20 listopada 2020 r. T-PD (2019) 06BISrev5

KOMITET KONSULTACYJNY KONWENCJI O OCHRONIE
OSÓB W ZWIĄZKU Z AUTOMATYCZNYM PRZETWARZANIEM
DANYCH OSOBOWYCH

KONWENCJA 108

Ochrona danych dzieci w środowisku edukacyjnym

Wytyczne

Dyrekcja Generalna Praw Człowieka i Rządów Prawa

Spis treści

1. Wprowadzenie

Środowisko cyfrowe kształtuje życie dzieci na wiele sposobów, stwarzając możliwości i zagrożenia dla ich dobrobytu i korzystania z praw człowieka. Niektóre narzędzia cyfrowe umożliwiają dostarczanie niezbędnych informacji, łącząc społeczności szkolne poza salą lekcyjną. Inne zapewniają sposoby dzielenia się treściami edukacyjnymi lub oferowania istotnych alternatywnych środków i trybów edukacji poprzez technologie wspomagające i rozszerzoną komunikację.

Niniejsze wytyczne[1] powinny wspierać organizacje i osoby fizyczne w kontekście edukacji, by szanować, chronić i wypełniać prawa dziecka do ochrony danych w środowisku cyfrowym w ramach zakresu art. 3 zmodernizowanej Konwencji 108 (częściej określanej jako „Konwencja 108+")[2], oraz zgodnie z instrumentami Rady Europy, w tym Wytycznymi dotyczącymi dzieci w środowisku cyfrowym, Zalecenie CM/Rec (2018)7.[3]

Komitet Praw Dziecka ONZ ustanowił w 2001 r., że

> *„Dzieci nie tracą praw człowieka, przechodząc przez bramy szkoły. Edukacja musi być prowadzona z poszanowaniem przyrodzonej godności dziecka i umożliwia dziecku swobodne wyrażanie swoich poglądów ... "*

Wprowadzenie narzędzi cyfrowych do sal lekcyjnych w efekcie otwiera bramy szkoły na szeroki zakres i dużą liczba interesariuszy, którzy wchodzą w interakcję z codziennymi czynnościami dzieci. Większość urządzeń i aplikacji, oprogramowania i platform edukacyjnych stosowanych w środowisku edukacyjnym, opracowują prywatne podmioty komercyjne.

Zainteresowane strony powinny współpracować w celu stworzenia środowiska szanującego prawa, zgodnie z art. 8 Europejskiej Konwencji Praw Człowieka oraz chroniącego godność człowieka i podstawowe wolności każdej osoby, w zakresie ochrony danych osobowych.

Wiele komercyjnych programów edukacyjnych jest znanych jako „darmowe"; oprogramowanie oferowane do celów środowiska edukacyjnego bez bezpośrednich kosztów finansowych. Zgodnie z dyrektywą UE w sprawie handlu elektronicznego (art. 1 ust. 1) zasadniczo mieści się to w definicji usługi społeczeństwa informacyjnego[4] „świadczonego za wynagrodzeniem".

---

1 Wytyczne są zgodne z raportem *„Ochrona danych dzieci w systemach edukacji: wyzwania i możliwe środki zaradcze"* sporządzonym przez Jen Persson, dostępnym pod adresem: https://rm.coe.int/t-pd-2019-06reveng-report-children-data-protection-in-educational-sys/168098d309

2 Konwencja 108+: Konwencja o ochronie osób w związku z przetwarzaniem danych osobowych, zaktualizowana Protokołem zmieniającym CETS 223, dostępna pod adresem: https://rm.coe.int/convention-108-convention-for-theprotection-of-individuals-with-regar/16808b36f1

3 Wytyczne Rady Europy w sprawie dzieci w środowisku cyfrowym, Zalecenie CM/Rec (2018)7 Komitetu Ministrów dla państw członkowskich w sprawie Wytycznych dotyczących poszanowania, ochrony i wypełniania praw dziecka w środowisku cyfrowym: https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

4 Aby określić zakres pojęcia „usługa społeczeństwa informacyjnego" np. w RODO, odsyła się w art. 4 ust. 25 RODO do Dyrektywy 2015/1535. Patrz: Wytyczne EROD 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679 (pkt 128), wersja w języku polskim:

Rozwój technologii edukacyjnych może oznaczać, że podmioty niepaństwowe rutynowo kontrolują dokumentację edukacyjną dzieci nie tylko w szkołach niezależnych, ale także w szkołach „publicznych" lub „państwowych". Infrastruktura cyfrowa służąca do dostarczania edukacji państwowej jest często własnością komercyjną. Może to wprowadzić nowe pytania dotyczące tego, gdzie ma miejsce kontrola programu nauczania, jeśli rodzaj treści i sposób ich dostarczania jest kształtowany przez platformę technologiczną, a także pytania dotyczące kwestii bezpieczeństwa i zrównoważonego rozwoju.

W związku z tym, w kompetencjach firm może leżeć zablokowanie w szkołach praktyk związanych z oprogramowaniem prawnie zastrzeżonym, a szkoły muszą być świadome potencjalnych konsekwencji dla interoperacyjności, dostępu do danych i ich ponownego wykorzystania, a także budżetowych i środowiskowych skutków przestarzałości, na przykład kiedy firma decyduje się na zaprzestanie aktualizowania sprzętu lub oprogramowania. W chwili pisania tego tekstu powszechne jest, że małe firmy są inkubowane przez aniołów biznesu, a później są wykupywane przez inne większe firmy. Administrowanie danymi osobowymi i przechowywanie danych osobowych mogą być zatem wielokrotnie przenoszone w przypadku przejęć w trakcie edukacji dziecka.

Wzrost przepływów danych w chmurze i transgranicznych w systemach danych edukacyjnych oznacza, że praktyki dotyczące bezpieczeństwa wymagają szczególnej uwagi, zgodnie z art. 7 Konwencji 108+.

Dzieci nie widzą ani nie rozumieją, jak duży stał się ich cyfrowy ślad, ani jak daleko przemieszcza się do tysięcy stron trzecich w całym świecie edukacji lub poza nim, przez całe ich życie. Chociaż organizacja zajmująca się dziećmi jest niezbędna i dzieci muszą być lepiej poinformowane o tym, jak ich własne dane osobowe są gromadzone i przetwarzane, jednocześnie istnieje zgoda co do tego, że nie można oczekiwać, że dzieci rozumieją bardzo złożone środowisko internetowe i same podejmą się swoich obowiązków.

Ciężar konieczności sprawdzenia przed zakupem produktów lub usług w placówkach edukacyjnych może utrudnić nawet dorosłym pełne zrozumienie narzędzi programowych i ich przetwarzania; włącznie z oceną porównawczych skutków korzystania z otwartych lub zastrzeżonych technologii informacyjno-komunikacyjnych (ICT), usług płatnych lub bezpłatnych lub w celu przeprowadzenia odpowiedniej oceny ryzyka oraz uzyskania i zaoferowania odpowiednich informacji wymaganych do udostępnienia osobie, której dane dotyczą. Utrudnia to posiadanie wystarczających kwalifikacji, aby spełniać i bronić praw użytkowników.

