

Oświadczenie



Oświadczenie 1/2025 w sprawie zapewnienia wieku

Przyjęte 11 lutego 2025 r.¹

Europejska Rada Ochrony Danych (EROD) przyjęła następujące oświadczenie:

1. KONTEKST I CEL NINIEJSZEGO OŚWIADCZENIA

1. Europejskie ramy regulacyjne zawierają wezwanie do zwiększonej ochrony dzieci w środowisku cyfrowym. Na przykład w dyrektywie o audiowizualnych usługach medialnych², którą państwa członkowskie transponowały do prawa krajowego, podkreślono możliwość wdrożenia środków weryfikacji wieku (art. 6a i 28b), w RODO wprowadzono wymogi dotyczące dolnej granicy wieku do wyrażenia zgody na przetwarzanie danych osobowych w ramach usług społeczeństwa informacyjnego (art. 8), w akcie o usługach cyfrowych³ przywołano weryfikację wieku jako środek ograniczający ryzyko (art. 35 ust. 1), a kilka państw członkowskich wprowadziło do przepisów krajowych wymogi dotyczące dolnej granicy wieku do dokonywania czynności prawnych, wykonywania określonych praw lub dostępu do niektórych towarów i usług.
2. W różnych inicjatywach krajowych i europejskich, takich jak strategia na rzecz lepszego internetu dla dzieci (BIK+), określono ponadto zabezpieczenie wiekowe jako rozwiązanie służące poprawie dobrostanu dzieci w internecie dzięki bezpiecznemu, odpowiedniemu do wieku środowisku cyfrowemu, które jest zgodne z europejskimi prawami i zasadami cyfrowymi⁴.

¹ 24 lutego 2025 r. wprowadzono drobne poprawki do formatowania niniejszego dokumentu. 1 kwietnia 2025 r. wprowadzono dalsze niewielkie zmiany w pkt 16 i 22 lit. b).

² Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1808 z dnia 14 listopada 2018 r. zmieniająca dyrektywę 2010/13/UE w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (dyrektywa o audiowizualnych usługach medialnych) ze względu na zmianę sytuacji na rynku, <https://eur-lex.europa.eu/eli/dir/2018/1808/oj>.

³ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych), <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>.

⁴ Lepszy internet dla dzieci, Przewodnik dotyczący zapewnienia wieku, <https://better-internet-for-kids.europa.eu/en/age-assurance-guide-oldest>.

3. Na podstawie definicji zawartej w sprawozdaniu z badań „Mapping age assurance typologies and requirements” [Mapowanie typologii i wymogów zapewnienia wieku]⁵ w niniejszym dokumencie używa się terminu „zapewnienie wieku” jako „zbiorczego określenia metod stosowanych do ustalenia wieku lub grupy wiekowej danej osoby z różnym poziomem przekonania lub pewności”. W tym samym sprawozdaniu wymieniono trzy podstawowe kategorie potwierdzenia wieku: szacowanie wieku, weryfikację wieku i oświadczenie własne.
4. Zapewnienie wieku stwarza szczególne ryzyko dla ochrony danych, które może mieć negatywny wpływ nie tylko na prawo osób fizycznych do ochrony ich danych osobowych, ale również na inne prawa i wolności⁶, takie jak prawo do niedyskryminacji, prawo do integralności osoby, prawo do wolności i bezpieczeństwa osobistego oraz prawo do wolności wypowiedzi i informacji.
5. Uznając znaczenie spójnego podejścia do kwestii zapewnienia wieku na szczeblu UE, EROD pragnie przedstawić szczegółowe wytyczne i ogólne zasady wynikające z RODO, które należy uwzględnić przy przetwarzaniu danych osobowych w kontekście zapewnienia wieku.
6. Proponowane zasady mają na celu pogodzenie ochrony dzieci z ochroną danych osobowych w ramach zapewnienia wieku.
7. Priorytetowe znaczenie nadano spełnieniu wymogów dotyczących głównych zasad określonych w art. 5 RODO (zgodność z prawem, rzetelność, przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość, ograniczenie przechowywania, poufność, integralność i rozliczalność) oraz zapewnieniu, aby te zasady ochrony danych były właściwie wdrażane i zachowały odporność w dłuższej perspektywie, jak określono w art. 25 RODO „Uwzględnianie ochrony danych w fazie projektowania i domyślna ochrona danych” oraz w art. 32 RODO „Bezpieczeństwo przetwarzania”.
8. W niniejszym oświadczeniu skupiono się na zasadach mających zastosowanie do różnych przypadków użycia online, w tym wtedy, gdy dolna granica wieku jest określona przez prawo lub w inny sposób jako warunek zakupu produktów, korzystania z usług, które mogą szkodzić dzieciom, lub dokonywania czynności prawnych; oraz gdy istnieje obowiązek dochowania należytej staranności w celu ochrony dzieci (na przykład w celu zapewnienia, aby usługi projektowano lub oferowano w sposób odpowiedni do wieku).
9. EROD może również rozważyć wydanie – w stosownych przypadkach i w innych dokumentach – dodatkowych wytycznych dotyczących konkretnych przypadków użycia.

⁵ Raiz Shaffique, M., i van der Hof, S. (2024). „Mapping age assurance typologies and requirements” [Mapowanie typologii i wymogów zapewnienia wieku]. Sprawozdanie z badań, część koordynowanego przez European Schoolnet (EUN) i zleconego przez Komisję Europejską projektu Lepszy internet dla dzieci (BIK).

