Oświadczenie w sprawie inteligentnych okularów

Przyjęte 13 października 2026 r.

(Tłumaczenie robocze przygotowane przez Urząd Ochrony Danych Osobowych. Tłumaczenie nie stanowi oficjalnego tłumaczenia Europejskiej Rady Ochrony Danych.)

Europejska Rada Ochrony Danych przyjęła następujące oświadczenie:

1 Wprowadzenie

1 W miarę jak inteligentne okulary stają się powszechnie dostępne i coraz częściej wykorzystywane, stwarzają one nowe możliwości w zakresie komunikacji, pomocy i innowacji, budząc jednocześnie istotne pytania dotyczące ochrony danych osobowych i praw osób fizycznych. Niniejsze oświadczenie przedstawia wstępne przemyślenia Europejskiej Rady Ochrony Danych (EROD) na temat skutków inteligentnych okularów dla ochrony prywatności, ze szczególnym uwzględnieniem ich zdolności do przetwarzania danych osobowych w sposób, który może być trudny do zauważenia lub kontrolowania przez osoby, których dane dotyczą.

2 Na potrzeby niniejszego dokumentu inteligentne okulary definiuje się jako urządzenia do noszenia na ciele, które często wyglądają jak zwykłe okulary lub okulary przeciwsłoneczne i które posiadają możliwości przetwarzania oraz elementy, takie jak kamery, głośniki, mikrofony oraz oprogramowanie lub aplikacje, w tym systemy sztucznej inteligencji służące różnym celom (np. tłumaczeniu lub identyfikacji obiektów). Mogą one łączyć się z Internetem, urządzeniami zewnętrznymi lub aplikacjami mobilnymi w celu zapewnienia dodatkowych funkcji. Mogą być obsługiwane za pomocą poleceń głosowych lub innych technologii wprowadzania danych, takich jak opaski na nadgarstek wykrywające gesty dłoni.

3 W przypadku gdy inteligentne okulary rejestrują, gromadzą, zapisują, dostosowują, przechowują lub w inny sposób przetwarzają jakiekolwiek informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, przetwarzają one dane osobowe, a przetwarzanie to podlega zatem przepisom RODO[1].

2 Przykłady zastosowań i konkretne zagrożenia związane z inteligentnymi okularami

4 Funkcje dostępnych na rynku inteligentnych okularów są zróżnicowane. Typowe przykłady zastosowań obejmują słuchanie muzyki, nawiązywanie lub odbieranie połączeń telefonicznych, robienie zdjęć lub nagrywanie filmów, korzystanie z usług tłumaczenia w czasie rzeczywistym oraz transmisję na żywo. Niektóre inteligentne okulary mogą również zapewniać „rozszerzone” doświadczenia poprzez wyświetlanie informacji użytkownikowi.

[1] Z wyjątkiem przypadków wymienionych w art. 2 ust. 2 RODO, takich jak sytuacje, w których przetwarzanie jest prowadzone przez osobę fizyczną w ramach działalności o charakterze czysto osobistym lub domowym (zob. również sekcja III niniejszego dokumentu)

5 Funkcje te mogą być wykorzystywane na przykład jako narzędzie używane bez użycia rąk do szerokiego zakresu potrzeb oraz w różnych kontekstach osobistych lub zawodowych, takich jak komunikacja, nawigacja, pomoc dla osób niepełnosprawnych (na przykład poprzez zapewnienie pomocy audio i ostrzeganie o zagrożeniach w czasie rzeczywistym), dokumentowanie wydarzeń lub tworzenie treści na platformy mediów społecznościowych[2]. Wraz z rozwojem technologii pojawiają się nowe funkcje.

6 Jednak niektóre z najczęstszych zastosowań inteligentnych okularów, w szczególności nagrywanie, transmisje na żywo oraz udostępnianie materiałów wideo w Internecie, mogą budzić konkretne i istotne obawy dotyczące ochrony danych osobowych[3], a także innych praw i wolności[(4)], takich jak prawo do prywatności, bezpieczeństwa, wolności wypowiedzi i swobody przemieszczania się.

