

# Statement



## Oświadczenie 1/2025 w sprawie zapewnienia wieku Przyjęte 11 lutego 2025 r.<sup>1</sup>

(tłumaczenie nieoficjalne)

**Europejska Rada Ochrony Danych przyjęła następujące oświadczenie:**

### 1 KONTEKST I CEL NINIEJSZEGO OŚWIADCZENIA

1. Europejskie ramy regulacyjne wzywają do zwiększenia ochrony dzieci w środowisku cyfrowym. Na przykład w dyrektywie o audiowizualnych usługach medialnych<sup>2</sup>, którą państwa członkowskie transponowały do swoich przepisów krajowych, podkreślono możliwość wdrożenia środków weryfikacji wieku (art. 6a i 28b), w RODO wprowadzono wymogi dotyczące minimalnego wieku do celów wyrażenia zgody na przetwarzanie danych osobowych w kontekście usług społeczeństwa informacyjnego (art. 8), w akcie o usługach cyfrowych<sup>3</sup> odniesiono się do weryfikacji wieku jako środka zmniejszającego ryzyko (art. 35 ust. 1), a szereg państw członkowskich wdrożyło wymogi dotyczące minimalnego wieku do celów dokonywania czynności prawnych, wykonywania niektórych praw lub dostępu do niektórych towarów i usług do swoich własnych przepisów krajowych.
2. Ponadto różne inicjatywy krajowe i europejskie, takie jak „Lepszy internet dla dzieci” (BIK+), wskazują zabezpieczenie wiekowe jako jedno z rozwiązań służących poprawie dobrostanu dzieci w internecie dzięki bezpiecznemu, dostosowanemu do wieku środowisku cyfrowemu zgodnie z europejskimi prawami i zasadami cyfrowymi.<sup>4</sup>

<sup>1</sup> Drobne poprawki w formatowaniu tego dokumentu zostały wprowadzone 24 lutego 2025 r. 1 kwietnia 2025 r. wprowadzono dalsze niewielkie zmiany w pkt 16 i 22 lit. b).

<sup>2</sup> 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>

<sup>3</sup> 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>.

<sup>4</sup> Better Internet for Kids [Lepszy internet dla dzieci], Guide to age assurance, <https://better-internet-for-kids.europa.eu/en/age-assurance-guide-oldest>.

3. W oparciu o definicję zawartą w sprawozdaniu z badań „Mapowanie typologii i wymagań dotyczących zapewnienia wieku”<sup>5</sup>, w niniejszym dokumencie będziemy się posługiwać pojęciem „zapewnienie wieku” jako „określeniem ogólnym metod stosowanych do określenia wieku lub przedziału wiekowego danej osoby do różnych poziomów pewności”. W tym samym sprawozdaniu wymieniono trzy podstawowe kategorie zapewnienia wieku: oszacowanie wieku, weryfikację wieku i oświadczenie własne.
4. Zapewnienie wieku stwarza szczególne ryzyko dla ochrony danych, które może negatywnie wpłynąć nie tylko na prawo osób fizycznych do ochrony ich danych osobowych, ale także na inne prawa i wolności<sup>6</sup>, 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 na szczeblu UE do kwestii zapewnienia wieku, EROD pragnie przedstawić szczegółowe wytyczne i ogólne zasady wynikające z RODO, które należy wziąć pod uwagę przy przetwarzaniu danych osobowych w kontekście zapewnienia wieku.
6. Proponowane zasady mają na celu pogodzenie ochrony dzieci i ochrony danych osobowych w kontekście zapewnienia wieku.
7. Priorytetowo potraktowano spełnienie 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 zapewnienie, aby te zasady ochrony danych były właściwie wdrażane i pozostawały trwałe, jak określono w art. 25 RODO „Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych i art. 32 RODO „Bezpieczeństwo przetwarzania”.
8. Oświadczenie to koncentruje się na zasadach mających zastosowanie do różnych przypadków korzystania z internetu, w tym w przypadku, gdy minimalny wiek jest przewidziany przez prawo lub w inny sposób do zakupu produktów, korzystania z usług, które mogą szkodzić dzieciom, lub do wykonywania czynności prawnych; oraz gdy istnieje obowiązek dochowania należytej staranności w celu ochrony dzieci (na przykład w celu zapewnienia, aby usługi były projektowane lub oferowane w sposób dostosowany do wieku).
9. EROD może również rozważyć wydanie – w stosownych przypadkach i w innych dokumentach – dodatkowych wytycznych dotyczących konkretnych przypadków użycia.

## 2 ZASADY PROJEKTOWANIA ZGODNEGO Z RODO ZAPEWNIENIA WIEKU

---

<sup>5</sup> Raiz Shaffique, M., & van der Hof, S. (2024). Mapowanie typologii i wymagań dotyczących zapewnienia wieku. Sprawozdanie z badań, część projektu „Lepszy internet dla dzieci” (BIK) koordynowanego przez European Schoolnet (EUN) i zleconego przez Komisję Europejską.