Uznając, że przepisy dotyczące placówek edukacyjnych oraz inne prawo krajowe i międzynarodowe mają wpływ na sposób stosowania zasad ochrony danych, w tym na prawa osób, których dane dotyczą, instytucje edukacyjne potrzebują solidnych ram prawnych i kodeksów postępowania, aby wzmocnić uprawnienia pracowników oraz wyjaśnić firmom, co jest dozwolone, a co nie, podczas przetwarzania danych dzieci w kontekście działań edukacyjnych, tworząc równe szanse dla wszystkich.

Decydenci i praktycy, w tym ustawodawcy, organy nadzorcze zgodnie z art. 15 ust. 2 lit. e) Konwencji 108+, władze oświatowe i branża edukacyjna powinny przestrzegać i promować niniejsze Wytyczne oraz wdrażać środki w celu spełnienia zobowiązań w zakresie ochrony danych i prywatności.

W placówkach edukacyjnych dzieci są pozbawione uprawnień w relacjach z organami publicznymi, a także są uznawane za podatne na zagrożenia ze względu na ich brak zrozumienia i rozwijające się zdolności, oraz stan bycia w procesie rozwoju ku dorosłości. Ze statycznego punktu widzenia dziecko to osoba, która nie osiągnęła jeszcze dojrzałości fizycznej i psychicznej. Z dynamicznego punktu

---

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_pl.pdf

widzenia, dziecko rozwija się, by stać się dorosłym (Grupa Robocza Art. 29, 2009).[5] Dzieci są również aktywnymi posiadaczami praw i podmiotami, którzy wymagają nie tylko ochrony, ale także dostarczania informacji, szkoleń i wskazówek.

Należy również przygotować materiały, takie jak przewodniki informacyjne i dokumenty dotyczące rzetelnego przetwarzania dostępne dla dzieci i ich przedstawicieli, w sposób przyjazny dzieciom i przystępny.

Należy uwzględnić zakres danych osobowych, które mogą być przetwarzane, ich szerokie zastosowanie, w tym jako pomoc w nauce i do innych celów, do celów administracyjnych, zarządzania behawioralnego i celów dydaktycznych, ich wrażliwość i trwające całe życie zagrożenia dla prywatności, które mogą wynikać z przetwarzania zarówno zbiorów niecyfrowych, jak i cyfrowych, w środowisku edukacyjnym.

Wytyczne te powinny mieć również zastosowanie wszędzie tam, gdzie wykorzystywane są rozwiązania i usługi zdalnego nauczania w wyniku zapisania dziecka do placówki edukacyjnej i są używane poza placówką edukacyjną, np. do pracy domowej lub nauki na odległość. Narzędzia i zasoby nauczania na odległość powinny podlegać tej samej rygorystycznej należytej staranności w zakresie jakości pedagogicznej i bezpieczeństwa oraz standardów ochrony danych, na przykład w zakresie ustawień domyślnych, tak aby korzystanie z aplikacji i oprogramowania nie naruszało praw osób, których dane dotyczą (ochrona danych domyślnie). Przetwarzanie nie może obejmować więcej danych, niż jest to konieczne do osiągnięcia uzasadnionego celu. Jest to szczególnie ważne, gdy zgoda nie może być dobrowolna, ponieważ wybór polega na korzystaniu z produktu i otrzymywaniu instrukcji zdalnej lub odmowie i nieotrzymaniu jej.

Gdy szkoła wymaga korzystania z narzędzi e-learningowych, podstawa w formie zgody na przetwarzanie danych osobowych albo przez szkołę, albo przez zewnętrzny podmiot przetwarzający nie będzie ważna, ponieważ zgoda musi być jednoznacznie dobrowolna[6] i można jej odmówić bez uszczerbku.[7]

Należy pamiętać, że zasady ochrony danych nie są stosowane w oderwaniu od ustawodawstwa w zakresie edukacji lub prawa dotyczącego równości, zatrudnienia, prywatności komunikacji oraz innych stosownych przepisów i prawa krajowego.

---

5 Opinia Grupy Roboczej Art. 29 2/2009 w sprawie ochrony danych osobowych dzieci (wytyczne ogólne i szczególny przypadek szkół): https://ec.europa.eu/justice/article-29/documentation/opinion- recommendation/files/2009/wp160_en.pdf, wersja w języku polskim: https://archiwum.giodo.gov.pl/pl/1520022/2991

6 Zgodnie z art. 5 ust. 2 Konwencji 108+ i w tym kontekście należy również wziąć pod uwagę, że motyw 43 RODO stanowi, że „aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie we wszystkich przypadkach. Zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne, lub jeżeli od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna" oraz że dzieci w placówce edukacyjnej stanowią typowy przykład sytuacji, w której istnieje nierównowaga między osobą, której dane dotyczą, a administratorem i w której należy raczej zastosować inną podstawę prawną.

7 Jak określono w pkt 42 Raportu wyjaśniającego do Konwencji 108+, na osobę, której dane dotyczą, nie można wywierać żadnego nadmiernego wpływu lub nacisku (który może mieć charakter ekonomiczny lub inny), bezpośredniego lub pośredniego, a zgoda nie powinna być dobrowolna, gdy osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru lub nie może odmówić lub cofnąć zgody bez uszczerbku.

Wytyczne należy stosować łącznie z obowiązującymi zasadami ochrony danych wskazanych w sekcji czwartej, w tym z zasadą minimalizacji danych.

Dorośli powinni zadbać o to, aby ochrona oferowana dzieciom była odpowiednia nie tylko na czas ich dzieciństwa, ale także uwzględniała przyszłe interesy dzieci. Mamy obowiązek promować zdolność dzieci do osiągania dojrzałości bez przeszkód i do pełnego i swobodnego rozwoju, aby w pełni wykorzystać swój potencjał i wspierać ludzki rozwój.

2. Zakres i cel

2.1. Niniejsze wytyczne mają na celu pomóc w wyjaśnieniu zasad ochrony danych zawartych w Konwencji 108+ w celu sprostania wyzwaniom związanym z ochroną danych osobowych wynikających z nowych technologii i praktyk, przy jednoczesnym zachowaniu neutralnych technologicznie przepisów.

2.2. Wytyczne mają na celu zapewnienie pełnego zakresu praw dziecka w zakresie ochrony danych w wyniku interakcji ze środowiskiem edukacyjnym, w tym prawa do informacji, reprezentacji, uczestnictwa i prywatności. Powinny być one w pełni szanowane i należycie uwzględnione dla poziomu dojrzałości i zrozumienia dziecka.

2.3. Żadne z postanowień Wytycznych nie może być interpretowane jako wykluczające lub ograniczające postanowienia Europejskiej Konwencji Praw Człowieka i Konwencji 108.[8] Niniejsze wytyczne uwzględniają również nowe gwarancje Konwencji 108+.

2.4. Wytyczne pozostają na wysokim poziomie. Organy nadzorcze mogą chcieć odnieść się do praktycznych sugestii dotyczących placówek edukacyjnych, w tym list kontrolnych dla tych, którzy chcą zintegrować technologie cyfrowe ze swoimi procesami, w ramach krajowych kodeksów postępowania i praktycznych wskazówek dotyczących prawa Państw-Stron. Kodeksy postępowania można by również przedłożyć (do zatwierdzenia) organom nadzorczym (wśród właściwych organów). Państwa powinny opracować oparte na dowodach standardy i wytyczne dla szkół i innych organów odpowiedzialnych za nabywanie i wykorzystywanie technologii i materiałów edukacyjnych, aby zapewnić, że dostarczają one udowodnionych korzyści edukacyjnych i będą przestrzegać pełnego zakresu praw dziecka.