7 Wynika to ze sposobu noszenia i działania inteligentnych okularów. W przeciwieństwie do wielu innych urządzeń rejestrujących, umożliwiają one niemal niewidoczne lub ukryte gromadzenie, przechowywanie i inne formy przetwarzania danych osobowych, ponieważ trudno je odróżnić od zwykłych okularów. W związku z tym mogą one ułatwiać nieuprawnione rejestrowanie osób, których dane dotyczą. Ponadto niektóre inteligentne okulary mogą być wyposażone w zaawansowane mikrofony, które mogą rejestrować rozmowy w tle, w których użytkownik nie bierze udziału. Co więcej, ich ewentualne wykorzystanie, w połączeniu z systemami rozpoznawania twarzy lub głosu, rodzi bezprecedensowe pytania dotyczące wyborów społecznych i stanowi wysokie ryzyko dla praw i wolności w przestrzeni publicznej.

8 Nawet jeśli urządzenie można zidentyfikować jako inteligentne okulary, osoby fizyczne mogą nadal sprzeciwiać się filmowaniu lub nagrywaniu, między innymi dlatego, że czują się niekomfortowo z samą możliwością, że coś takiego ma miejsce[5]. Może to również skutkować subtelnym efektem społecznym, przejawiającym się w tym, osoby fizyczne zmieniają swoje zachowanie, tłumią spontaniczność i dostosowują się do norm społecznych postrzeganych jako bardziej akceptowalne ze względu na odczuwane zagrożenie związane z niekontrolowanym nadzorem.

9 Użytkownicy inteligentnych okularów powinni zawsze dbać o poszanowanie prywatności i godności innych osób oraz unikać podejmowania jakichkolwiek działań, które mogłyby wyrządzić tym osobom krzywdę za pomocą inteligentnych okularów. Istotne w tym kontekście jest wyraźne informowanie innych osób o korzystaniu z inteligentnych okularów.

10 Korzystanie z inteligentnych okularów może być również szczególnie wrażliwą kwestią w niektórych kontekstach, takich jak placówki medyczne, szkoły i inne miejsca, w których przebywają osoby niepełnoletnie, szatnie, baseny lub plaże, toalety oraz inne sytuacje o charakterze prywatnym lub intymnym. Korzystanie z nich w miejscu pracy może budzić obawy dotyczące monitorowania pracowników oraz poufności informacji podmiotu (w tym tajemnic handlowych i własności intelektualnej). W takich sytuacjach nagrywanie obrazu lub dźwięku może być niewłaściwe lub zabronione na mocy prawa krajowego lub przepisów lokalnych[6].

---

[2] Kompendium podejść dotyczących inteligentnych okularów, organy ochrony danych G7,czerwiec 2026 r., s. 2, https://www.cnil.fr/sites/default/files/2026-06/g7 dpas compendium of approches on smar glasses.pdf.

[3] Dokument roboczy dotyczący rzeczywistości rozszerzonej, Międzynarodowa Grupa Robocza ds. Ochrony Danych w Technologii, 16 czerwca 2026 r., dostępny pod adresem https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20260616-WP-Extended-Reality.html?nn=253562.

Zob. również komunikat prasowy Konferencji organów ochrony danych rządu federalnego Niemiec i krajów związkowych z dnia 24 września 2026 r.: https://www.datenschutzkonferenz-online.de/media/pm/DSK PM 3 Zwischenkonferenz 2026.pdf.

[4] Zob. Karta praw podstawowych Unii Europejskiej.

[5] Szwedzki Organ ds. Ochrony Prywatności (IMY), „Inteligentne okulary", https://www.imy.se/en/individuals/camera-surveillance/to-be-a-controller-of-personal-data/smart-glasses/.

[6] Na przykład skłoniło to niektóre placówki do wprowadzenia ograniczeń dotyczących korzystania z inteligentnych okularów na ich terenie. Zob. kompendium podejść dotyczących inteligentnych okularów", organy ochrony danych państw G7, czerwiec 2026 r., s. 2,https://www.cnil.fr/sites/default/files/2026-06/g7 dpas compendium of approches on smart glasses.pdf

.

3 Ogólne uwagi dotyczące zgodności z przepisami o ochronie danych

3.1 Określenie administratora danych

11 W zależności od okoliczności, odpowiedzialność za przetwarzanie danych osobowych za pośrednictwem inteligentnych okularów może spoczywać na różnych podmiotach, w tym na użytkowniku inteligentnych okularów, producencie urządzenia lub dostawcy powiązanej aplikacji lub usługi (w tym systemów sztucznej inteligencji). W niektórych przypadkach jeden podmiot może pełnić rolę wyłącznego administratora; w innych przypadkach dwa lub więcej podmiotów może kwalifikować się jako współadministratorzy. Ocena będzie zależała od tego, kto określa cele i środki przetwarzania[7].