<sup>6</sup> Informacje na temat potencjalnego wpływu zapewnienia wieku na prawa i wolności, zob. np.: „Roadmap for age verification” (Australian eSafety Commission, 2023) [Plan działania dot. zapewnienia wieku] (Australijski Komisarz ds. e-Bezpieczeństwa) <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” (AEPD, 2024) [„Bezpieczny internet domyślnie dla dzieci i rola zapewnienia wieku”] <https://www.aepd.es/guides/technical-note-safe-internet-by-default-for-children.pdf> lub „Trustworthy Age Assurance?” [„Wiarygodne zapewnienie wieku”] badanie zlecone przez kłaster Zielonych/WSE ds. zielonej i społecznej w Parlamencie Europejskim (2024) <https://www.greens-efa.eu/en/article/document/trustworthy-age-assurance>

## 2.1 Pełne i skuteczne korzystanie z praw i wolności

Zapewnienie wieku musi być zgodne z pełnym poszanowaniem podstawowych praw<sup>7</sup> i wolności osób fizycznych, a dobro dziecka powinno być kwestią nadrzędną dla wszystkich stron zaangażowanych w ten proces.

10. Wdrażając zapewnienie wieku, dostawcy usług powinni upewnić się, że biorą pod uwagę nie tylko wpływ na prawo do ochrony danych osobowych, ale także na wszystkie podstawowe prawa osób fizycznych.
11. W szczególnym przypadku dzieci, najlepszy interes dziecka<sup>8</sup> powinien być kwestią nadrzędną dla wszystkich stron zaangażowanych w zapewnienie wieku. Należy zauważyć, że nie ma hierarchii w uwzględnianiu najlepszego interesu dziecka i należy uwzględnić wszystkie prawa dzieci,<sup>9</sup> w tym ich prawo do ochrony danych osobowych, do ochrony przed przemocą i wszelkimi innymi formami wykorzystywania, do dostępu do informacji z różnych źródeł oraz do należytego uwzględniania ich poglądów.

## 2.2 Oparta na analizie ryzyka ocena proporcjonalności zapewnienia wieku

Zapewnienie wieku powinno być zawsze wdrażane w sposób oparty na analizie ryzyka i proporcjonalny, zgodny z prawami i wolnościami osób fizycznych.

12. Dostawcy usług powinni przyjąć podejście oparte na analizie ryzyka przy projektowaniu i świadczeniu swoich usług. Należy wykazać konieczność i proporcjonalność stosowania środków bezpieczeństwa, takich jak zapewnienie wieku, z uwzględnieniem związanego z tym ryzyka. Konieczność tę można wykazać, przeprowadzając ocenę w<sup>10</sup> celu zidentyfikowania i oceny zagrożeń, jakie dana usługa stwarza dla dzieci,<sup>11</sup> takich jak narażenie na szkodliwy kontakt lub szkodliwe treści. W ramach tej oceny dostawcy usług mogą również wziąć pod uwagę prawa dzieci, możliwości oferowane przez środowisko cyfrowe, poglądy dzieci, a także ich zmieniające się zdolności, aby zapewnić uczestnictwo dostosowane do wieku.<sup>12</sup>
13. Dostawcy usług muszą również szanować prawa i wolności swoich użytkowników, w tym prawo do ochrony ich danych osobowych, równoważąc je z potrzebą wprowadzenia środków bezpieczeństwa, które zawsze powinny być najmniej ingerujące w te dostępne i które zawsze powinny być skuteczne. W wielu przypadkach zapewnienie wieku stwarza wysokie ryzyko dla praw i wolności osób, których dane dotyczą, co wymagałoby przeprowadzenia oceny skutków dla ochrony danych („ocena skutków dla ochrony danych”, art. 35 RODO) przed przetwarzaniem, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania. Ocena skutków dla ochrony danych powinna zawierać systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, w stosownych przypadkach, prawnie uzasadnionego interesu realizowanego przez administratora. Powinna ona również zawierać ocenę konieczności i proporcjonalności przetwarzania, identyfikować ryzyko wynikające z

<sup>7</sup> W szczególności gospodarki Powszechna deklaracja praw człowieka, Europejska konwencja praw człowieka, Karta praw podstawowych Unii Europejskiej oraz Konwencja ONZ o prawach dziecka.

<sup>8</sup> Komitet Praw Dziecka ONZ wyjaśnił, że zasada najlepszego interesu „*ma na celu zapewnienie zarówno pełnego, jak i skutecznego korzystania ze wszystkich praw uznanych w konwencji, a także całościowego rozwoju dziecka*”. Uwaga ogólna nr 14 (2013) dotycząca prawa dziecka do priorytetowego traktowania jego dobra (art. 3 ust. 1), [https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC\\_C\\_GC\\_14\\_ENG.pdf](https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC_C_GC_14_ENG.pdf)

<sup>9</sup> Komentarz ogólny nr 25 (2021) w sprawie praw dziecka w odniesieniu do środowiska cyfrowego, Wysoki Komisarz Narodów Zjednoczonych ds. Praw Człowieka (OHCHR), marzec 2021 r.

<sup>10</sup> Na przykład ocena skutków dla praw dziecka („CRIA”), która może, ale nie musi być częścią oceny skutków dla ochrony danych.