3. Definicje do celów Wytycznych

a. „dziecko" oznacza każdą osobę w wieku poniżej 18 lat, chyba że pełnoletność zostanie osiągnięta wcześniej zgodnie z prawem krajowym.

---

8 Europejska Konwencja Praw Człowieka (Konwencja o ochronie praw człowieka i podstawowych wolności, tekst w języku polskim dostępny: https://www.echr.coe.int/Documents/Convention_POL.pdf) oraz Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, ETS 108, dostępna pod adresem: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108, wersja w języku polskim: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802ecf76

b. „analiza danych” odnosi się do danych osobowych wykorzystywanych w technologiach obliczeniowych, które analizują duże ilości danych w celu odkrycia ukrytych wzorców, trendów i korelacji i odnosi się do całego cyklu życia zarządzania danymi polegającego na gromadzeniu, organizowaniu i analizowaniu danych w celu odkrywania wzorców, wnioskowania o sytuacjach lub stanach, przewidywania i rozumienia zachowań.

c. „środowisko cyfrowe” jest rozumiane jako obejmujące technologie informacyjne i komunikacyjne (ICT), w tym Internet, technologie i urządzenia mobilne i powiązane, a także sieci cyfrowe, bazy danych, aplikacje i usługi.

d. „bezpośrednia opieka i edukacja” oznacza działalność edukacyjną, administracyjną lub opiekę społeczną związaną z bezpośrednim prowadzeniem nauczania i jego administrowaniem, lub bezpośrednią opiekę nad zidentyfikowaną osobą, ogólnie wchodzącą w zakres ustawowych publicznych zadań edukacyjnych oraz przetwarzania danych, których dziecko i opiekunowie prawni mogliby racjonalnie oczekiwać w ramach bycia w szkole. Opieka bezpośrednia kontrastuje z wtórnym ponownym wykorzystaniem danych, które oznacza wszystkie inne pośrednie sposoby wykorzystania danych osobowych zebranych lub wywnioskowanych na temat osoby w kontekście jej czasu spędzonego „in loco parentis” w środowisku edukacyjnym; niewyczerpujące przykłady obejmują analizę uczenia się, przewidywanie ryzyka, badania interesu publicznego do przetwarzania w prasie lub mediach społecznościowych oraz do celów marketingowych.

e. „placówka edukacyjna” oznacza środowisko dostarczania edukacji dziecku, podlegające jurysdykcji Państw-Stron w sektorze prywatnym i publicznym, ale nie przez osobę fizyczną w ramach czynności o czysto domowym charakterze.

f. „e-learning” może w szerokim ujęciu obejmować uczenie się przy wsparciu technologii informacyjno-komunikacyjnych (ICT), zwłaszcza w celu dostarczania lub dostępu do treści, nauczania na odległość lub przez Internet (w tym narzędzia używane w trybie online i offline). E-learning może odbywać się bez żadnego połączenia na żywo z siecią lub połączenia internetowego, ale często będzie wymagał takiego dostępu w ramach usługi.

g. „opiekunowie prawni” odnoszą się do osób, które zgodnie z prawem krajowym są uznawane za sprawujących władzę rodzicielską nad dzieckiem i posiadających zbiór obowiązków, praw i uprawnień, których celem jest promowanie i ochrona praw i dobra dziecka zgodnie z rozwijającymi się zdolności dziecka.

h. „analitykę uczenia się” można opisać jako pomiar, gromadzenie, analizę i raportowanie danych o uczniach i ich kontekstach w celu zrozumienia i optymalizacji uczenia się oraz środowisk, w których się ono odbywa.[9]

i. „przetwarzanie” oznacza każdą operację lub zestaw operacji wykonywanych na danych osobowych, takie jak, ale nie tylko, gromadzenie, przechowywanie, zachowywanie, zmiana, odzyskiwanie, ujawnianie, udostępnianie, usuwanie lub niszczenie lub przeprowadzanie logicznych i / lub arytmetycznych operacji na takich danych.

j. „profil” odnosi się do zestawu cech przypisywanych osobie, charakteryzujących kategorię osób lub mających zastosowanie do danej osoby.

---

9 Learning and Academic Analytics, Siemens, G., 5 sierpnia 2011 r. https://www.researchgate.net/publication/254462827_Learning_analytics_and_educational_data_mining_Towards_communication_and_collaboration

k. „profilowanie” odnosi się do dowolnej formy zautomatyzowanego przetwarzania danych osobowych, w tym korzystania z systemów uczenia maszynowego, polegających na wykorzystaniu danych osobowych lub nieosobowych do oceny niektórych aspektów osobistych dotyczących osoby, w szczególności do analizy lub by przewidzieć aspekty dotyczące wyników pracy tej osoby, sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, niezawodności, zachowania, lokalizacji lub przemieszczania się.

l. „szczególna kategoria danych” ma takie samo znaczenie jak w art. 6 Konwencji 108+.

m. „organy nadzorcze” oznaczają organy wyznaczone jako odpowiedzialne za zapewnienie zgodności z postanowieniami rozdziału IV Konwencji 108+.

4. Zasady przetwarzania danych

Konwencja 108+ określa zasady, obowiązki i prawa, które mają zastosowanie do każdego przetwarzania danych osobowych, a zatem są niezbędne do zastosowania w placówkach edukacyjnych.

4.1. Legalność przetwarzania oraz zasady zgodności przetwarzania z prawem, rzetelności, konieczności, proporcjonalności, ograniczenia celu, prawidłowości, ograniczonego czasu zatrzymywania w możliwej do zidentyfikowania formie, przejrzystości i minimalizacji danych oraz zapewnienia, że dane osobowe są adekwatne, stosowne i nie nadmierne w stosunku do cele, w jakich są przetwarzane zgodnie z art. 5 Konwencji 108+.

4.2. Ostrożne podejście i wzmocniona ochrona wrażliwych, szczególnych kategorii danych, w tym danych genetycznych i biometrycznych, danych dotyczących pochodzenia etnicznego, orientacji seksualnej lub przestępstw, uznając dodatkową bezbronność dzieci (art. 6 Konwencji 108+).

4.3. Znacząca przejrzystość przetwarzania danych, z uznaniem znaczenia dostępności poprzez użycie jasnego języka, w odpowiednich dla dzieci warunkach i formatach, gdy to właściwe, w komunikacji, w trybie offline lub online oraz na dowolnym urządzeniu, zgodnie z art. 8 Konwencji 108+.

4.4. Rozliczalność administratorów danych i podmiotów przetwarzających dane musi być jasno określona we wszelkich ustaleniach umownych, określonych ze względu na charakter przetwarzania, zgodnie z art. 10 ust. 1 Konwencji 108+.

4.5. W praktyce należy stosować zasady ochrony prywatności i danych już w fazie projektowania oraz odpowiednie środki organizacyjne i techniczne (art. 10 ust. 2 Konwencji 108+).