12 Kwalifikacja użytkownika na mocy RODO zależy od sposobu, w jaki korzysta on z inteligentnych okularów.

13 Użytkownik inteligentnych okularów nie podlega przepisom RODO, pod warunkiem że jego działania są wykonywane w ramach działalności czysto osobistej lub domowej, poza jakimkolwiek kontekstem zawodowym lub handlowym (wyłączenie dot. czynności o czysto osobistym lub domowym charakterze[8]). Ma to miejsce na przykład wtedy, gdy użytkownik udostępnia zdjęcie lub film wyłącznie członkowi rodziny lub przyjacielowi[9] lub korzysta z urządzenia do osobistego tłumaczenia w kontekście prywatnym.

14 Wyłączenie to należy jednak interpretować w sposób zawężający[10] i rozpatrywać indywidualnie dla każdego przypadku w świetle okoliczności przetwarzania. Na przykład nie miałoby ono zastosowania, gdyby zdjęcie lub film zostały udostępnione nieokreślonej liczbie osób na publicznym koncie w mediach społecznościowych[11] lub gdyby inteligentne okulary były wykorzystywane w ramach działalności urzędowej, zawodowej, politycznej lub innej działalności o charakterze nieosobistym. W takich sytuacjach użytkownik kwalifikowałby się jako administrator lub współadministrator danych i w związku z tym musiałby przestrzegać wszystkich obowiązków przewidzianych w RODO, w szczególności dotyczących przejrzystości.

15 W każdym razie użytkownik rejestrujący głos lub obrazy za pomocą inteligentnych okularów może podlegać innym przepisom prawnym. Na przykład niektóre sposoby wykorzystania mogą podlegać przepisom prawa karnego.

16 Należy zauważyć, że RODO nadal ma zastosowanie do administratorów lub podmiotów przetwarzających, którzy zapewniają środki do przetwarzania danych osobowych w ramach takich działań osobistych lub domowych[12], takich jak producent inteligentnych okularów lub dostawca powiązanej aplikacji lub usługi (w tym systemów sztucznej inteligencji).

17 Producent inteligentnych okularów lub dostawca powiązanej aplikacji lub usługi (w tym systemów sztucznej inteligencji) może być uznany za niezależnego administratora lub współadministratora, jeżeli samodzielnie lub wspólnie określa cele i sposoby przetwarzania. Dotyczy to w szczególności sytuacji, gdy dostawca funkcji sztucznej inteligencji w inteligentnych okularach przetwarza dane osobowe w celu

---

Zob. również kolejną inicjatywę w Wolnym i Hanzeatyckim Mieście Hamburg w Niemczech, mającą na celu zaproponowanie zakazu używania inteligentnych okularów w transporcie publicznym i na basenach (tutaj).

[7] Wytyczne EROD nr 07/2020 dotyczące pojęć administratora i podmiotu przetwarzającego w RODO, wersja 2.1, przyjęte w dniu 7 lipca 2021 r.

[8] Artykuł 2 ust. 2 lit. c) RODO.

[9] Wytyczne EROD 3/2019 w sprawie przetwarzania danych osobowych za pomocą urządzeń wideo, wersja 2.0, przyjęte 29 stycznia 2020 r.

[10] Sprawa C-212/13, *František Ryneš przeciwko Úrad pro ochranu osobních údajů*, ECLI:EU:C:2014:2428.

[11] Sprawa C-101/01, *Lindqvist*, ECLI:EU:C:2003:596 oraz sprawa C-345/17, *Buivids,* ECLI:EU:C:2019:122.

[12] Motyw 18 RODO.

udzielenia użytkownikowi informacji na temat jego otoczenia, na przykład poprzez analizę obrazu z kamery wbudowanej w okulary, na którym widoczne są inne osoby.

18 Jeżeli podmioty te są administratorami danych, ponoszą odpowiedzialność za zgodność swoich operacji przetwarzania z RODO. W związku z tym nie powinny polegać na działaniach użytkowników w celu wypełnienia własnych obowiązków wynikających z RODO, takich jak przejrzystość wobec innych osób, których dane mogą być przetwarzane podczas korzystania z inteligentnych okularów.

19 Ponadto, w przypadku dalszego przetwarzania danych osobowych w nowym celu, administratorzy muszą zapewnić, aby ten nowy cel pozostawał zgodny z celem, w jakim dane zostały pierwotnie zebrane[13]. Przy ocenie zgodności należy zwrócić szczególną uwagę na kontekst, w jakim dane osobowe zostały zebrane, zwłaszcza gdy osoby, których dane dotyczą, nie mają żadnego związku z administratorem.