<sup>11</sup> Eksperti w dziedzinie praw dziecka podkreślili korzyści płynące z wykorzystania ocen skutków dla praw dziecka (CRIA) jako skutecznego narzędzia „*do przełożenia Konwencji [o prawach dziecka] i jej art. 3, dotyczącego priorytetowego traktowania najlepszego interesu dziecka, na praktykę w konkretny, ustrukturyzowany sposób*” (w: Mukherjee, S., Pothong, K., & Livingstone, S. (2021). Ocena wpływu na prawa dziecka: Narzędzie służące realizacji praw dziecka w środowisku cyfrowym. Londyn: Fundacja 5Rights). Ponadto Komitet ONZ wezwał państwa do upoważnienia do korzystania z CRIA w celu włączenia praw dziecka do regulacji i projektowania środowiska cyfrowego.

<sup>12</sup> Komentarz ogólny nr 25 (2021) w sprawie praw dziecka w odniesieniu do środowiska cyfrowego, OHCHR, marzec 2021 r.

przetwarzania danych osobowych do celów zapewnienia wieku oraz zawierać środki mające na celu ograniczenie tego ryzyka.<sup>13</sup>

14. Ocena skutków dla ochrony danych powinna stanowić wytyczne przy opracowywaniu i wdrażaniu odpowiednich środków technicznych i organizacyjnych służących zapewnieniu zgodności z przepisami o ochronie danych. To podejście oparte na analizie ryzyka ma kluczowe znaczenie dla zrównoważenia potencjalnej ingerencji w prawa i wolności osób fizycznych z zamierzonym celem w tym szczególnym kontekście, a mianowicie bezpieczeństwem dzieci. Należy zawsze dokładnie ocenić zakres, zasięg i intensywność tej ingerencji pod względem wpływu na prawa i wolności.<sup>14</sup> Na przykład dostawca usług przetwarzający dane osobowe w celu sprawdzenia wieku wszystkich swoich użytkowników podczas uzyskiwania dostępu do wszystkich swoich treści lub usług, nawet jeśli treści lub usługi są odpowiednie dla wszystkich odbiorców i pozbawione jakiegokolwiek ryzyka, nie przeszedłby testów konieczności i proporcjonalności.

## 2.3 Zapobieganie zagrożeniom dla ochrony danych

Zapewnienie wieku nie powinno prowadzić do niepotrzebnego ryzyka dla osób fizycznych związanego z ochroną danych. W szczególności zapewnienie wieku nie powinno zapewniać dostawcom usług dodatkowych środków identyfikacji, lokalizowania, profilowania lub śledzenia osób fizycznych.

15. Dostawcy usług i wszelkie osoby trzecie zaangażowane w zapewnienie wieku powinny wdrożyć skuteczne środki i zabezpieczenia, aby zapobiec powodowaniu przez ten proces niepotrzebnych zagrożeń dla ochrony danych, takich jak zagrożenia wynikające z identyfikacji, lokalizacji, profilowania lub śledzenia osób fizycznych. Przetwarzanie danych osobowych w celu zapewnienia wieku nie powinno dostarczać dodatkowych środków służących realizacji celów niezwiązanych z samym zapewnieniem wieku.. Wymaga to wyboru podejść opartych na zapewnieniu wieku, które są w pełni zgodne z zasadą uwzględniania ochrony danych w fazie projektowania i zasadą domyślnej ochrony danych (zob. sekcja 2.8), oraz środków wykonawczych gwarantujących zasadę sprawiedliwości, zapewniających, aby dane osobowe nie były przetwarzane w sposób bez uzasadnienia szkodliwy, bezprawnie dyskryminujący, nieoczekiwany lub wprowadzający w błąd osoby, których dane dotyczą.
16. Na przykład osoba fizyczna zobowiązana do zweryfikowania swojego wieku w celu uzyskania dostępu do treści dla dorosłych nie oczekiwałaby, że dostawca usług użyje zapewnienia wieku do określenia jej tożsamości lub dokładnego położenia geograficznego lub do monitorowania, oceny lub wnioskowania o osobistych aspektach jej tożsamości. Fakt ten ma szczególne znaczenie dla zgodności z zasadami ochrony danych określonymi w art. 5 ust. 1, w tym z zasadami rzetelności, przejrzystości i ograniczenia celu, a także z przepisami art. 6 ust. 4 dotyczącymi późniejszego wykorzystywania danych osobowych. Podobnie, zgodnie z zasadami ograniczenia celu i minimalizacji danych określonymi w art. 5 ust. 1, proces zapewnienia wieku nie powinien umożliwiać dalszego targetowania lub profilowania użytkowników, w tym zarówno w odniesieniu do celów komercyjnych (np. reklamy spersonalizowane), jak i złośliwego targetowania (np. uwodzenie, zastraszanie, prześladowanie lub nękanie). EROD przypomina, że zgodnie z motywem 75, prawa do ochrony danych mogą być szczególnie zagrożone, jeżeli dane osobowe dotyczą osób fizycznych wymagających szczególnego traktowania, w szczególności dzieci. Ogólnie rzecz biorąc, nie powinno być możliwe dowiedzenie się więcej niż to konieczne o osobie fizycznej i jej działaniach poprzez profilowanie tej osoby na podstawie informacji wykorzystywanych w procesie zapewnienia wieku. Należy to zapewnić w najszerszym możliwym zakresie, również w przypadku naruszenia ochrony danych.

