywania, który nie może być dłuższy niż to, co jest niezbędne do konkretnego celu przetwarzania, oraz należy zapewnić usunięcie szablonów biometrycznych po zakończeniu tego celu. Przy określaniu okresu zatrzymywania, należy wziąć pod uwagę biometryczny charakter danych osobowych.

Prawidłowość

Należy zapewnić prawidłowość i uaktualnianie szablonów biometrycznych i obrazów cyfrowych. Na przykład, jakość obrazów i szablonów biometrycznych umieszczonych na listach obserwacyjnych musi być sprawdzona, aby zapobiec potencjalnym fałszywym dopasowaniom, ponieważ niska jakość obrazów może spowodować wzrost liczby błędów. Jest to bezpośrednio związane ze źródłami obrazów zestawionych na liście obserwacyjnej, które wymagają ścisłego przestrzegania zasad ochrony danych, takich jak zasada ograniczenia celu.

W przypadku błędnych dopasowań należy podjąć wszelkie uzasadnione kroki w celu skorygowania przyszłych zdarzeń oraz zapewnienia dokładności obrazów cyfrowych i szablonów biometrycznych.

Biometria w dokumentach Rady Europy

Iwona Piórkowska-Kapica, Departament Współpracy Międzynarodowej i Edukacji

Bezpieczeństwo danych

Jakiekolwiek niepowodzenie w zakresie bezpieczeństwa danych może mieć szczególnie poważne konsekwencje dla osób, których dane dotyczą, ponieważ nieuprawnione ujawnienie takich wrażliwych danych nie może zostać naprawione.

Należy wdrożyć silne środki bezpieczeństwa, zarówno na poziomie technicznym, jak i organizacyjnym, w celu ochrony danych dotyczących rozpoznawania twarzy i zestawów obrazów przed utratą i nieuprawnionym dostępem lub wykorzystaniem danych na wszystkich etapach przetwarzania, niezależnie od tego, czy chodzi o zbieranie, przekazywanie i przechowywanie. Należy także podjąć działania mające na celu zapobieganie atakom specyficznym dla technologii.

Każde naruszenie bezpieczeństwa danych, które może poważnie kolidować z prawami i podstawowymi wolnościami osób, których dane dotyczą, musi zostać zgłoszone organowi nadzorczemu oraz, w stosownych przypadkach, osobom, których dane dotyczą.

Środki bezpieczeństwa powinny ewoluować w czasie i w odpowiedzi na zmieniające się zagrożenia oraz zidentyfikowane ryzyka. Powinny być również proporcjonalne do wrażliwości danych, kontekstu wykorzystywania określonej technologii rozpoznawania twarzy i jej celów, prawdopodobieństwa wyrządzenia szkody osobom fizycznym a także innych istotnych czynników.

Rozliczalność

Należy podjąć wszelkie odpowiednie działania w celu wypełnienia swoich zobowiązań i wykazania, że przetwarzanie danych pod ich kontrolą jest zgodne ze zobowiązaniami, jak przewidziano w przepisach.

Należy uwzględnić niezbędne środki organizacyjne i techniczne w celu zapewnienia jakości danych biometrycznych poprzez stosowanie uzgodnionych na szczeblu międzynarodowym norm technicznych, w zależności od kontekstu ich wykorzystania.

Biometria w dokumentach Rady Europy

Iwona Piórkowska-Kapica, Departament Współpracy Międzynarodowej i Edukacji

Ocena skutków dla ochrony danych

Ostatnia, lecz nie najmniej ważna rzecz, to ocena skutków dla ochrony danych, której należy dokonać przed przetwarzaniem, ponieważ stosowanie technologii rozpoznawania twarzy wiąże się z przetwarzaniem danych biometrycznych i stanowi wysokie ryzyko naruszenia praw podstawowych osób, których dane dotyczą.

Podczas dokonywania oceny skutków należy nie tylko rozpoznać ryzyko wynikające z potencjalnego przetwarzania, ale także rozważyć niezbędne środki łagodzące, aby zaradzić tym zagrożeniom poprzez podjęcie niezbędnych środków technicznych i organizacyjnych.

W tej ocenie wyjaśnią one m.in.:

- zgodność z prawem stosowania tych technologii;
- jakie prawa podstawowe są zagrożone w procesie przetwarzania biometrycznego;
- podatność na zagrożenia osób, których dane dotyczą;
- w jaki sposób można skutecznie ograniczyć te zagrożenia.

Podsumowanie

- Dane biometryczne to wszystkie dane umożliwiające identyfikację osoby fizycznej dotyczące:
  - cech fizycznych (np. kod DNA, wizerunek twarzy, układ linii papilarnych, tęczówka oka);
  - cech fizjologicznych (np. sposób poruszania się)cech behawioralnych (np. analiza głosu).
- Nie ma przepisu, który zezwalałby szkołom na pozyskiwanie od uczniów i pracowników odcisków palców w celu zapewnienia kontroli osób wchodzących do budynku.
- Praktyka pokazuje, że konieczności przetwarzania danych biometrycznych nie uzasadniają nawet względy bezpieczeństwa oraz wyrażenie zgody przez zainteresowane osoby.
- Co do zasady nie – przetwarzamy danych biometrycznych, jeśli nie jest to konieczne.
- Jeśli zachodzi uzasadniona konieczność – należy pamiętać o tym, by przetwarzanie było zgodne z obowiązującymi przepisami prawa.
- W celu ułatwienia procesu przetwarzania danych biometrycznych, warto zapoznać się z dobrymi praktykami i wskazówkami, np.
  - Wytycznymi dot. ochrony danych dzieci w środowisku edukacyjnym;
  - Wytycznymi dot. rozpoznawania twarzy.

Źródła

- 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)
- Dane biometryczne mogą być wykorzystywane tylko w wyjątkowych sytuacjach https://uodo.gov.pl/pl/138/1943
- Szkoła z karą za odciski palca uczniów https://uodo.gov.pl/pl/138/1453
- Decyzja Prezesa UODO z 18 lutego 2020 r. sygn. ZSZZS.440.768.2018
- Opinia Grupy Roboczej Art. 29 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych (WP 193), 27.04.2012 r. https://archiwum.giodo.gov.pl/pl/1520111/4676
- Wytyczne Europejskiej Rady Ochrony Danych 3/2019 w sprawie przetwarzania danych osobowych za pomocą urządzeń wideo https://uodo.gov.pl/pl/414/1332
- Dokument: 14 nieporozumień odnośnie identyfikacji i uwierzytelniania biometrycznego (ang. 14 misunderstandings with regard to biometric identification and authentication) https://edps.europa.eu/data-protection/our-work/publications/papers/14-misunderstandings-regard-biometric-identification_en
- Dokument: „Stan biometrii" Informacje od Europejskiego Inspektora Ochrony Danych (ang. "The State of Biometrics" Update from the European Data Protection Supervisor), 7.10.2020 https://edps.europa.eu/sites/default/files/publication/20-10-07_edps_biometrics_speech_en.pdf
- Europejska Konwencja Praw Człowieka https://www.echr.coe.int/Documents/Convention_POL.pdf
- Konwencja nr 108 (zmodernizowana protokołem z 2018 r.) https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf
- Wytyczne dot. ochrony danych dzieci w środowisku edukacyjnym https://rm.coe.int/t-pd-2019-6bisrev5-eng-guidelines-education-setting-plenary-clean-2790/1680a07f2b
  wersja w jęz. polskim https://uodo.gov.pl/pl/138/1824
- Wytyczne dot. rozpoznawania twarzy https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3
  (polska wersja w przygotowaniu)

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl/tdts