3.2 Przejrzystość

20 Zgodność z wymogami dotyczącymi przejrzystości, określonymi w RODO[14], stanowi poważne wyzwanie w kontekście inteligentnych okularów. Przejrzystość ma zasadnicze znaczenie dla uświadomienia osobom, których dane dotyczą – niezależnie od tego, czy są to użytkownicy, czy osoby postronne (zwane również „osobami niebędącymi użytkownikami") – że ich dane osobowe są przetwarzane oraz w jakim zakresie[15]. Informacje takie stanowią niezbędny warunek wstępny, umożliwiający osobom fizycznym wykonywanie swoich praw jako osób, których dane dotyczą.

21 Dyskretny charakter inteligentnych okularów oznacza, że osoby niebędące użytkownikami mogą nie być świadome, że przetwarzane są dane osobowe dotyczące ich[16], przez kogo jest to dokonywane i w jakich celach. Niektóre funkcje, takie jak usługi tłumaczeniowe lub korzystanie z funkcji sztucznej inteligencji, mogą być również szczególnie niewidoczne dla osób postronnych.

22 Obecny stan wiedzy na temat wskaźników na inteligentnych okularach sprawia, że wiele osób niekorzystających z nich nie zdaje sobie sprawy z tego, że ich dane są przetwarzane.

23 Tradycyjne oświadczenia dotyczące przejrzystości, które mogą służyć do informowania użytkowników i zazwyczaj zawierają informacje na temat przetwarzania danych, nie wydają się wystarczające ani odpowiednie do informowania osób niebędących użytkownikami w kontekście inteligentnych okularów. Dotyczy to w szczególności sytuacji, gdy administratorem danych jest producent inteligentnych okularów lub dostawca powiązanej aplikacji lub usługi (w tym systemów sztucznej inteligencji), a podmioty te przetwarzają dane osobowe dotyczące osób niebędących użytkownikami, ponieważ nie mają z nimi żadnych powiązań i nie są w stanie się z nimi skontaktować.

24 Biorąc pod uwagę obecny stan techniki, administratorzy i producenci powinni rozważyć połączenie szerokiego zakresu mechanizmów zapewniających przejrzystość podczas projektowania i opracowywania inteligentnych okularów, w tym środków zapewniających domyślnie natychmiastową informację o tym, że przetwarzanie ma miejsce[17], a także dostarczających informacji wymaganych na mocy RODO[18]. Środki istotne dla poinformowania osób niebędących użytkownikami o tym, że odbywa się przetwarzanie danych (co niekoniecznie musi rozwiązywać wszystkie istotne kwestie związane z przejrzystością), mogą obejmować między innymi połączenie poniższych rozwiązań:

---

[13] Art. 5 ust. 1 lit. b) i art. 6 ust. 4 RODO.

[14] Art. 12 i 13 RODO.

[15] Motyw 39 RODO.

[16] Kompendium podejść dotyczących inteligentnych okularów, organy ochrony danych państw G7, czerwiec 2026 r., s.6, https://www.cnil.fr/sites/default/files/2026-06/g7 dpas compendium of approches on smart glasses.pdf.

[17] Takie środki powinny być niemożliwe lub trudne do wyłączenia (biorąc pod uwagę stan techniki) oraz łatwe do zauważenia w praktyce przez osoby postronne.

[18] Na przykład informacje wymagane na mocy art. 12, 13 i 14.