---

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

<sup>14</sup> Wytyczne EIOD w sprawie oceny proporcjonalności środków ograniczających podstawowe prawa do prywatności i ochrony danych osobowych, [https://www.edps.europa.eu/sites/default/files/publication/19-02-25\\_proportionality\\_guidelines\\_en.pdf](https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf)

17. Należy unikać sytuacji braku równowagi sił, aby uniemożliwić dostawcom usług zmuszanie osób fizycznych do stawienia czoła niepotrzebnym zagrożeniom dla ochrony danych ze względu na brak sprawczości.<sup>15</sup> Jeżeli nie jest to możliwe, sytuacje te należy uznać i uwzględnić za pomocą odpowiednich środków zaradczych.<sup>16</sup> Na przykład użytkownikom, którzy nie mogą lub nie chcą korzystać z określonej metody zapewnienia wieku, należy zapewnić realne alternatywy w celu udowodnienia ich wieku. Ponadto dostawcy usług powinni regularnie oceniać, czy wybrane metody i technologie, w tym te dostarczane przez osoby trzecie, funkcjonują zgodnie z ich celami, i dostosowywać je, aby zapewnić rzetelność przetwarzania. Osoby trzecie zaangażowane w zapewnianie wieku powinny również starać się wspierać dostawców usług w wypełnianiu ich obowiązków, nie wprowadzając zbędnych zagrożeń dla ochrony danych oraz terminowo powiadamiając o wszelkich istotnych zmianach w swoich politykach, projektach, usługach itp.

## 2.4 Ograniczenie celu i minimalizacja danych

Dostawcy usług i wszelkie osoby trzecie zaangażowane w zapewnianie wieku powinny przetwarzać wyłącznie *atrybuty* związane z wiekiem, które są absolutnie niezbędne do ich określonego, wyraźnego i prawnie uzasadnionego celu.

18. W większości przypadków celem zapewnienia wieku jest podejmowanie związanych z wiekiem decyzji dotyczących kontroli dostępu, zapobieganie szkodom w internecie dla dzieci, oferowanie odpowiedniego projektu lub doświadczenia w zależności od wieku itp. Niezależnie od przypadku użycia cel przetwarzania danych osobowych powinien być konkretny i wyraźny (art. 5 ust. 1 lit. b) RODO). Po zebraniu danych osobowych nie mogą one być dalej przetwarzane ani łączone 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 („PET”). Należy również wdrożyć środki organizacyjne, takie jak polityki i zobowiązania umowne, które ograniczają ponowne wykorzystywanie danych osobowych.<sup>17</sup>
19. Atrybut związany z wiekiem to dowolny atrybut wskazujący, że osoba fizyczna jest w określonym wieku, powyżej lub poniżej określonego wieku lub w określonym przedziale wiekowym. Specyfikacja celu określi odpowiednie i niezbędne atrybuty związane z wiekiem, które należy gromadzić. Pozwoli to również administratorowi ocenić proporcjonalność procesu zapewnienia wieku. Korzyści wynikające z tego procesu nie powinny być równoważone żadnymi niedogodnościami związanymi z korzystaniem z praw podstawowych<sup>18</sup> (zob. sekcja 2.2 powyżej).
20. Administrator powinien zatem gromadzić wyłącznie dane osobowe, które są niezbędne, adekwatne i istotne do celów, które mają być realizowane. W ten sposób minimalizacja danych pomaga uzasadnić i wdrożyć zasady konieczności<sup>19</sup> i proporcjonalności. Na przykład dostawca usług może tylko wiedzieć, czy użytkownik przekroczył lub nie przekroczył progu wiekowego. Można to wdrożyć za pomocą tokenizowanego podejścia opartego na udziale dostawcy usług będącego osobą trzecią, w którym

<sup>15</sup> Na przykład gdy osoby, których dane dotyczą, stają w obliczu zautomatyzowanego podejmowania decyzji bez odpowiednich mechanizmów dochodzenia roszczeń lub gdy nie można dobrowolnie wyrazić zgody. Koncepcję „nierównowagi sił” omówiono w opinii EROD 08/2024 w sprawie ważnej zgody w kontekście modeli zgoda lub zapłata wdrażanych przez duże platformy internetowe (sekcja 4.2.1.3), [https://www.edpb.europa.eu/system/files/2024-04/edpb\\_opinion\\_202408\\_consentorpay\\_en.pdf](https://www.edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf)

<sup>16</sup> Z wytycznych EROD 03/2022 w sprawie zwodniczych wzorców projektowych w interfejsach platform mediów społecznościowych: jak je rozpoznać i 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](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)

<sup>17</sup> Z wytycznych EROD nr 4/2019 dotyczących art. 29 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](https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf)

<sup>18</sup> Z wytycznych EIOD w sprawie oceny proporcjonalności środków ograniczających podstawowe prawa do prywatności i ochrony danych osobowych, [https://www.edps.europa.eu/sites/default/files/publication/19-02-25\\_proportionality\\_guidelines\\_en.pdf](https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf)

<sup>19</sup> Z zestawu narzędzi EIOD do 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](https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf)

dostawca usług widzi jedynie funkcjonalny wynik procesu zapewnienia wieku (np. „przekroczenie” lub „poniżej” progu wieku).<sup>20</sup> Różne podejścia mogą być istotne, gdy usługodawca musi wiedzieć, czy użytkownik znajduje się w określonym przedziale wiekowym, czy też urodził się w określonym roku.