4.6. Ocena prawdopodobnego wpływu zamierzonego przetwarzania na prawa i wolności osoby, której dane dotyczą, przed rozpoczęciem na początku każdego przetwarzania danych i w całym jego cyklu życia. Szczególną uwagę należy zwrócić na wczesnym etapie, w jaki sposób będzie prowadzona komunikacja dotycząca przetwarzania danych między administratorem danych a dzieckiem lub jego opiekunem prawnym po opuszczeniu placówki edukacyjnej.

4.7. Środki bezpieczeństwa[10] są niezbędne, aby zapobiegać zagrożeniom, takim jak przypadkowy lub nieuprawniony dostęp, zniszczenie, utrata, niewłaściwe użycie, modyfikacja, ataki dla okupu lub ujawnienie danych osobowych.

4.8. W kontekście edukacyjnym administratorzy danych muszą uznać prawa opiekunów prawnych do działania w imieniu i w najlepszym interesie dziecka, zgodnie z prawem krajowym i międzynarodowym oraz zgodnie z art. 9 Konwencji 108+. Należy dołożyć wszelkich starań, aby zaangażować dziecko w podejmowanie decyzji na jego temat i, w stosownych przypadkach, przekazać rodzinie odpowiednie informacje.

5. Podstawowe zasady praw dziecka w placówce edukacyjnej

Wytyczne opierają się na istniejących zasadach zapisanych w Konwencji 108+, Strategii Rady Europy na rzecz Praw Dziecka (2016–2021)[11] oraz orzecznictwie Europejskiego Trybunału Praw Człowieka. Każde dziecko ma prawo do korzystania z pełnego zakresu praw człowieka chronionych przez Europejską Konwencję Praw Człowieka, Konwencję Narodów Zjednoczonych o Prawach Dziecka (UNCRC) i inne międzynarodowe instrumenty praw człowieka. Niniejsze Wytyczne zachęcają Państwa-Strony Konwencji 108 do uznania tych praw w kontekście ochrony danych dzieci w edukacji. W celu zagwarantowania najlepszego interesu dziecka we wszystkich działaniach, które ich dotyczą, państwa strony mogą rozważyć wprowadzenie i poprawę jakości i efektów ocen wpływu na dzieci zgodnie ze Strategią Rady Europy na rzecz Praw Dziecka (2016–2021).

5.1. Najlepszy interes dziecka

5.1.1. We wszystkich działaniach dotyczących dziecka w środowisku cyfrowym najważniejszy jest interes dziecka.

5.1.2. Oceniając najlepszy interes dziecka, Państwa-Strony powinny dołożyć wszelkich starań, aby zrównoważyć i pogodzić prawo dziecka do ochrony z innymi prawami, w szczególności z prawem do wolności wypowiedzi i informacji oraz do uczestnictwa, a także z prawem do bycia wysłuchanym.

5.1.3. Konieczne może być zwrócenie szczególnej uwagi na definicję najlepiej pojętego interesu dzieci bardziej wrażliwych w edukacji, takich jak dzieci bez rodziców, dzieci migrantów, dzieci uchodźców i ubiegające się o azyl, dzieci bez opieki, dzieci niepełnosprawne, dzieci bezdomne, dzieci romskie i dzieci przebywające w placówkach opiekuńczych, placówkach medycznych lub dla młodocianych przestępców.

10 Sugerowane odniesienie do bezpieczeństwa danych osobowych podczas zdalnego nauczania - przewodnik UODO dla szkół https://uodo.gov.pl/en/553/1118
11 Strategia Rady Europy na rzecz Praw Dziecka (2016-2021) https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168066cff8, wersja w języku polskim: https://rm.coe.int/strategia-rady-europy-na-rzecz-praw-dziecka-2016-2021-/1680931c80

5.2. Ewoluujące zdolności dziecka

5.2.1. Możliwości dziecka ewoluują od urodzenia do 18 roku życia. Poszczególne dzieci osiągają różny poziom dojrzałości w różnym wieku.

5.2.2. Jak określono w Wytycznych dotyczących poszanowania, ochrony i wypełniania praw dziecka w środowisku cyfrowym[12], wszystkie zainteresowane strony powinny uznać ewoluujące zdolności dzieci, w tym dzieci niepełnosprawnych lub znajdujących się w szczególnie trudnej sytuacji, oraz zapewnić, aby były przyjęte polityki i praktyki w odpowiedzi na ich potrzeby w zakresie środowiska cyfrowego.

5.3. Prawo do bycia wysłuchanym

5.3.1. Dzieci mają prawo do swobodnego wypowiadania się we wszystkich sprawach, które ich dotyczą, a ich poglądom należy nadawać odpowiednią wagę, stosownie do ich wieku i dojrzałości. Państwa powinny zadbać o to, aby dzieci były świadome swoich praw w środowisku cyfrowym w sposób przyjazny dla dzieci, przejrzysty, zrozumiały i przystępny. Każdy w systemie edukacji powinien zapewnić dzieciom dostęp do mechanizmów egzekwowania swoich praw.

5.3.2. Pracownicy placówek oświatowych powinni przyjąć domyślne stanowisko dotyczące dobrych praktyk, aby zaangażować opiekunów prawnych i dzieci, zgodnie z ich możliwościami, w konsultacje dotyczące decyzji o przyjęciu nowej technologii, która skutkuje przetwarzaniem danych osobowych dzieci, w celu zapewnienia właściwej równowagi wszystkich przedmiotowych interesów, dostosowane do art. 5 ust. 1 Konwencji 108+. Państwa powinny również zapewnić, aby procesy konsultacyjne obejmowały dzieci, które nie mają dostępu do technologii[13] w domu.

5.3.3. Zgodnie z art. 5 ust. 4 lit. a) Konwencji 108+ opiekunowie prawni i dzieci powinni być rzetelnie poinformowani o przetwarzaniu danych, chyba że udostępnienie takich informacji stwarza zagrożenie dla dobra dziecka, z uwagi na art. 11 lit. b) Konwencji lub jeżeli właściwe dziecko nie wniesie sprzeciwu wobec zaangażowania jednego lub więcej opiekunów prawnych.

5.3.4. Zgodnie z prawem Państw-Stron, w tym z uwzględnieniem wszelkich ograniczeń wiekowych określonych w prawie dla wyrażenia zgody na przetwarzanie danych przez usługi społeczeństwa informacyjnego (ISS), w przypadku gdy definicja ISS jest stosowany w placówkach edukacyjnych, oraz w celu wspierania dziecka jako osoby, której dane dotyczą, opiekunowie prawni powinni mieć możliwość wykonywania praw wynikających z art. 9 ust. 1 lit. b) Konwencji 108+ w imieniu dziecka uczącego się, jeżeli dziecko nie wyraża sprzeciwu, biorąc pod uwagę jego poziom zdolności i dobro dziecka.