- **Wskaźniki wizualne lub LED** – aby były skuteczne, takie wskaźniki[19] powinny być widoczne w różnych warunkach oświetleniowych i wystarczająco zauważalne, aby przyciągać uwagę osób znajdujących się w zasięgu gromadzenia danych. Powinny być aktywowane na wystarczająco długo, aby osoby te zrozumiały, że inteligentne okulary rejestrują lub nagrywają obrazy/filmy wideo w celu przetworzenia przez asystenta AI. Wskaźnik ten mógłby działać na różne sposoby, w zależności od używanej funkcji (na przykład: jego dłuższe działanie podczas nagrywania obrazu lub dźwięku; miganie podczas robienia zdjęcia; itp.), a rejestrowanie informacji nie powinno być możliwe, gdy wskaźnik jest zasłonięty.
- **Wskaźniki dźwiękowe** – Wskaźniki dźwiękowe oraz wymóg aktywacji głosowej (tj. konieczność wydania polecenia na głos przez użytkownika) również mogą zwiększyć świadomość osób postronnych, podobnie jak ma to miejsce w przypadku innych urządzeń fotograficznych lub wideo (na przykład: dźwięk kliknięcia podczas robienia zdjęcia[20]).
- Powiadomienia w **smartfonach o znajdującym się w pobliżu urządzeniu** – Kilka aplikacji mobilnych wykrywa znajdujące się w pobliżu inteligentne okulary poprzez rozpoznawanie nadawanych identyfikatorów Bluetooth powiązanych z producentami okularów. Obecnie tego typu sygnał może służyć wyłącznie do wykrywania okularów znajdujących się w pobliżu (niezależnie od tego, czy prowadzą one nagrywanie, czy nie), jednak producenci urządzeń mogliby również rozważyć wysyłanie określonych sygnałów w momencie, gdy urządzenia prowadzą nagrywanie, umożliwiając w ten sposób powiadomienie użytkowników znajdujących się w pobliżu. W każdym razie, takie powiadomienia nie powinny stanowić jedynej metody zapewnienia przejrzystości, ponieważ wykluczałoby to osoby, które nie mają tego rodzaju aplikacji aktywnej przez cały czas, a także dlatego, że użytkownik powinien zawsze mieć możliwość zaakceptowania lub odrzucenia otrzymania takiego powiadomienia na swoim urządzeniu. Ponadto aplikacja powinna być zaprojektowana w taki sposób, aby nie prowadziła do śledzenia użytkowników inteligentnych okularów.
- **Konstrukcja inteligentnych okularów –** Oprócz wskaźników, sygnalizujących aktywację funkcji inteligentnych okularów, można przewidzieć inne elementy konstrukcyjne, które pomogą osobom niekorzystającym z nich odróżnić inteligentne okulary od zwykłych okularów[21].

25 Ilekroć zgodność z wymogami dotyczącymi przejrzystości, zawartymi w RODO, opiera się na środkach technicznych, konieczne jest zapewnienie, by były one skuteczne, niemożliwe lub trudne do obejścia oraz aktualizowane w razie potrzeby.

26 EROD zaleca opracowanie standardów branżowych oraz prowadzenie kampanii uświadamiających, aby zapewnić, że osoby fizyczne potrafią rozpoznać inteligentne okulary i rozumieją, jaki rodzaj przetwarzania danych może mieć miejsce w różnych sytuacjach.

3.3 Podstawa prawna

[19] Producenci powinni również wziąć pod uwagę, że diody LED mogą być trudne lub niemożliwe do zauważenia dla osób z wadami wzroku oraz że biała dioda LED może być ogólnie mylona z odbiciem lub odblaskiem słonecznym.

[20] Japońskie rozporządzenie w sprawie zdrowego rozwoju nieletnich, które zostało zmienione w 2015 r., zakazuje nawet wyciszania dźwięku migawki w smartfonach.

[21] Zgodnie z motywem 78 RODO, zachęca się producentów inteligentnych okularów oraz dostawców powiązanych aplikacji lub usług do uwzględniania prawa do ochrony danych podczas opracowywania i projektowania takich produktów, usług i aplikacji oraz, z należytym uwzględnieniem stanu wiedzy technicznej, do zapewnienia, by administratorzy i podmioty przetwarzające dane byli w stanie wypełniać swoje obowiązki w zakresie ochrony danych.

27 Każde przetwarzanie wchodzące w zakres RODO musi mieć ważną podstawę prawną, zgodnie z art. 6 ust. 1 RODO[22]. Biorąc pod uwagę złożoność i różnorodność przetwarzania danych za pośrednictwem inteligentnych okularów, ważność każdej wybranej podstawy prawnej może wymagać oceny indywidualnej dla każdego przypadku, z uwzględnieniem przepisów krajowych, konkretnego przetwarzania i jego kontekstu oraz wszelkiego dalszego wykorzystania danych.

28 Zgoda na podstawie art. 6 ust. 1 lit. a RODO może stanowić podstawę prawną przetwarzania, o ile spełnione są warunki określone w art. 7 RODO[23]. Niektóre przepisy krajowe chronią prawo do wizerunku, co wymaga uzyskania zgody osoby na powielanie i publiczne rozpowszechnianie jej wizerunku: w takich sytuacjach zgoda będzie prawdopodobnie najbardziej odpowiednią podstawą prawną przetwarzania.