## 2.5 Skuteczność zapewnienia wieku

Zapewnienie wieku powinno wyraźnie osiągnąć poziom skuteczności adekwatny do celu, dla którego jest przeprowadzane.

21. Środki, za pomocą których przeprowadzane jest zapewnienie wieku, powinny być odpowiednie do osiągnięcia celu przetwarzania. W szczególności skuteczność wszelkich prawnie umocowanych środków zapewnienia wieku należy uznać za warunek wstępny spełnienia zasad konieczności<sup>21</sup> i proporcjonalności.<sup>22</sup>
22. Skuteczność zapewnienia wieku należy oceniać w odniesieniu do kilku aspektów, w tym:
  - a) Dostępności. Zapewnienie wieku powinno być szeroko dostępne dla osób fizycznych w celu weryfikacji ich wieku lub udowodnienia, że spełniają wymóg związany z wiekiem. W przypadku gdy niektóre kategorie osób są narażone na dyskryminację ze względu na określoną metodę zapewnienia wieku, na przykład dlatego, że nie posiadają odpowiedniego dokumentu tożsamości lub telefonu komórkowego, lub ze względu na niepełnosprawność, należy udostępnić alternatywne metody zapewnienia wieku, o ile jest to racjonalnie możliwe, z zachowaniem odpowiedniego poziomu prywatności, bezpieczeństwa i ochrony. Rozwiązania zapewniające wiek powinny być również zgodne z wszelkimi obowiązującymi przepisami dotyczącymi dostępności.<sup>23</sup>
  - b) Wiarygodności. Zgodnie z zasadą prawidłowości (art. 5 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 spełnia ten wymóg. Należy udostępnić odpowiednie mechanizmy dochodzenia roszczeń, zwłaszcza gdy zautomatyzowane podejmowanie decyzji może mieć znaczący wpływ na użytkowników, na przykład gdy ich atrybuty związane z wiekiem nie zostały odpowiednio ustalone (zob. sekcja 2.7 poniżej).
  - c) Odporności. Zapewnienie wieku powinno być w stanie poradzić sobie z nieoczekiwanymi sytuacjami i oprzeć się racjonalnie prawdopodobnym próbom oszukania lub obejścia systemu. Należy zauważyć, że odporność ma niewielkie znaczenie w kontekście oświadczenia własnego dotyczącego atrybutu związanego z wiekiem, ponieważ wiarygodność takiej metody zależy głównie od dobrej woli użytkownika.<sup>24</sup>

Ponadto dostawcy usług wdrażający mechanizm zapewnienia wieku oraz wszelkie osoby trzecie zaangażowane w ten proces powinny być w stanie wykazać jego skuteczność oraz zapewnić

<sup>20</sup> Dostawca zewnętrzny przeprowadza kontrolę wieku i dostarcza użytkownikowi „token wieku”, który użytkownik może przedstawić dostawcy usług bez konieczności ponownego udowadniania swojego wieku. Token wieku może zawierać różne atrybuty użytkownika oraz informacje o tym, kiedy, gdzie i w jaki sposób przeprowadzono kontrolę wieku.

<sup>21</sup> Zestaw narzędzi EIOD do 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](https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf)

<sup>22</sup> Wytyczne w sprawie oceny proporcjonalności środków ograniczających podstawowe prawa do prywatności i ochrony danych osobowych,

[https://www.edps.europa.eu/sites/default/files/publication/19-02-25\\_proportionality\\_guidelines\\_en.pdf](https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf)

<sup>23</sup> Na przykład dostępność stron internetowych i aplikacji mobilnych sektora publicznego oraz dostępność produktów i usług są przewidziane odpowiednio w dyrektywie w sprawie dostępności stron internetowych (WAD) i europejskim akcie w sprawie dostępności (EAA). Rozwiązania zapewniające wiek muszą być zgodne z tymi przepisami, spełniając wymogi zharmonizowanej normy europejskiej dotyczącej wymogów dostępności produktów i usług ICT, EN 301 549 v3.2.1.

<sup>24</sup> EROD wyraziła wcześniej poważne wątpliwości co do skuteczności oświadczenia własnego jako metody weryfikacji wieku w kontekście przetwarzania wysokiego ryzyka w wiążącej decyzji 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\\_tl\\_children\\_en.pdf](https://www.edpb.europa.eu/system/files/2023-09/edpb_bindingdecision_202302_ie_sa_tl_children_en.pdf)

przejrzystość w odniesieniu do środków, za pomocą których osiągają odpowiedni poziom dostępności, wiarygodności i odporności (zob. sekcja 2.10).

## 2.6 Zgodność z prawem, rzetelność i przejrzystość

Dostawcy usług i wszelkie osoby trzecie zaangażowane w zapewnienie wieku powinny zapewnić, aby przetwarzanie wszelkich danych osobowych do celów zapewnienia wieku było zgodne z prawem, rzetelne i przejrzyste dla użytkowników.