⁶ Na temat potencjalnego wpływu potwierdzenia wieku na prawa i wolności zob. np.: „Roadmap for age verification” [Plan działania dot. zapewnienia wieku] (Australijski Komisarz ds. e-Bezpieczeństwa, 2023) <https://www.esafety.gov.au/sites/default/files/2023-08/Age-verification-background-report.pdf?v=1731644498261>, „A safe internet by default for children and the role of age verification” [Domyślnie bezpieczny internet dla dzieci i rola zapewnienia wieku] (AEPD, 2024) <https://www.aepd.es/guides/technical-note-safe-internet-by-default-for-children.pdf> lub „Trustworthy Age Assurance?” [Wiarygodne zapewnienie wieku?], badanie zlecone przez klastę Zieloni/WSE dotyczący zielonej i społecznej gospodarki w Parlamencie Europejskim (2024) <https://www.greens-efa.eu/pl/article/document/trustworthy-age-assurance>.

2. ZASADY PROJEKTOWANIA ZGODNEGO Z RODO SYSTEMU ZAPEWNIENIA WIEKU.

2.1 Pełne i skuteczne korzystanie z praw i wolności

System zapewnienia wieku musi działać z poszanowaniem pełnego zakresu podstawowych praw⁷ i wolności osób fizycznych, a priorytetem dla wszystkich stron zaangażowanych w ten proces powinien być najlepszy interes dziecka.

10. Wdrażając system zapewnienia wieku, usługodawcy powinni uwzględnić nie tylko wpływ na prawo do ochrony danych osobowych, ale także na wszystkie prawa podstawowe osób fizycznych.
11. W szczególnym przypadku dzieci priorytetem dla wszystkich stron zaangażowanych w proces zapewnienia wieku powinien być najlepszy interes dziecka⁸. Należy zauważyć, że nie istnieje hierarchia w uwzględnianiu najlepszego interesu dziecka i należy wziąć pod uwagę wszystkie prawa dzieci⁹, w tym ich prawo do ochrony danych osobowych, do ochrony przed przemocą i wszelkimi innymi formami wykorzystywania, do uzyskania dostępu do informacji z różnych źródeł i do potraktowania ich opinii z należytą uwagą.

2.2 Oparta na analizie ryzyka ocena proporcjonalności zapewnienia wieku

Zapewnienie wieku należy zawsze wdrażać w sposób oparty na analizie ryzyka i proporcjonalny, który jest zgodny z prawami i wolnościami osób fizycznych.

12. Przy projektowaniu i świadczeniu usług dostawcy powinni przyjąć podejście oparte na analizie ryzyka. Należy wykazać konieczność i proporcjonalność stosowania środków bezpieczeństwa takich jak zapewnienie wieku, z uwzględnieniem związanego z tym ryzyka. Konieczność można wykazać przez przeprowadzenie oceny¹⁰, która pozwoli zidentyfikować i ocenić ryzyko stwarzane przez daną usługę dla dzieci¹¹, takie jak narażenie na szkodliwe kontakty lub treści. W ramach tej oceny usługodawcy mogą również wziąć pod uwagę prawa dzieci, możliwości, które stwarza środowisko cyfrowe, opinie dzieci, a także – aby zapewnić uczestnictwo odpowiednie do wieku¹² – rozwój ich zdolności.
13. Dostawcy usług muszą również przestrzegać praw i wolności użytkowników tych usług, w tym prawa do ochrony danych osobowych, i równoważyć je z koniecznością stosowania środków

⁷ W szczególności Powszechna deklaracja praw człowieka, Konwencja o ochronie praw człowieka i podstawowych wolności, Karta praw podstawowych Unii Europejskiej oraz Konwencja ONZ o prawach dziecka.

⁸ Komitet Praw Dziecka wyjaśnił, że zasada dobra dziecka „ma na celu zapewnienie pełnego i skutecznego korzystania ze wszystkich praw określonych w konwencji oraz całościowego rozwoju dziecka”. Komentarz ogólny nr 14 (2013) w sprawie prawa dziecka do zabezpieczenia jego najlepiej pojętego interesu jako sprawy nadrzędnej (art. 3 ust. 1), https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC_C_GC_14_ENG.pdf.

⁹ Komentarz ogólny nr 25 (2021) w sprawie praw dzieci w odniesieniu do środowiska cyfrowego, OHCHR, marzec 2021 r.

¹⁰ Na przykład ocena wpływu na prawa dziecka, która może, ale nie musi wchodzić w skład oceny skutków dla ochrony danych.

¹¹ Eksperti w dziedzinie praw dziecka podkreślili korzyści płynące z wykorzystywania ocen wpływu na prawa dziecka jako skutecznego narzędzia „do praktycznego i systematycznego wdrażania Konwencji [o prawach dziecka], w szczególności jej art. 3, który dotyczy priorytetowego traktowania najlepszego interesu dziecka” (w: Mukherjee, S., Pothong, K. i Livingstone, S. (2021). Ocena wpływu na prawa dziecka: Narzędzie służące wykonywaniu praw dziecka w środowisku cyfrowym. Londyn: 5Rights Foundation). Komitet Praw Dziecka wezwał ponadto państwa, aby nakazały stosowanie ocen wpływu na prawa dziecka w celu włączenia praw dziecka do procesów regulowania i projektowania środowiska cyfrowego.