---

12 Wytyczne Rady Europy w sprawie dzieci w środowisku cyfrowym, Zalecenie CM/Rec (2018)7 Komitetu Ministrów dla państw członkowskich w sprawie Wytycznych dotyczących poszanowania, ochrony i wypełniania praw dziecka w środowisku cyfrowym
https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

13 Komitet Praw Dziecka Organizacji Narodów Zjednoczonych, Projekt Komentarza ogólnego dotyczącego praw dziecka w odniesieniu do środowiska cyfrowego, sierpień 2020 r.
https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC/C/GC/25&Lang=en

5.3.5. Przetwarzanie danych na podstawie zgody może być nieważne w przypadku braku równowagi sił, w szczególności między organem publicznym a osobą fizyczną, co narusza dobrowolny charakter zgody. Ten brak równowagi jest jeszcze bardziej znaczący, gdy osobą, której dane dotyczą, jest dziecko. W związku z tym istnieje większe prawdopodobieństwo, że inna podstawa będzie miała zastosowanie w przypadku rutynowych czynności przetwarzania i takie przetwarzanie powinno być oparte na przepisach prawa.

5.3.6. Poprzez dostarczanie przyjaznych dzieciom, przejrzystych, zrozumiałych i dostępnych informacji na temat przetwarzania danych, dzieci powinny mieć możliwość wyrażenia zgody i jej wycofania, jeżeli mają zdolność zrozumienia konsekwencji, a przetwarzanie leży w ich własnym najlepszym interesie i jest zgodne z wszelkimi przepisami prawnymi dotyczącymi wieku w ustawodawstwie krajowym i międzynarodowym.

5.3.7. Dzieci powinny mieć prawo dostępu do odpowiednich, zrozumiałych, niezależnych i skutecznych mechanizmów składania skarg oraz korzystania z przysługujących im praw.

5.4. Prawo do niedyskryminacji

5.4.1. Prawa dziecka dotyczą wszystkich dzieci bez dyskryminacji z jakiegokolwiek względu. Podczas gdy należy podejmować wysiłki w celu poszanowania, ochrony i przestrzegania praw każdego dziecka w placówce edukacyjnej, mogą być potrzebne ukierunkowane środki w celu zaspokojenia określonych potrzeb, uznając, że środowisko cyfrowe może zarówno zwiększyć wrażliwość dzieci, jak i wzmocnić ich pozycję, chronić je i wspierać.

6. Zalecenia dla prawodawców i decydentów

Wykorzystanie technologii cyfrowych do celów edukacyjnych prowadzi do przetwarzania danych osobowych dzieci przez różne podmioty (od rządów krajowych, publicznych i prywatnych placówek edukacyjnych po podmioty prywatne, takie jak dostawcy produktów lub usług oraz twórcy oprogramowania, a także osoby takie jak nauczyciele, opiekunowie prawni i rówieśnicy). Przetwarzane dane są dostarczane nie tylko przez dzieci, rodziców lub wychowawców, ale są to także dane, które powstają w wyniku zaangażowania użytkownika lub dane wywnioskowane (np. na podstawie profilowania). Instytucje edukacyjne coraz częściej gromadzą dane szczególnie chronione, takie jak dane biometryczne. Takie gromadzenie danych może mieć konsekwencje dla dzieci na całe życie. Jako że zdarzają się sytuacje, w których różne organy są prawnie zobowiązane do współpracy, przed zebraniem wszystkich danych osobowych należy przeprowadzić ścisły test konieczności i proporcjonalności, aby zapewnić minimalizację danych oraz że każde wykorzystanie spełni uzasadnione oczekiwania dziecka i będzie zgodne z zasadami ograniczenia celu oraz z ograniczeniami dotyczącymi przechowywania i zatrzymywania. Należy koniecznie przyznać, że edukacja i technologie cyfrowe mają wpływ nie tylko na prawo dziecka do ochrony danych, a także że prawo do prywatności i ochrony danych umożliwia ochronę dalszych praw dziecka. Prawo do niedyskryminacji, prawo do rozwoju, prawo do wolności wypowiedzi, prawo do zabawy i prawo do ochrony przed wyzyskiem gospodarczym również mogą być zagrożone. Ustawodawcy i decydenci powinni zapewnić pełen zakres praw za pomocą innych instrumentów, protokołów i wytycznych przy rozważaniu implikacji przetwarzania danych dzieci w kontekście edukacji.

6.1. Przejrzyj ustawodawstwo, politykę i praktykę

6.1.1. Zapewnij zgodność z tymi zasadami i wytycznymi oraz promuj ich wdrażanie we wszystkich procesach przetwarzania danych w środowisku edukacyjnym, w środowisku edukacyjnym i po jego opuszczeniu w trakcie cyklu życia danych.

6.1.2. Określ wysokie oczekiwania co do konfiguracji prywatności w fazie projektowania w normach dotyczących wymagań technicznych zamawianych usług.

6.1.3. Utrzymuj lub ustanów ramy, w tym, w stosownych przypadkach, niezależne mechanizmy, w celu promowania i monitorowania wdrażania niniejszych wytycznych, zgodnie z ich systemami edukacyjnymi, nadzorczymi i administracyjnymi.

6.2. Zapewnij skuteczne wsparcie praw dzieci do bycia wysłuchanymi

6.2.1. Zapewnij organom nadzorczym wystarczające zasoby, aby zapewnić, że przepisy dotyczące ochrony danych są odpowiednio stosowane w środowisku edukacyjnym, a powiązane technologie są konsekwentnie stosowane.

6.2.2. Reprezentacja dzieci, których dane dotyczą, przed organami nadzorczymi (art. 18) przez osoby trzecie powinna być dostępna i wzmocniona. Państwa-Strony mogą przewidzieć w swoim ustawodawstwie na mocy art. 13 rozszerzoną ochronę. Należy umożliwić każdemu organowi, organizacji lub zrzeszeniu niezależnie od mandatu osoby, której dane dotyczą, prawo wniesienia skargi do właściwego organu nadzorczego w tym Państwie-Stronie, o ile zezwala na to prawo, jeżeli uzna, że prawa osoby, której dane dotyczą, zostały naruszone w wyniku przetwarzania.

6.2.3. Ustanów procedury umożliwiające dzieciom wyrażanie siebie i wyrażanie swoich opinii w zakresie korzystania z prawa do prywatności w placówkach edukacyjnych oraz zapewnij uwzględnienie ich poglądów.

6.2.4. Ułatw dziecku dostęp do środków odwoławczych w przypadku naruszeń postanowień Konwencji na mocy art. 12 oraz w duchu Wytycznych Rady Europy w sprawie wymiaru sprawiedliwości przyjaznego dzieciom[14], usuń wszelkie przeszkody w dostępie do sądu dla dzieci, podając podstawy do niezbędnej współpracy i wzajemnej pomocy między organami nadzorczymi (art. 15, 16 i 17 ust. 3) w sprawach dotyczących ochrony danych w placówkach edukacyjnych.

6.2.5. Uznając, że szczególną uwagę należy zwracać na prawa do ochrony danych dzieci i innych osób w trudnej sytuacji, placówki edukacyjne zapewniają przeszkolenie personelu w celu zapewnienia odpowiedniej zdolności zrozumienia ich roli w należytej staranności oraz uwzględnienia prawa dziecka do bycia wysłuchanym.