23. Dostawcy usług muszą zapewnić, aby mieli mającą zastosowanie podstawę prawną na mocy art. 6 RODO (oraz, w stosownych przypadkach, mający zastosowanie wyjątek określony w art. 9 ust. 2) do przetwarzania danych osobowych w kontekście zapewnienia wieku. Na przykład mogą być oni zmuszeni do wdrożenia zapewnienia wieku w celu wywiązania się z obowiązku prawnego (art. 6 ust. 1 lit. c) RODO), biorąc pod uwagę, że zapewnienie wieku musi być proporcjonalne do prawnie uzasadnionego zamierzonego celu i wymogów określonych w art. 6 ust. 3 RODO.
24. Ponadto dostawcy usług muszą w przejrzysty sposób informować użytkowników o tym, w jaki dokładnie sposób i przez kogo wykorzystywane są ich dane osobowe. Jest to szczególnie ważne, gdy w proces zapewnienia wieku zaangażowanych jest wiele stron. Przed przetwarzaniem jakichkolwiek danych osobowych do celów zapewnienia wieku użytkownicy muszą zostać poinformowani (zgodnie z art. 12, 13 i 14 RODO), między innymi o tym:<sup>25</sup>
  - jakie dane osobowe będą przetwarzane i w jaki sposób;
  - czy osoby trzecie będą zaangażowane w ten proces, a jeśli tak, to kim są i kim są administratorzy i podmioty przetwarzające w tym scenariuszu;
  - czy ich dane będą udostępniane innym podmiotom lub przekazywane do państwa trzeciego;
  - jak długo ich dane osobowe będą przechowywane lub, jeżeli nie jest to możliwe, kryteria ustalania okresu przechowywania;
  - jakie są ich prawa w odniesieniu do ich danych osobowych (art. 15–22 RODO), w tym w jaki sposób mogą zakwestionować nieprawidłową decyzję podjętą w wyniku zapewnienia wieku.
25. Przejrzystość w kontekście zapewnienia wieku jest szczególnie ważna w przypadku dzieci. Dostawcy usług muszą dopilnować, aby w stosownych przypadkach przekazywali dzieciom informacje dotyczące przejrzystości w sposób jasny i łatwy do zrozumienia.
26. Pojęcie przejrzystości jest zasadniczo związane z rzetelnością. Jeżeli dostawcy usług nie zapewniają jasności i przejrzystości co do tego, w jaki sposób przetwarzają informacje o osobach fizycznych w celu zapewnienia wieku, jest mało prawdopodobne, aby takie przetwarzanie można było uznać za rzetelne, co z kolei sprawia, że jest mało prawdopodobne, aby takie przetwarzanie było zgodne z prawem. W szczególności, jeśli dostawca oferuje użytkownikom różne metody weryfikacji ich wieku, powinien zapewnić przejrzystość w zakresie wpływu, jaki każda metoda ma z perspektywy ochrony danych.

## 2.7 Zautomatyzowane podejmowanie decyzji

Wszelkie przypadki zautomatyzowanego podejmowania decyzji w kontekście zapewnienia wieku powinny być zgodne z RODO. W stosownych przypadkach dostawcy usług i wszelkie zaangażowane

---

<sup>25</sup> Zob. wytyczne Grupy Roboczej Art. 29 dotyczące przejrzystości na mocy rozporządzenia 2016/679, [https://www.edpb.europa.eu/system/files/2023-09/wp260rev01\\_en.pdf](https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf).

osoby trzecie powinni zapewnić odpowiednie środki ochrony praw, wolności i prawnie uzasadnionych interesów osób fizycznych.

27. Prawodawca unijny opowiedział się za szeroką definicją zautomatyzowanego podejmowania decyzji, która wymaga analizy poszczególnych przypadków.<sup>26</sup> Zautomatyzowane decyzje mogą być podejmowane na różnych etapach procesu zapewnienia wieku, zarówno w celu uzyskania dostępu do treści lub usługi, jak i za pomocą metod wdrożonych w celu udowodnienia wieku.
28. W pełni zautomatyzowane zapewnienie wieku może wywoływać skutki prawne dla zainteresowanych osób fizycznych – na przykład w odniesieniu do korzystania przez nie z wolności wypowiedzi – lub co najmniej może znacząco wpływać na nie w podobny sposób.<sup>27</sup> Wpływ automatycznego zapewnienia wieku na prawa osób fizycznych może być różny w zależności od rodzaju treści lub usług.
29. W związku z tym dostawcy usług i wszelkie osoby trzecie zaangażowane w zapewnianie wieku powinny zapewnić środki ochrony prawnej i odpowiednie mechanizmy dochodzenia roszczeń dla użytkowników, których atrybuty związane z wiekiem nie są odpowiednio ustalone. W zależności od struktury procesu zapewnienia wieku muszą oni określić, z kim osoba, której dane dotyczą, powinna się skontaktować, aby skorzystać ze swoich praw.<sup>28</sup>
30. Dostawcy usług i wszelkie zaangażowane strony trzecie powinni zwracać szczególną uwagę na 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. Wyjątki od tej zasady powinny być stosowane w ograniczonych okolicznościach, takich jak konieczność „ochrony dobra dziecka”<sup>29</sup>. W każdym przypadku dostawcy usług i każda zaangażowana strona trzecia powinni wdrożyć odpowiednie środki – np. realne alternatywy, mechanizmy dochodzenia roszczeń oraz, w stosownych przypadkach, interwencję człowieka – wraz z informacjami dostosowanymi w stosownych przypadkach do potrzeb dzieci.