¹² Komentarz ogólny nr 25 (2021) w sprawie praw dzieci w odniesieniu do środowiska cyfrowego, OHCHR, marzec 2021 r.

bezpieczeństwa, które zawsze powinny być jak najmniej inwazyjne spośród dostępnych i jednocześnie zawsze skuteczne. W wielu przypadkach zapewnienie wieku stwarza istotne ryzyko dla praw i wolności osób, których dane dotyczą, co oznacza, że należałoby przeprowadzać oceny skutków dla ochrony danych (art. 35 RODO) przed przetwarzaniem, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania. W ocenie skutków dla ochrony danych należy uwzględnić systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie, prawnie uzasadnionych interesów realizowanych przez administratora. Powinna ona również zawierać ocenę konieczności i proporcjonalności przetwarzania, identyfikować ryzyko wynikające z przetwarzania danych osobowych do celów potwierdzenia wieku oraz zawierać środki mające na celu ograniczenie tego ryzyka¹³.

14. Ocena skutków dla ochrony danych powinna stanowić wytyczne przy opracowywaniu i wdrażaniu odpowiednich środków technicznych i organizacyjnych w zakresie zgodności z przepisami o ochronie danych. To podejście oparte na analizie ryzyka ma kluczowe znaczenie przy równoważeniu potencjalnej ingerencji w prawa i wolności osób fizycznych z zamierzonym celem w tym konkretnym kontekście, którym jest bezpieczeństwo dzieci. Zawsze należy starannie ocenić zakres, stopień i nasilenie tej ingerencji pod względem wpływu na prawa i wolności¹⁴. Na przykład dostawca usług przetwarzający dane osobowe w celu sprawdzenia wieku wszystkich użytkowników tych usług przy dostępie do wszystkich treści lub usług nawet jeśli treści lub usługi są odpowiednie dla wszystkich odbiorców i pozbawione jakiegokolwiek ryzyka, nie przeszedłby pomyślnie testów konieczności i proporcjonalności.

2.3 Zapobieganie ryzyku w zakresie ochrony danych

Zapewnienie wieku nie powinno prowadzić do powstania niepotrzebnego ryzyka w zakresie ochrony danych osób fizycznych. W szczególności zapewnienie wieku nie powinno stwarzać dodatkowych możliwości identyfikacji, lokalizacji, profilowania lub śledzenia osób fizycznych przez usługodawców.

15. Usługodawcy i wszelkie osoby trzecie zaangażowane w zapewnienie wieku powinni wdrożyć skuteczne środki i zabezpieczenia, aby zapobiec stwarzaniu przez ten proces niepotrzebnego ryzyka w zakresie ochrony danych, takiego jak ryzyko wynikające z identyfikacji, lokalizacji, profilowania lub śledzenia osób fizycznych. Przetwarzanie danych osobowych w celu zapewnienia wieku nie powinno zapewniać dodatkowych środków do realizacji celów niezwiązanych z samym zapewnieniem wieku. Wymaga to wyboru podejść do zapewnienia wieku, które są w pełni zgodne z zasadą uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych (zob. sekcja 2.8), oraz wdrożenia środków gwarantujących przestrzeganie zasady rzetelności, zapewniających, aby dane osobowe nie były przetwarzane w sposób, który stwarza nieuzasadnioną szkodę, jest bezprawnie dyskryminujący, nieoczekiwany lub wprowadzający w błąd osoby, których dane dotyczą.

¹³ Wytyczne EROD dotyczące oceny skutków dla ochrony danych oraz określające, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679, <https://ec.europa.eu/newsroom/article29/items/611236/en>.

¹⁴ Wytyczne EIOD w sprawie oceny proporcjonalności środków ograniczających prawa podstawowe do prywatności i ochrony danych osobowych, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

16. Na przykład osoba fizyczna zobowiązana do poddania się weryfikacji wieku, aby uzyskać dostęp do treści dla dorosłych, nie oczekiwałaby od usługodawcy stosowania zapewnienia wieku w celu określenia jej tożsamości lub dokładnej lokalizacji geograficznej ani monitorowania, oceny czy wywnioskowania osobistych aspektów jej tożsamości. Fakt ten ma szczególne znaczenie dla zgodności z zasadami ochrony danych określonymi w art. 5 ust. 1 RODO, w tym zasadami rzetelności, przejrzystości i ograniczenia celu, oraz z przepisami art. 6 ust. 4 RODO dotyczącymi dalszego wykorzystywania danych osobowych. Podobnie zgodnie z zasadami ograniczenia celu i minimalizacji danych, które określono w art. 5 ust. 1 RODO, proces zapewnienia wieku nie powinien umożliwiać dalszego targetowania lub profilowania użytkowników, zarówno w celach komercyjnych (np. spersonalizowane reklamy), jak i w celu szkodliwego targetowania (np. nagabywania dzieci w celach seksualnych, nękania, uporczywego nękania lub molestowania). EROD przypomina, że zgodnie z motywem 75 RODO może istnieć szczególne ryzyko dla praw ochrony danych, jeżeli dane osobowe dotyczą osób fizycznych wymagających szczególnej opieki, w szczególności dzieci. Ogólnie rzecz biorąc, profilowanie osoby fizycznej na podstawie informacji wykorzystywanych w procesie zapewnienia wieku nie powinno umożliwiać uzyskania większej ilości danych na temat tej osoby i jej działań, niż jest to konieczne. Należy to zapewnić, w jak największym stopniu, także w przypadku naruszenia ochrony danych.
17. Należy unikać sytuacji nierównowagi sił, aby uniemożliwić usługodawcom narażenie osób fizycznych na niepotrzebne ryzyko w zakresie ochrony danych ze względu na brak sprawczości¹⁵. Jeśli nie jest to możliwe, sytuacje te należy rozpoznać i uwzględnić za pomocą odpowiednich środków zaradczych¹⁶. Na przykład użytkownikom, którzy nie mogą lub nie chcą stosować określonej metody zapewnienia wieku, należy zapewnić realne alternatywy, aby mogli udowodnić swój wiek. Usługodawcy powinni ponadto regularnie oceniać, czy wybrane metody i technologie, w tym metody i technologie zapewniane przez osoby trzecie, funkcjonują zgodnie z ich celami, a także dostosowywać je, aby zapewnić rzetelność przetwarzania. Osoby trzecie zaangażowane w zapewnienie wieku powinny również wspierać usługodawców w wypełnianiu obowiązków przez niewprowadzanie zbędnego ryzyka w zakresie ochrony danych oraz terminowe powiadamianie o wszelkich istotnych zmianach w ich polityce, projektach, usługach itp.