14 Wytyczne w sprawie wymiaru sprawiedliwości przyjaznego dzieciom przyjęte przez Komitet Ministrów Rady Europy w dniu 17 listopada 2010 r. Zobacz także rezolucję Zgromadzenia Parlamentarnego 2010(2014) „Przyjazny dziecku wymiar sprawiedliwości dla nieletnich: od retoryki do rzeczywistości" oraz wytyczne dotyczące promowania i wspierania wdrożenia Wytycznych w sprawie wymiaru sprawiedliwości przyjaznego dzieciom przez Europejski Komitet Współpracy Prawnej (CDCJ(2014)15)

6.3. Rozpoznaj i zintegruj prawa dziecka

6.3.1. Szanuj i wypełniaj obowiązki i zobowiązania w ramach istniejących norm Rady Europy i Organizacji Narodów Zjednoczonych dotyczących praw dziecka.[15] Niniejsze Wytyczne mają zastosowanie do wszystkich dzieci, mając na celu realizację tego prawa do edukacji bez dyskryminacji i na zasadzie równości szans.

6.3.2. Szanuj, chroń i realizuj prawa dziecka w środowisku cyfrowym, w środowisku edukacyjnym, zgodnie z Wytycznymi w sprawie dzieci w środowisku cyfrowym.[16]

6.3.3. Przestrzegaj Ogólnego komentarza ONZ nr 16 (2013) w sprawie zobowiązań państwa dotyczących wpływu sektora biznesowego na prawa dzieci.[17] Państwa muszą podjąć kroki w celu zapewnienia, że zamówienia publiczne są udzielane oferentom, którzy są zobowiązani do poszanowania praw dzieci, a państwa nie powinny inwestować finansów publicznych i innych zasobów w działalność biznesową, która narusza prawa dzieci. Państwa powinny podjąć odpowiednie środki w celu zapobiegania, monitorowania i badania naruszeń przez firmy w środowisku edukacyjnym i środowisku cyfrowym.

6.3.4. Uznaj zobowiązania zawarte w art. 24 Konwencji o prawach osób niepełnosprawnych do edukacji oraz w odniesieniu do włączenia i udziału w podejmowaniu decyzji o przyjęciu technologii, zapewnij powszechną dostępność już w fazie projektowania i promuj sprawiedliwe świadczenie.

7. Zalecenia dla administratorów danych

W łańcuchu przetwarzania danych jest wiele podmiotów, które mogą być administratorami danych; nie tylko instytucje edukacyjne i organy rządowe, ale także dostawcy platform, urządzeń, programów i aplikacji. Te ostatnie podmioty komercyjne mogą również być samodzielnymi administratorami danych, jeżeli samodzielnie lub wspólnie z innymi określają charakter przetwarzania w rozumieniu art. 2 Konwencji 108+ i należy zwrócić szczególną uwagę, aby zrozumieć, że charakter przetwarzania określa każdą rolę, a nie tylko to, co jest określone w warunkach umowy. W rezultacie obowiązki administratora danych nie zawsze mogą leżeć wyłącznie w zakresie edukacji. Aby spełnić wszystkie istotne zasady ochrony danych, w tym zasady prawidłowości, konieczności i bezpieczeństwa danych,

---

15 Art. 29 ust. 1 Konwencji ONZ o prawach dziecka: „Państwa-Strony są zgodne, że nauka dziecka będzie ukierunkowana na: (a) rozwijanie w jak najpełniejszym zakresie osobowości, talentów oraz zdolności umysłowych i fizycznych dziecka; b) rozwijanie w dziecku szacunku dla praw człowieka i podstawowych swobód oraz dla zasad zawartych w Karcie Narodów Zjednoczonych. https://www.ohchr.org/en/professionalinterest/pages/crc.aspx i Zasady 7 Deklaracji Praw Dziecka (1959) (proklamowanej przez Zgromadzenie Ogólne ONZ w rezolucji 1386 (XIV), A / RES / 14/1386, 20 listopada 1959)

16 Wytyczne Rady Europy w sprawie dzieci w środowisku cyfrowym, Zalecenie CM/Rec (2018)7 Komitetu Ministrów dla państw członkowskich w sprawie Wytycznych dotyczących poszanowania, ochrony i wypełniania praw dziecka w środowisku cyfrowym https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

17 Komitet Praw Dziecka Komentarz ogólny nr 16 (2013) dotycząca zobowiązań państwa dotyczących wpływu sektora biznesowego na prawa dzieci
https://www.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf
Dla niektórych dzieci wykorzystanie technologii adaptacyjnych może być niepożądaną oznaką ich niepełnosprawności.

placówki edukacyjne muszą zachęcać do wszechstronnej i zgodnej kultury zarządzania danymi, w której ocena ryzyka aktywnie uwzględnia prawa i wolności w ramach każdego przetwarzania lub udzielania zamówień, a jakość danych jest aktywnie monitorowana i efektywnie zarządzana poprzez zarządzanie dokumentacją, ze wsparciem przez szkolenie umiejętności i polityki.

7.1. Legalność i podstawa prawna

7.1.1. Zgodnie z art. 10 ust. 1 Konwencji 108+, na administratorze spoczywa obowiązek zapewnienia odpowiedniej ochrony danych i możliwości wykazania, że przetwarzanie danych jest zgodne z obowiązującymi przepisami.

7.1.2. Wszystkie strony zaangażowane w przetwarzanie danych w placówkach edukacyjnych powinny wyjaśnić obowiązki i rozliczalność między rolami w celu ustanowienia uprawnień i ich obowiązkami w zakresie przetwarzania danych oraz w przypadku zawierania umów z dostawcami i podmiotami przetwarzającymi dane będącymi stronami trzecimi.

7.1.3. Dane dziecka szczególnej kategorii, zgodnie z definicją w art. 6, wymagają wzmocnionej ochrony podczas przetwarzania, począwszy od odpowiedniej podstawy prawnej przetwarzania. W przypadku braku innej zgodnej z prawem podstawy przetwarzania, na przetwarzanie danych dotyczących zdrowia i innych szczególnych kategorii danych należy uzyskać świadomą i dobrowolnie wyrażoną zgodę od opiekuna prawnego i zarejestrować ją jako odpowiednie zabezpieczenie na mocy art. 6 ust. 1 dla dziecka, gdy przetwarzanie leży w najlepszym interesie dziecka. Takie dane specjalnej kategorii mogą być udostępniane do celów wykraczających poza ich bezpośrednią opiekę i edukację, wyłącznie za dobrowolną, konkretną, świadomą i wyraźną zgodą osoby, której dane dotyczą, lub jej prawnego opiekuna.

7.1.4. Zgoda na jakiekolwiek przetwarzanie danych, w tym między innymi szczególnej kategorii danych dziecka, nie może być nigdy domniemywana w imieniu opiekunów prawnych lub dzieci w celu uzasadnienia przetwarzania danych przez dostawców zewnętrznych.

7.1.5. Administratorzy danych powinni uznać, że dzieci i opiekunowie prawni nie mogą wyrazić ważnej zgody na korzystanie z podmiotów przetwarzających będących stronami trzecimi, jeżeli nie można jej dobrowolnie odmówić bez uszczerbku.