29 Jednakże w przypadku, gdy administratorem danych jest producent inteligentnych okularów lub dostawca powiązanej aplikacji lub usługi (w tym systemów sztucznej inteligencji), a przetwarza on dane osobowe dotyczące osób niebędących użytkownikami, z którymi nie ma żadnych powiązań, uzyskanie ich dobrowolnej, konkretnej, świadomej i jednoznacznej zgody, zgodnie z wymogami art. 7 RODO, byłoby trudne[24]. Zgoda uzyskana po zebraniu danych, na przykład po dokonaniu nagrania, nie byłaby ważna, ponieważ podstawa prawna musi istnieć przed rozpoczęciem przetwarzania i w trakcie jego trwania.

30 Powołanie się na prawnie uzasadnione interesy, określone w art. 6 ust. 1 lit. f RODO, jako odpowiednią podstawę prawną wymagałoby starannej analizy każdego przypadku z osobna w świetle praw, wolności i rozsądnych oczekiwań osób, których dane dotyczą[25]. Biorąc pod uwagę charakter danych, kontekst przetwarzania oraz obecny brak wystarczającej przejrzystości, który negatywnie wpływa na uzasadnione oczekiwania osób niebędących użytkownikami[26], konieczne będzie wprowadzenie wystarczających środków łagodzących w celu osiągnięcia sprawiedliwej równowagi między interesami stron. Byłoby to szczególnie trudne do wykazania w przypadku dalszego przetwarzania w celach komercyjnych wykraczających poza świadczenie usługi wyraźnie zamówionej przez użytkownika końcowego lub w przypadku trenowania sztucznej inteligencji[27], czego osoby postronne nie oczekiwałyby, zwłaszcza jeśli nie są świadome początkowego gromadzenia danych. Nawet jeśli warunki, określone w art. 6 ust. 1 lit. f RODO, są spełnione, administratorzy musieliby również zapewnić wszystkim osobom, których dane dotyczą, możliwość wniesienia sprzeciwu[28] w dowolnym momencie, co w wielu przypadkach może okazać się trudne

3.4 Inne aspekty ochrony danych

[22] W przypadku przetwarzania szczególnych kategorii danych powinno mieć również zastosowanie jedno z wyłączeń przewidzianych w art. 9 ust. 2 RODO.
[23] Wytyczne EROD 05/2020 w sprawie zgody na mocy rozporządzenia 2016/679, wersja 1.1, przyjęte 4 maja 2020 r.
[24] Tamże; zob. również Komisja Ochrony Danych, Wytyczne dotyczące stosowania kamer noszonych na ciele i kamer sportowych, styczeń 2020 r., https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Body%20Worn%20Cameras%20or%20Action%20Cameras Jan20.pdf.
[25] Aby powołać się na art. 6 ust. 1 lit. f RODO, muszą być spełnione trzy warunki łącznie, a mianowicie: (i) realizowany interes musi być prawnie uzasadniony, (ii) przetwarzanie musi być niezbędne oraz (iii) interesy lub podstawowe prawa i wolności osoby, której dane dotyczą nie mogą być nadrzędne wobec prawnie uzasadnionego interesu administratora. Zob. wytyczne EROD 1/2024 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO, wersja 1.0, 8 października 2024 r.
[26] W odniesieniu do rozsądnych oczekiwań spełnienie wymogów dotyczących przejrzystości nie oznacza samo w sobie, że osoby, których dane dotyczą, mogą racjonalnie oczekiwać przetwarzania, w szczególności w przypadku dalszego przetwarzania, takiego jak trenowanie modeli sztucznej inteligencji.
[27] Opinia EROD nr 28/2024 w sprawie niektórych aspektów ochrony danych związanych z przetwarzaniem danych osobowych w kontekście modeli sztucznej inteligencji, przyjęta 18 grudnia 2024 r.; zob. również sprawa C-252/21, *Meta przeciwko Bundeskartellamt*, ECLI:EU:C:2023:537, pkt 123.
[28] rArt.. 21 ust. 1 RODO.