## 2.8 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

Zapewnienie wieku powinno być projektowane, wdrażane i oceniane z uwzględnieniem najbardziej chroniących prywatność dostępnych metod i technologii w celu spełnienia wymogów RODO i skutecznej ochrony praw osób, których dane dotyczą.

31. Zgodnie z art. 25 RODO administratorzy danych zaangażowani w zapewnianie wieku powinni wdrożyć odpowiednie środki techniczne i organizacyjne oraz niezbędne zabezpieczenia, aby zapewnić skuteczne wdrożenie wszystkich zasad ochrony danych, a w konsekwencji praw i wolności osób, których dane dotyczą. Wymóg domyślnego uwzględniania przez administratorów ochrony danych w

<sup>26</sup> 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 związku z przetwarzaniem danych osobowych – Rozporządzenie (UE) 2016/679 – Artykuł 22 – Zautomatyzowane podejmowanie decyzji indywidualnych – Agencje informacji kredytowej – Zautomatyzowane ustalanie wartości prawdopodobieństwa dotyczącej zdolności danej osoby do wywiązania się ze zobowiązań płatniczych w przyszłości („scoring”) – Wykorzystanie tej wartości prawdopodobieństwa przez osoby trzecie), <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62021CA0634>

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

<sup>28</sup> Jak stwierdzono w wytycznych EROD (wyżej wymienionych): „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”.

<sup>29</sup> Z 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”.

fazie projektowania każdej czynności przetwarzania danych osobowych ma również zastosowanie do podmiotów przetwarzających i przez cały cykl przetwarzania.

32. Biorąc pod uwagę różnorodność i powagę zagrożeń związanych z systemami zapewnienia wieku, zwłaszcza w przypadku przetwarzania dokumentów tożsamości lub szczególnych kategorii danych osobowych, takich 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 dla takich systemów powinny być również regularnie weryfikowane i aktualizowane, w razie potrzeby, aby uwzględnić szybko zmieniający się krajobraz technologii zwiększających prywatność w dziedzinie zarządzania tożsamością cyfrową.
33. Jak wspomniano w wytycznych EROD dotyczących uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych,<sup>30</sup> odniesienie do „stanu wiedzy technicznej” w kontekście art. 25 RODO nakłada na administratorów danych obowiązek uwzględnienia obecnego postępu technologii dostępnej na rynku przy określaniu wyżej wymienionych odpowiednich środków technicznych i organizacyjnych. Przy określaniu takich środków pomocne mogą być normy, najlepsze praktyki i kodeksy postępowania uznane przez odpowiednie zainteresowane strony. Należy jednak zweryfikować stosowność tych środków w odniesieniu do każdej konkretnej czynności przetwarzania.
34. W związku z tym EROD zaleca, aby w oparciu o stan wiedzy technicznej na temat zapewnienia wieku w czasie przygotowywania niniejszego dokumentu należy uwzględnić technologie i architektury sprzyjające danym przechowywanym przez użytkownika i bezpiecznemu przetwarzaniu lokalnemu (opartemu na urządzeniu), umożliwiające takie właściwości, jak brak powiązania<sup>31</sup> (z punktu widzenia różnych stron, a nawet w przypadku złów lub naruszeń ochrony danych) oraz selektywne ujawnianie danych<sup>32</sup> osobowych pod kontrolą osoby, której dane dotyczą. Ponadto osobom, których dane dotyczą,<sup>33</sup> należy udostępnić podejścia, takie jak podejścia oparte na seryjnym wydawaniu<sup>34</sup> danych uwierzytelniających jednorazowego użytku lub protokoły kryptograficzne, takie jak dowody z wiedzą zerową, w przypadkach gdy zapewnienie wieku może wiązać się z wysokim ryzykiem dla ich prywatności.

## 2.9 Bezpieczeństwo przy zapewnieniu wieku

Dostawcy usług i wszelkie osoby trzecie zaangażowane w zapewnianie wieku powinny wdrożyć odpowiednie środki techniczne i organizacyjne w celu zapewnienia poziomu bezpieczeństwa odpowiedniego do ryzyka.

35. RODO wymaga, aby zarówno administratorzy, jak i podmioty przetwarzające dysponowali odpowiednimi środkami technicznymi i organizacyjnymi w celu zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku związanemu z przetwarzaniem danych osobowych (motyw 83 i art. 32). Charakter, wrażliwość i ilość danych osobowych, które mogą być zaangażowane w zapewnienie wieku, podkreślają potencjalne negatywne skutki, jakie może pociągać za sobą naruszenie ochrony danych.

---

<sup>30</sup> Wytyczne nr 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](https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf)

<sup>31</sup> Właściwość w postaci braku powiązania oznacza, że niemożliwe jest powiązanie lub skorelowanie różnych elementów danych, działań lub transakcji z konkretną osobą, której dane dotyczą.