2.4 Zasada ograniczenia celu i minimalizacji danych

Usługodawcy i wszelkie osoby trzecie zaangażowane w zapewnienie wieku powinni przetwarzać jedynie te atrybuty związane z wiekiem, które są absolutnie niezbędne do ich konkretnego, wyraźnego i prawnie uzasadnionego celu.

18. W większości przypadków celem potwierdzenia wieku jest podejmowanie decyzji dotyczących kontroli dostępu ze względu na wiek, zapobieganie szkodom wyrządzanym dzieciom w internecie, oferowanie odpowiedniego projektu lub doświadczenia w zależności od wieku

¹⁵ Na przykład gdy wobec osób, których dane dotyczą, stosowany jest proces zautomatyzowanego podejmowania decyzji bez odpowiednich mechanizmów dochodzenia roszczeń lub gdy zgody nie można wyrazić dobrowolnie. Koncepcję „nierównowagi sił” omówiono w opinii EROD 08/2024 w przedmiocie ważnej zgody w kontekście modeli „zapłać lub wyraż zgodę” (Consent or Pay) wdrożonych przez duże platformy internetowe (sekcja 4.2.1.3), https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf.

¹⁶ Na podstawie wytycznych EROD 03/2022 dotyczących zwodniczych interfejsów platform społecznościowych: jak je rozpoznać i jak ich unikać (sekcja 2.3), wersja 2.0, https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf.

itp. Cel przetwarzania danych osobowych, bez względu na przypadek użycia, powinien być konkretny i wyraźny (art. 5 ust. 1 lit. b) RODO). Po zgromadzeniu danych osobowych nie należy ich dalej przetwarzać ani łączyć z dodatkowymi danymi w sposób niezgodny z tymi celami. Aby ograniczyć możliwość zmiany przeznaczenia danych osobowych, należy stosować środki techniczne takie jak technologie służące wzmocnieniu ochrony prywatności. Należy również wdrożyć środki organizacyjne, takie jak polityki i zobowiązania umowne¹⁷, które ograniczają ponowne wykorzystywanie danych osobowych.

19. Atrybutem związanym z wiekiem jest każdy atrybut wskazujący, że dana osoba fizyczna jest w określonym wieku, powyżej lub poniżej określonego wieku lub mieści się w określonej grupie wiekowej. Określenie celu wskaże odpowiednie i niezbędne atrybuty związane z wiekiem, które należy zebrać. Umożliwi to również administratorowi ocenę proporcjonalności procesu zapewnienia wieku. Wszelkie niedogodności związane z korzystaniem z praw podstawowych¹⁸ nie powinny przeważać nad korzyściami, które wynikają z tego procesu (zob. sekcja 2.2 powyżej).
20. Administrator powinien zatem gromadzić wyłącznie dane osobowe, które są niezbędne, adekwatne i istotne do zamierzonych celów. W ten sposób minimalizacja danych pomaga uzasadnić i wdrożyć zasady konieczności¹⁹ i proporcjonalności. Na przykład dostawca usług może potrzebować jedynie informacji, czy użytkownik przekroczył określony próg wiekowy, czy nie osiągnął tego progu. Można byłoby to wdrożyć za pomocą podejścia obejmującego tokeny opartego na udziale dostawcy usług będącego osobą trzecią, gdy usługodawca widzi jedynie funkcjonalny wynik procesu zapewnienia wieku (np. „powyżej” lub „poniżej” progu wiekowego)²⁰. Różne podejścia mogą być właściwe, gdy usługodawca musi wiedzieć, czy użytkownik należy do określonej grupy wiekowej lub urodził się w konkretnym roku.

2.5 Skuteczność zapewnienia wieku

Poziom skuteczności zapewnienia wieku powinien być wyraźnie odpowiedni do celu, dla którego potwierdzanie to jest przeprowadzane.

21. Środki, za pomocą których potwierdza się wiek, powinny być odpowiednie do osiągnięcia celu przetwarzania. W szczególności skuteczność wszelkich prawnie wymaganych środków

¹⁷ Na podstawie wytycznych EROD 4/2019 dotyczących artykułu 25 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych, wersja 2.0, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

¹⁸ Na podstawie wytycznych EIOD w sprawie oceny proporcjonalności środków ograniczających prawa podstawowe do prywatności i ochrony danych osobowych, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

¹⁹ Zgodnie z zestawem narzędzi EIOD w zakresie oceny konieczności środków ograniczających podstawowe prawo do ochrony danych osobowych, https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

²⁰ Dostawca usług będący osobą trzecią przeprowadza kontrolę wieku i przekazuje użytkownikowi „token wieku”, który użytkownik może przedstawić usługodawcy bez konieczności ponownego udowadniania swojego wieku. Token wieku może zawierać różne cechy użytkownika i informacje o tym, kiedy, gdzie lub w jaki sposób przeprowadzono kontrolę wieku.

zapewnienia wieku należy uznać za warunek wstępny spełnienia zasad konieczności²¹ i proporcjonalności²².