31 Korzystanie z inteligentnych okularów może również budzić wątpliwości w świetle innych przepisów i zasad unijnego prawa o ochronie danych, w zależności od konkretnej funkcjonalności, kontekstu użytkowania oraz rodzaju przetwarzanych danych. W tym zakresie wiele kwestii związanych z inteligentnymi okularami pojawia się również w odniesieniu do innych technologii: na przykład wideodomofonów, kamer samochodowych, kamer noszonych na ciele przez konsumentów[29] oraz asystentów głosowych (które mogą znajdować się w domu, być wbudowane w telefon lub w inteligentnych zegarkach [30]). Ponadto, podobnie jak w przypadku każdej technologii rejestracji obrazu, nagrania mogą być udostępniane na publicznych kontach w mediach społecznościowych, a czasami są wykorzystywane do analizy zachowań i profilowania lub do celów wtórnych, w tym do trenowania sztucznej inteligencji[31].

32 Nie wchodząc szczegółowo w te kwestie, EROD przypomina w szczególności, że administratorzy oraz, w stosownych przypadkach, podmioty przetwarzające muszą również uwzględniać inne istotne obowiązki, w tym ochronę danych w fazie projektowania i domyślną ochronę danych, bezpieczeństwo przetwarzania[32], przetwarzanie szczególnych kategorii danych[33], korzystanie z usług podmiotów przetwarzających i podwykonawców przetwarzania[34] , przekazywanie danych osobowych poza Unię Europejską[35] oraz ochronę dzieci. Szczególną uwagę należy zwrócić na ochronę dzieci, które mogą być mniej świadome obecności lub konsekwencji stosowania inteligentnych okularów, a zatem bardziej narażone na potajemne lub inwazyjne przetwarzanie ich danych osobowych. Ponadto w niektórych okolicznościach[36] inteligentne okulary mogą być traktowane jako urządzenia końcowe, do których mogą mieć również zastosowanie ramy prawne dotyczące prywatności i łączności elektronicznej. Dzieje się tak w szczególności wtedy, gdy w urządzeniu wbudowane są czujniki gromadzące, lokalnie przechowujące i przetwarzające informacje (np. obrazy, filmy lub dźwięk) lub gdy informacje te są domyślnie udostępniane zdalnemu serwerowi (np. profilowi w sieci społecznościowej lub stronie internetowej).

33 Ponadto administratorzy powinni przyczyniać się do zapewnienia, by osoby, których dane dotyczą, mogły skutecznie wykonywać swoje prawa i zachować znaczącą kontrolę nad swoimi danymi osobowymi[37]. EROD zachęca do stosowania dodatkowych środków technicznych, które mogłyby ograniczyć ryzyko dla osób, których dane dotyczą, w tym:

a. Środki minimalizacji danych, takie jak ograniczenie ciągłego nagrywania, transmisji na żywo lub okresów przechowywania. W szczególności użytkownik nie powinien uzasadniać ciągłego lub masowego nagrywania innych osób wyłącznie ogólną lub hipotetyczną troską o swoje bezpieczeństwo osobiste.

---

[29] Wytyczne EROD 3/2019 w sprawie przetwarzania danych osobowych za pomocą urządzeń wideo, wersja 2.0, przyjęte 29 stycznia 2020 r.; zob. również Grupa Robocza Art. 29, Opinia nr 8/2014 w sprawie najnowszych zmian w zakresie Internetu rzeczy, 16 września 2014 r., s. 34, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223 en.pdf; oraz wytyczne EROD nr 05/2020 w sprawie zgody na mocy rozporządzenia 2016/679, wersja 1.1, przyjęte 4 maja 2020 r.

[30] Wytyczne EROD 02/2021 w sprawie wirtualnych asystentów głosowych, wersja 2.0, przyjęte 7 lipca 2021 r.

[31] Wytyczne EROD 3/2019 w sprawie przetwarzania danych osobowych za pomocą urządzeń wideo, wersja 2.0, przyjęte 29 stycznia 2020 r.;Wytyczne EROD 8/2020 w sprawie targetowania użytkowników mediów społecznościowych, wersja 2.0, przyjęte 2 września 2020 r.; Grupa Robocza Art. 29, Wytyczne w sprawie zautomatyzowanego podejmowania decyzji dotyczących osób fizycznych oraz profilowania na potrzeby rozporządzenia 2016/679, przyjęte 3 października 2017 r., ostatnio zmienione i przyjęte 6 lutego 2018 r.

[32] Wytyczne EROD 4/2019 dotyczące art. 25 „Ochrona danych w fazie projektowania oraz domyślna ochrona danych", wersja 2.0, przyjęte dnia 20 października 2020 r.