<sup>32</sup> Selektywne ujawnianie jest cechą tokenów, danych uwierzytelniających i poświadczeń, która umożliwia osobom, których dane dotyczą, udostępnianie tylko informacji, których chcą, konkretnym stronom w poszczególnych przypadkach.

<sup>33</sup> Wydawanie seryjne polega na udzieleniu odpowiedzi na jedno żądanie danych uwierzytelniających od osoby, której dane dotyczą, za pomocą zestawu lub grupy danych uwierzytelniających wygenerowanych w tym samym czasie.

<sup>34</sup> Dowód z wiedzą zerową to protokół, w którym jedna strona (udowadniający) może wykazać drugiej stronie (weryfikatorowi), że dane oświadczenie jest prawdziwe, bez przekazywania weryfikatorowi jakichkolwiek informacji poza samym faktem prawdy tego oświadczenia.

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 relacji. Ponadto pseudonimizacja i szyfrowanie danych osobowych mogą być pomocne w łagodzeniu ewentualnych negatywnych skutków naruszeń ochrony danych. Spełnienie zasady ograniczenia przechowywania i stosowanie krótkich okresów zatrzymywania może być również niezbędne dla zagwarantowania bezpieczeństwa przy zapewnieniu wieku, co obniża poziom narażenia. Politykę braku logów można uznać za cenne zabezpieczenie: po zweryfikowaniu wieku użytkownika nie prowadzi się rejestru danych osobowych wykorzystywanych w procesie zapewnienia wieku.
37. W praktyce, biorąc pod uwagę rosnącą presję prawną na wdrożenie zapewnienia wieku i liczbę dostawców, którzy mogą podlegać takim przepisom, należy spodziewać się wystąpienia naruszeń bezpieczeństwa. Należy sprawdzić, czy wprowadzono wszelkie odpowiednie techniczne środki ochrony i odpowiednie 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 zastosowanie<sup>35</sup>. Kluczowym elementem każdej polityki bezpieczeństwa danych jest zdolność, w miarę możliwości, zapobiegania naruszeniom oraz, w przypadku ich wystąpienia, reagowania w odpowiednim czasie. W związku z tym zdolność do szybkiego przywrócenia dostępności zapewnienia wieku po naruszeniu bezpieczeństwa należy również uznać za niezbędną. Podobnie kluczowe znaczenie ma zapewnienie odporności ekosystemu zapewnienia wieku poprzez sprzyjanie istnieniu różnych alternatyw i luźno powiązanych stron,<sup>36</sup> które nie są od siebie tak bardzo zależne, że błąd lub awaria jednego z nich spowodowałaby znaczne ograniczenia dostępu.
38. Chociaż środki bezpieczeństwa mają ogromne znaczenie dla zapewnienia wieku, nie gwarantują one, że upoważniony lub nieuprawniony dostęp do danych osobowych nie będzie miał wpływu 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

Dostawcy usług i wszelkie zaangażowane strony trzecie powinni wdrożyć metody zarządzania, które pozwolą im ponosić odpowiedzialność za swoje podejście do zapewniania wieku oraz za wykazanie zgodności z ogólnym rozporządzeniem o ochronie danych i innymi wymogami prawnymi.

39. Biorąc pod uwagę zaangażowanie różnych zainteresowanych stron, zarządzanie zapewnieniem wieku odgrywa kluczową rolę w jego rozliczalności. Zapewnienie wieku powinno funkcjonować w ramach zarządzania, zapewniając, aby wszystkie procesy i systemy były projektowane, wdrażane, zmieniane, dokumentowane, oceniane, wykorzystywane, utrzymywane, testowane lub poddawane audytowi w sposób zgodny z przepisami o ochronie danych i innymi wymogami prawnymi. Ramy te powinny obejmować co najmniej politykę 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 w całym cyklu życia zapewnienia wieku.
40. Na przykład ramy zarządzania powinny określać, kto jest odpowiedzialny i w jaki sposób, z perspektywy administratora/podmiotu przetwarzającego, dokładnie za jakie działania lub operacje w ramach przetwarzania. Powinny one również zapewnić, aby organy i odpowiednie zainteresowane strony

<sup>35</sup> Z 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](https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf)

<sup>36</sup> Strony są od siebie zależne w jak najmniejszym stopniu, ograniczając zakres wpływu w przypadku wystąpienia zmian lub awarii.

mogły skutecznie kontrolować zapewnienie wieku. Ramy zarządzania mają zasadnicze znaczenie dla rozliczalności, ale także dla przejrzystości i zaufania do zapewnienia wieku. Osoby, których dane dotyczą, częściej ufają metodom, które są przejrzyste w odniesieniu do ich sposobu działania, podejmowania decyzji itp.

41. Ponadto część ram zarządzania obejmuje zapewnienie skuteczności (sekcja 2.5), uwzględnianie ochrony danych w fazie projektowania oraz domyślną ochronę danych (sekcja 2.8), a także bezpieczeństwo (sekcja 2.9) zapewnienia wieku.

W imieniu Europejskiej Rady Ochrony Danych  
Przewodnicząca

(Anu Talus)