22. Skuteczność zapewnienia wieku należy oceniać w odniesieniu do kilku aspektów, w tym:

- a) Dostępności. Zapewnienie wieku powinno być szeroko dostępne dla osób fizycznych, aby sprawdzić ich wiek lub wykazać, że spełniają wymóg związany z wiekiem. W przypadku gdy niektóre kategorie osób są narażone na dyskryminację ze względu na szczególną metodę zapewnienia wieku, na przykład dlatego, że nie posiadają odpowiedniego dokumentu tożsamości, telefonu komórkowego lub z powodu niepełnosprawności, należy udostępnić alternatywne metody zapewnienia wieku, w miarę możliwości, z zachowaniem odpowiedniego poziomu prywatności, bezpieczeństwa i ochrony. Rozwiązania dotyczące zapewnienia wieku powinny być również zgodne z wszelkimi mającymi zastosowanie przepisami w zakresie dostępności²³.
- b) Wiarygodności. Zgodnie z zasadą prawidłowości (art. 5 ust. 1 lit. d) RODO) każda metoda, której celem jest ustalenie, czy osoba fizyczna spełnia wymóg związany z wiekiem, powinna zapewniać odpowiedni i spójny poziom prawidłowości przy ustalaniu, czy osoba spełnia ten wymóg. Należy udostępnić odpowiednie mechanizmy dochodzenia roszczeń, zwłaszcza w sytuacjach, gdy zautomatyzowane podejmowanie decyzji może mieć znaczący wpływ na użytkowników, np. gdy nie ustalono odpowiednio ich atrybutów związanych z wiekiem (zob. sekcja 2.7 poniżej).
- c) Odporności. System zapewnienia wieku powinien móc odpowiednio reagować w nieoczekiwanych sytuacjach i udaremniać próby wykorzystania, wobec których istnieje uzasadnione prawdopodobieństwo, że są próbami oszukania lub obejścia systemu. Należy zauważyć, że odporność ma niewielkie znaczenie w kontekście oświadczenia własnego w sprawie atrybutu związanym z wiekiem, ponieważ wiarygodność takiej metody zależy głównie od dobrej woli użytkownika²⁴.

Ponadto usługodawcy stosujący system zapewnienia wieku i wszelkie osoby trzecie zaangażowane w ten proces powinni być w stanie wykazać skuteczność i zachować przejrzystość w odniesieniu do środków, za pomocą których osiągają odpowiedni poziom dostępności, wiarygodności i odporności (zob. sekcja 2.10).

²¹ Zestaw narzędzi EIOD w zakresie oceny konieczności środków ograniczających podstawowe prawo do ochrony danych osobowych, https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

²² Wytyczne w sprawie oceny proporcjonalności środków ograniczających prawa podstawowe do prywatności i ochrony danych osobowych, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

²³ Na przykład dostępność stron internetowych i aplikacji mobilnych organów sektora publicznego oraz dostępność produktów i usług przewidziano odpowiednio w dyrektywie w sprawie dostępności stron internetowych i europejskim akcie prawnym w sprawie dostępności. Rozwiązania w zakresie zapewnienia wieku muszą być zgodne z tymi przepisami, co można osiągnąć przez spełnienie wymagań zharmonizowanej normy europejskiej określającej wymagania dotyczące dostępności produktów i usług ICT – EN 301 549 v3.2.1.

²⁴ EROD wyraziła już wcześniej poważne wątpliwości co do skuteczności oświadczenia własnego jako metody weryfikacji wieku w kontekście przetwarzania wysokiego ryzyka w wiążącej decyzji nr 2/2023 w sprawie sporu przedłożonego przez irlandzki organ nadzorczy dotyczącego TikTok Technology Limited (art. 65 RODO), https://www.edpb.europa.eu/system/files/2023-09/edpb_bindingdecision_202302_ie_sa_ttl_children_en.pdf.

2.6 Zgodność z prawem, rzetelność i przejrzystość

Usługodawcy i wszelkie osoby trzecie zaangażowane w proces zapewnienia wieku powinni zapewnić, aby przetwarzanie wszelkich danych osobowych do celów zapewnienia wieku było zgodne z prawem, rzetelne i przejrzyste dla użytkowników.