[33] Sprawa C-184/20, *OT przeciwko Vyriausioji tarnybinės etikos komisija*, ECLI:EU:C:2022:601

[34] Opinia EROD 22/2024 w sprawie niektórych obowiązków wynikających z polegania na podmiocie przetwarzającym (podmiotach przetwarzających) i podwykonawcy (podwykonawcach) przetwarzania danych, przyjęta 7 października 2024 r.; Wytyczne EROD 07/2020 w sprawie pojęć administratora i podmiotu przetwarzającego w RODO, wersja 2.1, przyjęte 7 lipca 2021 r.

[35] Wytyczne EROD 05/2021 w sprawie wzajemnych zależności między stosowaniem art. 3 a przepisami dotyczącymi międzynarodowego przekazywania danych zgodnie z rozdziałem V RODO, przyjęte dnia 18 listopada 2021 r.

[36] Wytyczne EROD 2/2023 w sprawie zakresu technicznego art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej, wersja 2.0, przyjęte 7 października 2024 r.; oraz dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) [2002] Dz.U. L 201/37

[37] Opinia GR Art. 29 8/2014 w sprawie najnowszych zmian w zakresie Internetu rzeczy, przyjęta 16 września 2014 r.

- Inne domyślne ustawienia sprzyjające ochronie prywatności oraz środki ochrony, zgodne z zasadą ochrony danych w fazie projektowania i domyślnej ochrony danych, w tym środki mające na celu zamazanie/zasłonięcie lub uniknięcie przetwarzania tożsamości osób postronnych, pseudonimizację lub anonimizację przed udostępnieniem lub ponownym wykorzystaniem. W miarę możliwości przetwarzanie to powinno odbywać się na urządzeniu. Ponadto w przypadku gdy inteligentne okulary są zaprojektowane przede wszystkim w celu zapewnienia pomocy w czasie rzeczywistym, trwałe przechowywanie zarejestrowanych danych audio, obrazów lub nagrań wideo może nie być konieczne i w związku z tym powinno być domyślnie wyłączone, chyba że jest to wymagane do zapewnienia zamierzonej funkcjonalności lub zostało celowo aktywowane przez użytkownika, z zastrzeżeniem odpowiednich zabezpieczeń.
- Ograniczenia techniczne, w tym, w stosownych przypadkach, ograniczenia oparte na lokalizacji (geofencing) w kontekstach, które mogą być szczególnie wrażliwe, w celu ograniczenia niepotrzebnego gromadzenia danych osobowych.
- Wprowadzenie „barier prywatności", które spowalniają udostępnianie treści na platformach mediów społecznościowych.

34 Wreszcie korzystanie z inteligentnych okularów może budzić obawy wykraczające poza samą tylko ochronę danych. Użytkownicy okularów z dostępem do Internetu powinni pamiętać o wszelkich obowiązujących przepisach unijnych, krajowych lub lokalnych. W zależności od okoliczności niektóre sposoby wykorzystania mogą być zabronione na mocy krajowego prawa karnego[38], cywilnego lub prawa pracy, a także innych przepisów sektorowych[39]. Nieprzestrzeganie takich przepisów może również, w zależności od okoliczności, podważyć zgodność przetwarzania danych osobowych z zasadą rzetelności zgodnie z art. 5 ust. 1 lit. a) RODO.

Wnioski

35 W miarę dalszego rozwoju inteligentnych okularów i związanych z nimi przypadków użycia przydatne mogą być dalsze wytyczne, które pozwolą kompleksowo zająć się kwestiami ochrony danych oraz zwiększyć świadomość wśród producentów, użytkowników, administratorów danych i stron trzecich.

36 EROD zwraca uwagę na znaczenie zapewnienia aktualnych i zwięzłych wytycznych, które są dostępne, łatwe do zrozumienia i praktyczne w kwestiach ochrony danych, zgodnie z podejściem opartym na ryzyku. EROD będzie dalej analizować i zajmować się kwestiami prywatności związanymi z inteligentnymi okularami, w tym w powiązaniu z innymi urządzeniami wideo, które budzą podobne wątpliwości prawne.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Anu Talus)

[38] Na przykład w niektórych sytuacjach i jurysdykcjach filmowanie obiektów objętych ochroną, wewnątrz domu, w przebieralni lub w celu nękania może stanowić przestępstwo. Ponadto udostępnianie takich zarejestrowanych danych może stanowić odrębne lub dodatkowe przestępstwo.

[39] EROD zauważa, że w niektórych innych krajach toczą się dyskusje nad projektami aktów prawnych dotyczącymi noszonych urządzeń rejestrujących (zob. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill id=202520260SB1130).