7.1.6. Uprawnienia opiekuna prawnego do wykonywania praw w imieniu dziecka jako osoby, której dane dotyczą, wygasają, gdy właściwe dziecko osiągnie pełnoletność zgodnie z prawem. Osoba, której dane dotyczą (dziecko) powinna być informowana o wszelkim trwającym przetwarzaniu danych na jej temat, na które wyraził zgodę opiekun prawny, aby móc wykonywać prawa osoby, której dane dotyczą, jako osoba pełnoletnia.

7.1.7. Nie należy oczekiwać, że dzieci będą zawierać umowy ze stronami trzecimi, na przykład z dostawcą e-learningu lub aplikacją wymaganą przez placówkę edukacyjną. Placówka edukacyjna powinna przetwarzać dane dzieci na podstawie pisemnej umowy między placówką a stroną trzecią. Przetwarzanie danych osobowych przez takie usługi powinno odbywać się na prawnie uzasadnionej podstawie określonej prawem.

7.1.8. Umowy między stronami trzecimi a dostawcami usług edukacyjnych powinny zapobiegać jakimkolwiek zmianom warunków, które mają wpływ na podstawowe prawa i wolności osoby, której dane dotyczą. Wszelkie zmiany w umowach między stronami trzecimi a dostawcami usług

edukacyjnych domyślnie wymagałyby zmiany umowy i powiadomienia osoby, której dane dotyczą (lub, w stosownych przypadkach, jej opiekunów prawnych) z wyjaśnieniem proponowanych zmian w jasny i prosty sposób.

7.1.9. Aby wypełnić zobowiązania wynikające z prawa dziecka do nauki, placówki powinny oferować odpowiedni poziom alternatywnego świadczenia edukacji bez uszczerbku dla dziecka, jeżeli rodziny lub dziecko skorzystają z prawa do sprzeciwu wobec przetwarzania danych w narzędziach cyfrowych, jako środka ochrony prawnej zgodnie z art. 9 ust. 1 lit. f) Konwencji 108+.

7.1.10. Zgodnie z art. 9 ust. 1 lit. d) reklamy nie należy uznawać za uzasadnioną podstawę lub zgodny cel w rozumieniu art. 5 ust. 4 lit. b), który jest nadrzędny wobec najlepszego interesu dziecka lub jego podstawowych praw i wolności.

7.1.11. Analizy danych i opracowywania produktów z wykorzystaniem danych osobowych nie należy uznawać za zgodne z prawem i zgodne wykorzystanie do dalszego przetwarzania, które jest nadrzędne wobec dobra dziecka lub jego praw i podstawowych wolności lub uzasadnionych oczekiwań osób, których dane dotyczą, zgodnie z pkt 49 Sprawozdania wyjaśniającego do Konwencji 108 +.

7.1.12. Administratorzy i podmioty przetwarzające nie udostępniają danych osobowych dzieci zebranych w trakcie ich edukacji, aby inni mogli na nich zarabiać lub przetwarzać je ponownie w celu sprzedaży zanonimizowanych lub pozbawionych identyfikacji danych, na przykład brokerom danych.

7.1.13. Dalsze przetwarzanie danych osobowych, o którym mowa w art. 5 ust. 4 lit. b), do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, jest zgodne, jeżeli cele są określone w pkt 50 sprawozdania wyjaśniającego z Konwencji 108+.

7.1.14. Zgodnie z prawem krajowym Państw-Stron, kodeksy postępowania powinny określać wytyczne dotyczące sytuacji, w których personel lub dzieci uzyskują dostęp do systemów oprogramowania edukacyjnego, baz danych lub innych produktów stron trzecich za pośrednictwem osobistych urządzeń elektronicznych lub z domu, a zatem łączą dane osobowe, w tym metadane, z życie prywatne i rodzinne z ich historią zawodową lub edukacyjną.

7.2. Rzetelność

7.2.1. Zgodnie z art. 5 ust. 4 lit. a) dane są przetwarzane rzetelnie i w przejrzysty sposób. W art. 8 ust. 1 lit. a) –e) Konwencji 108+ określono, jakie są oczekiwania dotyczące spełnienia wymogu przejrzystości i kompletności przetwarzania danych. Zgodnie z pkt 68 Sprawozdania wyjaśniającego do Konwencji format może być dowolny, jeśli tylko rzetelnie i skutecznie zapewnia informacje osobie, której dane dotyczą. Oznacza to na przykład, zgodnie z rozwijającymi się zdolnościami dziecka, w przyjaznym dla dziecka, zrozumiałym języku i dostępnych formatach alternatywnych do samego tekstu, w stosownych przypadkach. Powinien być interpretowany w kontekście edukacyjnym jako konieczny do zrozumienia przez kompetentne dziecko lub przez prawnych opiekunów młodszych dzieci lub odpowiednio do zmieniających się zdolności dziecka.

7.2.2. Proaktywne dostarczanie dostępnych informacji o wszystkich prawach osoby, której dane dotyczą, przysługujących dziecku i jego opiekunowi prawnemu przed rozpoczęciem procesu zbierania danych, jest niezbędne do spełnienia obowiązków w zakresie przejrzystości. Co do zasady zarówno dziecko, jak i opiekunowie prawni powinni otrzymywać informacje bezpośrednio. Udzielenie informacji

opiekunowi prawnemu nie powinno stanowić alternatywy dla przekazania informacji dziecku, stosownie do jego rozwijających się zdolności.

7.2.3. Placówki edukacyjne powinny prowadzić i publikować na poziomie instytucji rejestr swoich czynności przetwarzana danych, listę partnerów, takich jak sprzedawcy i podwykonawcy, oceny skutków dla ochrony danych, informacje o prywatności oraz wszelkie zmiany warunków w czasie.

7.2.4. Placówki edukacyjne powinny zgłaszać organom nadzorczym zgodnie z Konwencją 108+ oraz samym osobom, których dane dotyczą, w przypadku naruszeń zgodnie z art. 7 ust. 2 Konwencji i udostępniać raporty z audytów w celu wykazania ich rozliczalności i przejrzystości przetwarzania danych stronom trzecim.

7.2.5. Oświadczenia o przetwarzanych danych osobowych powinny być dostępne na żądanie w ramach praw dostępu osoby. Za dobrą praktykę można uznać oferowanie takich informacji za pośrednictwem narzędzi samoobsługowych, bezpłatnych dla dziecka jako osoby, której dane dotyczą.

7.2.6. Przed transgranicznym przepływem danych osobowych i z zapewnieniem odpowiedniego stopnia ochrony zgodnie z art. 14 ust. 3 i 4 należy poinformować osobę, której dane dotyczą, oraz jej opiekunów prawnych.

7.3. Ocena ryzyka

7.3.1. Administratorzy muszą ocenić prawdopodobny wpływ zamierzonego przetwarzania danych na prawa i podstawowe wolności dziecka, przed rozpoczęciem przetwarzania danych, zgodnie z art. 10 ust. 2 Konwencji 108+ i zaplanować przetwarzanie danych w sposób zapobiegający lub minimalizujący ryzyko ingerencji w te prawa i podstawowe wolności w odniesieniu do art. 10 ust. 3 Konwencji 108+ i wszystkich innych jej zasad.