23. Usługodawcy muszą zagwarantować, że mają odpowiednią podstawę prawną zgodnie art. 6 RODO (oraz, w stosownych przypadkach, odpowiednim wyjątkiem przewidzianym w art. 9 ust. 2) do przetwarzania danych osobowych w kontekście zapewnienia wieku. Usługodawcy mogą na przykład być zobowiązani do wdrożenia systemu zapewnienia wieku, aby wypełnić obowiązek prawny (art. 6 ust. 1 lit. c) RODO), i są zobowiązani pamiętać, że zapewnienie wieku musi być proporcjonalne do prawnie uzasadnionego zamierzonego celu i wymogów określonych w art. 6 ust. 3 RODO.
24. Usługodawcy muszą ponadto zachować przejrzystość w kontaktach z użytkownikami w odniesieniu do tego, w jaki sposób i przez kogo ich dane osobowe są wykorzystywane. Jest to szczególnie istotne w przypadku, gdy w proces zapewnienia wieku zaangażowanych jest wiele stron. Przed przetwarzaniem jakichkolwiek danych osobowych do celów zapewnienia wieku należy poinformować użytkowników (zgodnie z art. 12, 13 i 14 RODO) m.in. o tym²⁵,
 - jakie dane osobowe będą przetwarzane oraz w jaki sposób będą one przetwarzane;
 - czy osoby trzecie będą zaangażowane w ten proces, a jeżeli tak, to kim są takie osoby trzecie i kim w takim przypadku są administratorzy i podmioty przetwarzające;
 - że ich dane zostaną udostępnione innym podmiotom lub przekazane do państwa trzeciego;
 - jaki jest okres przechowywania ich danych osobowych lub, jeżeli nie jest to możliwe, jakie są kryteria określania okresu przechowywania danych;
 - jakie są ich prawa w odniesieniu do ich danych osobowych (art. 15–22 RODO), w tym w jaki sposób mogą oni odwołać się od błędnej decyzji podjętej w wyniku zapewnienia wieku.
25. Przejrzystość w kontekście potwierdzenia wieku jest szczególnie ważna w odniesieniu do dzieci. Usługodawcy muszą dopilnować, aby przekazano dzieciom, w stosownych przypadkach, informacje dotyczące przejrzystości w jasny i zrozumiały dla dzieci w sposób.
26. Pojęcie przejrzystości jest zasadniczo związane z rzetelnością. Jeżeli usługodawcy nie komunikują jasno i przejrzystość tego, w jaki sposób przetwarzają informacje dotyczące osób fizycznych w celu potwierdzenia wieku, jest mało prawdopodobne, że przetwarzanie to będzie można uznać za rzetelne, co z kolei sprawia, że jest mało prawdopodobne, aby takie przetwarzanie było zgodne z prawem. W szczególności jeśli usługodawca oferuje użytkownikom różne metody weryfikacji wieku, powinien zachować przejrzystość co do skutków wynikających z każdej z tych metod z punktu widzenia ochrony danych.

²⁵ Zob. art. 29 wytycznych Grupy Roboczej w sprawie przejrzystości na podstawie rozporządzenia 2016/679, https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_pl.pdf.

2.7 Zautomatyzowane podejmowanie decyzji

Wszelkie przypadki zautomatyzowanego podejmowania decyzji w kontekście potwierdzenia wieku powinny być zgodne z RODO. W stosownych przypadkach usługodawcy i wszelkie zaangażowane osoby trzecie powinny zapewnić odpowiednie środki ochrony praw, wolności i prawnie uzasadnionych interesów osób fizycznych.

27. Prawodawca Unii przyjął szeroką definicję zautomatyzowanego podejmowania decyzji, które wymaga analizy w każdym konkretnym przypadku²⁶. Automatyczne decyzje mogą pojawić się na różnych etapach procesu zapewnienia wieku, albo w celu uzyskania dostępu do treści lub usługi, albo poprzez metody zastosowane do dokumentowania wieku.
28. W pełni zautomatyzowany proces zapewnienia wieku może wywołać skutki prawne dla zainteresowanych osób fizycznych – na przykład w odniesieniu do korzystania przez nie z wolności wypowiedzi – lub przynajmniej może znacząco wpłynąć na te osoby w podobny sposób²⁷. Wpływ zautomatyzowanego zapewnienia wieku na prawa osób fizycznych może różnić się w zależności od rodzaju treści lub usług.
29. W związku z tym usługodawcy i wszelkie osoby trzecie zaangażowane w proces zapewnienia wieku powinni zapewnić środki ochrony prawnej i odpowiednie mechanizmy dochodzenia roszczeń dla użytkowników, których atrybuty związane z wiekiem nie zostały właściwie określone. W zależności od struktury procesu zapewnienia wieku muszą oni wskazać, z kim osoba, której dane dotyczą, powinna się skontaktować, aby skorzystać z przysługujących jej praw²⁸.
30. Usługodawcy i wszelkie zaangażowane strony trzecie powinni zwracać szczególną uwagę w sytuacjach, gdy dotyczy to dzieci. Jak stwierdzono w motywie 71 RODO, wyłącznie zautomatyzowane podejmowanie decyzji, które wywołuje skutki prawne względem danej osoby lub w podobny sposób znacząco na nią wpływa, nie powinno dotyczyć dzieci. Odstępstwa od tej zasady powinny mieć miejsce jedynie w ściśle określonych okolicznościach, takich jak przypadki, w których jest to konieczne, aby „chronić dobro dziecka”²⁹. W każdym razie usługodawcy i wszelkie zaangażowane osoby trzecie powinni wdrożyć odpowiednie środki – np. realne alternatywy, mechanizmy dochodzenia roszczeń oraz, w stosownych przypadkach, interwencję człowieka – z informacjami dostosowanymi do potrzeb dzieci, jeżeli ich to dotyczy.

²⁶ Sprawa C-634/21, SCHUFA Holding (Scoring): Wyrok Trybunału (pierwsza izba) z dnia 7 grudnia 2023 r. (wniosek o wydanie orzeczenia w trybie prejudycjalnym złożony przez Verwaltungsgericht Wiesbaden – Niemcy) – OQ/Land Hessen (Odesłanie prejudycjalne – Ochrona osób fizycznych w zakresie przetwarzania danych osobowych – Rozporządzenie (UE) 2016/679 – Artykuł 22 – Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach – Biura informacji kredytowej – Zautomatyzowane wyliczenie wartości prawdopodobieństwa dotyczącej zdolności osoby do wypełnienia zobowiązań płatniczych w przyszłości („scoring”) – Wykorzystanie tej wartości prawdopodobieństwa przez osoby trzecie), <https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A62021CA0634>.

²⁷ Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679, <https://ec.europa.eu/newsroom/article29/items/612053/en>.

²⁸ Jak stwierdzono w wytycznych EROD (wspomnianych powyżej): „prawa te są wykonywalne wobec administratora tworzącego dany profil i administratora odpowiedzialnego za zautomatyzowane podjęcie decyzji dotyczącej osoby, której dane dotyczą (niezależnie od tego, czy miała miejsce interwencja ludzka), jeżeli nie jest to ten sam podmiot”.

²⁹ Na podstawie wytycznych w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679: „Mogą jednak wystąpić pewne okoliczności, w których administratorzy muszą uciec się do w pełni zautomatyzowanego podejmowania decyzji, w tym do profilowania, które wywołuje wobec dzieci skutki prawne lub w podobny sposób istotnie na nie wpływa, na przykład aby chronić ich dobro”.

2.8 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

System zapewnienia wieku należy projektować, wdrażać i oceniać z uwzględnieniem najlepiej chroniących prywatność dostępnych metod i technologii, aby spełnić wymogi RODO i skutecznie chronić prawa osób, których dane dotyczą.

31. Zgodnie z art. 25 RODO administratorzy danych zaangażowani w proces zapewnienia wieku powinni wdrożyć odpowiednie środki techniczne i organizacyjne oraz konieczne zabezpieczenia, aby zapewnić skuteczne wykonywanie wszystkich zasad ochrony danych, a w konsekwencji praw i wolności osób, których dane dotyczą. Wymóg, aby administratorzy domyślnie uwzględniali ochronę danych w fazie projektowania każdej czynności przetwarzania danych osobowych, ma również zastosowanie do podmiotów przetwarzających i na każdym etapie procesu przetwarzania danych.
32. Biorąc pod uwagę różnorodność i powagę ryzyka związanego z systemami zapewnienia wieku, zwłaszcza w sytuacjach, gdy przetwarza się dokumenty tożsamości lub szczególne kategorie danych osobowych, takie jak dane biometryczne, należy zwrócić szczególną uwagę na unikanie niepotrzebnego dostępu do danych osobowych, ich przetwarzania, udostępniania i przechowywania. Systemy zapewnienia wieku oraz wszelkie instrumenty prawne lub techniczne określające wymogi dotyczące takich systemów również należy regularnie poddawać przeglądowi i w razie potrzeby aktualizować, aby uwzględnić szybko zmieniający się krajobraz technologii służących wzmocnieniu ochrony prywatności w dziedzinie zarządzania tożsamością cyfrową.
33. Jak wspomniano w wytycznych EROD dotyczących uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych³⁰, odniesienie do „stanu wiedzy technicznej” w kontekście art. 25 RODO nakłada na administratorów danych obowiązek uwzględnienia postępu w dziedzinie technologii dostępnej na rynku przy określaniu wyżej wymienionych odpowiednich środków technicznych i organizacyjnych. Normy, najlepsze praktyki i kodeksy postępowania uznawane przez odpowiednie zainteresowane strony mogą być pomocne przy określaniu takich środków. Należy jednak sprawdzić stosowność tych środków w odniesieniu do każdej konkretnej czynności przetwarzania.
34. W związku z tym EROD zaleca, aby w oparciu o stan wiedzy technicznej w zakresie zapewnienia wieku w czasie opracowywania niniejszego dokumentu należycie uwzględnić technologie i architekturę sprzyjające danym przechowywanym przez użytkownika i bezpiecznemu lokalnemu przetwarzaniu (opartemu na urządzeniach) i zapewnić takie właściwości jak brak możliwości powiązania³¹ (z punktu widzenia różnych stron, a nawet w przypadku zmywu lub naruszenia ochrony danych) oraz selektywne ujawnianie³² danych

³⁰ Wytyczne EROD 4/2019 dotyczące artykułu 25 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych, wersja 2.0, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

³¹ Właściwość związana z brakiem możliwości powiązania oznacza, że nie można powiązać lub skorelować różnych elementów danych, działań lub transakcji z konkretną osobą, której dane dotyczą.

³² Selektywne ujawnianie jest cechą tokenów, danych uwierzytelniających i poświadczeń, która umożliwia osobom, których dane dotyczą, wymianę jedynie wybranych przez siebie informacji z konkretnymi stronami i w indywidualnych przypadkach.

osobowych pod kontrolą osoby, której dane dotyczą. Osobom, których dane dotyczą, należy ponadto udostępnić podejścia takie jak wydawanie seriami³³ danych uwierzytelniających jednorazowego użytku lub protokoły kryptograficzne, na przykład dowody z wiedzą zerową³⁴, w przypadkach gdy zapewnienie wieku może wiązać się z wysokim ryzykiem dla prywatności tych osób.

2.9 Bezpieczeństwo procesu zapewnienia wieku

Usługodawcy i wszelkie osoby trzecie zaangażowane w proces zapewnienia wieku powinni wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić odpowiedni do ryzyka poziom bezpieczeństwa.

35. Przepisy RODO zobowiązują zarówno administratorów, jak i podmioty przetwarzające do przyjęcia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych (motyw 83 i art. 32). Charakter, wrażliwość oraz ilość danych osobowych, które mogą być włączone w proces zapewnienia wieku, wskazują na potencjalne negatywne skutki, które może wywołać naruszenie ochrony danych.
36. Modele zaufania mają kluczowe znaczenie dla zapobiegania naruszeniom ochrony danych w kontekście zapewnienia wieku, ponieważ określają, w jaki sposób poszczególne strony mogą wzajemnie weryfikować swoją tożsamość i integralność. Ułatwiają one bezpieczną komunikację i wymianę danych między uczestnikami, którzy mogą nie mieć wcześniejszych powiązań. Ponadto w łagodzeniu potencjalnych negatywnych skutków naruszeń ochrony danych mogą być pomocne pseudonimizacja i szyfrowanie danych osobowych. Dla zapewnienia bezpieczeństwa w procesie zapewnienia wieku może być również niezbędne przestrzeganie zasady ograniczenia przechowywania i stosowanie krótkich okresów zatrzymywania, co obniża poziom narażenia. Za wartościowe zabezpieczenie można uznać politykę braku logów: po zweryfikowaniu wieku użytkownika nie prowadzi się rejestru danych osobowych wykorzystanych w procesie zapewnienia wieku.
37. W praktyce, biorąc pod uwagę rosnącą presję prawną na wdrożenie systemu zapewnienia wieku oraz liczbę usługodawców, którzy mogą podlegać takim przepisom, należy oczekiwać wystąpienia naruszeń zasad bezpieczeństwa. Należy ustalić, czy przyjęto wszystkie odpowiednie techniczne środki ochrony i odpowiednie środki organizacyjne, aby od razu stwierdzić naruszenie ochrony danych osobowych, co z kolei ma decydujące znaczenie dla ustalenia, czy w danym przypadku obowiązek zgłoszenia naruszenia ma zastosowanie³⁵. Kluczowym elementem każdej polityki w zakresie bezpieczeństwa danych jest zapobieganie naruszeniom, gdy to możliwe, oraz szybkie reagowanie w przypadku ich wystąpienia. W związku z tym zdolność do szybkiego przywrócenia dostępności systemu zapewnienia wieku po naruszeniu bezpieczeństwa również należy uznać za niezbędną. Podobnie kluczowe znaczenie ma to, aby zapewnić odporność ekosystemu zapewnienia wieku przez wspieranie

³³ Wydawanie seriami polega na odpowiedzi na jeden wniosek o dane uwierzytelniające od osoby, której dane dotyczą, za pomocą zestawu lub grupy danych uwierzytelniających wygenerowanych w tym samym czasie.

³⁴ Dowód z wiedzą zerową to procedura, w której jedna ze stron (dowodzący) może wykazać drugiej stronie (weryfikującemu) prawdziwość danego stwierdzenia bez ujawniania innych informacji poza potwierdzeniem, że to stwierdzenie jest prawdziwe.

³⁵ Na podstawie wytycznych EROD 9/2022 dotyczących zgłaszania naruszeń ochrony danych osobowych na podstawie RODO, https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf.

istnienia różnych alternatyw oraz luźno połączonych ze sobą stron³⁶, które nie są od siebie na tyle zależne, by awaria lub uszkodzenie jednego z nich wywołała poważne ograniczenia dostępu.

38. Chociaż środki bezpieczeństwa są niezwykle ważne dla systemu zapewnienia wieku, nie gwarantują one, że uprawniony lub nieuprawniony dostęp do danych osobowych nie wpłynie na prawa osób fizycznych. Nie mogą one zastąpić stosowania zasad konieczności, proporcjonalności lub uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych.

2.10 Rozliczalność

Usługodawcy i wszelkie zaangażowane strony trzecie powinni wdrożyć metody zarządzania, które umożliwią im wzięcie odpowiedzialności za stosowane przez nich podejście do zapewnienia wieku oraz wykazanie zgodności z ogólnym rozporządzeniem o ochronie danych i innymi wymogami prawnymi.

39. Biorąc pod uwagę zaangażowanie różnych zainteresowanych stron, zarządzanie potwierdzeniem wieku odgrywa kluczową rolę w jego rozliczalności. Zapewnienie wieku powinno odbywać się w oparciu o ramy zarządzania, aby zagwarantować, że wszystkie procesy i systemy są projektowane, wdrażane, zmieniane, dokumentowane, oceniane, użytkowane, utrzymywane i testowane lub kontrolowane w sposób zgodny z przepisami dotyczącymi ochrony danych osobowych i innymi wymogami prawnymi. Ramy te powinny obejmować co najmniej polityki ochrony danych (art. 24 ust. 2 RODO) oraz procesy ustalania priorytetów i podejmowania decyzji niezbędne do osiągnięcia celów w zakresie zgodności i odpowiedniego zarządzania ryzykiem przez cały cykl życia zapewnienia wieku.
40. Na przykład w ramach zarządzania należy określić, kto jest odpowiedzialny i w jaki sposób, z perspektywy administratora/podmiotu przetwarzającego, za jakie dokładnie działania lub operacje dotyczące przetwarzania. Ramy powinny również zapewnić, aby organy i odpowiednie zainteresowane strony mogły skutecznie kontrolować zapewnienie wieku. Ramy zarządzania mają zasadnicze znaczenie dla rozliczalności, ale również dla przejrzystości i zaufania do zapewnienia wieku. Osoby, których dane dotyczą, częściej ufają metodom, które w przejrzysty sposób informują o tym, jak działają, jak podejmowane są decyzje itp.
41. Ponadto część ram zarządzania obejmuje zapewnienie skuteczności (sekcja 2.5), uwzględnianie ochrony danych w fazie projektowania i domyślnej ochrony danych (sekcja 2.8) oraz bezpieczeństwo (sekcja 2.9) procesu zapewnienia wieku.

W imieniu Europejskiej Rady Ochrony Danych

³⁶ Strony są od siebie zależne w jak najmniejszym stopniu, co ogranicza zakres oddziaływania w przypadku zmian lub awarii.

Przewodnicząca

(Anu Talus)