7.3.2. Zakup narzędzi i usług, które przetwarzają dane dzieci, zapewnia poszanowanie dzieci jako osób, których dane dotyczą, oraz praw ich opiekunów prawnych i ich uzasadnionych oczekiwań w ramach podejmowania decyzji przy wprowadzaniu dowolnego produktu zakupionego lub tzw. freeware.

7.3.3. Tam, gdzie przepisy dotyczące wolności informacji mają zastosowanie do organów publicznych, kodeksy postępowania mogą zawierać sugestię jako najlepszą praktykę, aby oceny skutków dla ochrony danych mogły być udostępniane w ramach rutynowych programów publikacji, aby ułatwić szeroką przejrzystość i rozliczalność.

7.3.4. Zgodnie z najlepszą praktyką oraz zgodnie z prawem krajowym i międzynarodowym, opinie dzieci powinny być częścią każdej przeprowadzanej oceny skutków dla praw dziecka w celu uwzględnienia ich punktu widzenia w odniesieniu do przetwarzania danych.

7.4. Zatrzymywanie

7.4.1. W momencie, gdy dziecko kończy naukę, należy przechowywać jedynie minimalną niezbędną ilość danych umożliwiających jego identyfikację, a także w najlepszym interesie dziecka, aby wykazać osiągnięcia, zabezpieczyć jego przyszłe prawa dostępu i wypełnić ustawowe zobowiązania.

7.4.2. Dane osobowe opuszczające placówkę edukacyjną nie powinny być przechowywane w formie umożliwiającej identyfikację dłużej niż to niezbędne, zgodnie z art. 5 ust. 4 lit. e).

7.4.3. Placówki edukacyjne nie powinny przechowywać danych osobowych w formie umożliwiającej identyfikację dłużej niż to niezbędne, z należytym uwzględnieniem przepisów art. 5 ust. 4, art. 7 ust. 2, art. 8 ust. 1 i art. 9 Konwencji 108+ . Mogą mieć zastosowanie wyjątki, które szanują istotę podstawowych praw i wolności dziecka i stanowią proporcjonalny środek, niezbędny w społeczeństwie demokratycznym do celów art. 11 Konwencji 108+.

7.4.4. Po zakończeniu każdego etapu kształcenia obowiązkowego lub w przypadku zmiany placówki (dla wszystkich grup wiekowych, w przedszkolu, szkole podstawowej, średniej, dalszej i wyższej) najlepszą praktyką powinno być, aby dzieci otrzymywały pełną kopię swoich akt zawierających informacje o zatrzymywaniu danych osobowych i zniszczeniu, czyli aby uzyskały informacje, które dane osobowe są nadal zatrzymywane i przetwarzane, przez kogo, w jakim celu, po opuszczeniu placówki przez dziecko, a w każdym przypadku administratorzy danych muszą utrzymywać mechanizmy umożliwiające im wypełnianie bieżących obowiązków osobie, której dane dotyczą.

7.4.5. W związku z tym, że pozbawienie danych charakteru identyfikującego jest tak trudne, najlepszą praktyką powinno być zakazywanie ponownej identyfikacji i wymaganie, aby strony trzecie nie podejmowały żadnych prób ponownej identyfikacji ani nie pozwalały na to innym po otrzymaniu danych, które nie umożliwiają identyfikacji. W przypadku gdy ma to zastosowanie zgodnie z prawem krajowym niektórych Państw-Stron, należy uznać, że ponowna identyfikacja może stanowić przestępstwo.

7.5. Zabezpieczanie danych osobowych w środowisku edukacyjnym

Placówki edukacyjne mogą być zaangażowane w przetwarzanie danych dzieci na dużą skalę przez długi czas. Stosowanie odpowiednich środków bezpieczeństwa w odniesieniu do tych danych i ich środowisk przetwarzania, zarówno danych nieaktywnych, jak i danych w trakcie przekazywania, ma kluczowe znaczenie dla zapewnienia ochrony danych dzieci zgodnie z najwyższymi standardami. Jak stanowi Konwencja, środki bezpieczeństwa powinny uwzględniać aktualny stan wiedzy w zakresie metod i technik zabezpieczenia danych w dziedzinie przetwarzania danych. Ich koszt powinien być współmierny do wagi i prawdopodobieństwa potencjalnego ryzyka. Bezpieczeństwo danych obejmuje dalsze obowiązki, wymienione poniżej kontrole są szczególnie istotne w przypadku przetwarzania w placówkach edukacyjnych.

7.5.1. Środki ochrony stosowane wobec danych osobowych powinny opierać się na ocenie ryzyka zgodnie z normami branżowymi i najlepszymi praktykami oraz z wykorzystaniem ustalonych wskazówek technicznych (takich jak seria ISO 27000 i inne, w stosownych przypadkach).

7.5.2. Środki powinny być dostosowane do okoliczności przetwarzania i ryzyka, na jakie narażone są dzieci, a także powinny mieć na celu zapewnienie poufności, integralności, dostępności i autentyczności danych dzieci w każdym kontekście, w jakim są one przetwarzane, a także odporność systemów przetwarzania oraz usług.

7.5.3. Ocena ryzyka powinna zatem dążyć do osiągnięcia wyników, które uwzględniają wysokie standardy bezpieczeństwa w całym przetwarzaniu, biorąc pod uwagę jego charakter, zakres, kontekst i cele, a także stwarzane przez nie ryzyko. Taka ocena musi być uzasadniona względami konieczności i proporcjonalności oraz podstawowymi zasadami ochrony danych:

- w zakresie zagrożeń, w tym fizycznej dostępności;
- sieciowy dostęp do urządzeń i danych oraz
- tworzenie kopii zapasowych i archiwizacja danych.

7.5.4. Dostępność fizyczna (np. do urządzeń i danych w środowisku edukacyjnym) obejmuje dane gromadzone lub przechowywane co najmniej w następujących kontekstach:

- nauczanie stacjonarne / e-learning (w tym nauczanie na odległość poza terenem szkoły);
- administracja szkolna;
- pomieszczenia (dostęp fizyczny, CCTV w tym w pojazdach szkolnych, czytnikach biometrycznych).

7.5.5. Należy rozważyć, w jaki sposób użytkownicy-dzieci powinni uwierzytelniać się w systemach, w tym, czy jest to wymagane w kontekście przetwarzania. Oceny ryzyka powinny uwzględniać metody uwierzytelniania wymagane w każdym wdrożeniu, z należytym uwzględnieniem alternatywnych podejść, jeśli są one dostępne, i chronią prywatność użytkowników, takich jak w pełni identyfikowalne systemy identyfikatorów i haseł w porównaniu z tokenami i autoryzacją na poziomie atrybutów. Uwierzytelnianie powinno być solidne i być w stanie zapewniać ochronę danych. Zasady ograniczenia celu i minimalizacji danych powinny również stanowić element oceny każdego systemu uwierzytelniania.

7.5.6. W przypadku dostępu do danych w sieci prawie na pewno wymagane jest uwierzytelnianie i jest pożądane, aby zapobiec nieuprawnionemu dostępowi. Powstają te same pytania, jak w przypadku dostępu na miejscu: jaka jest najbardziej odpowiednia technologia uwierzytelniania i czy dostęp jest przyznawany na podstawie indywidualnej tożsamości (imię, nazwisko) lub atrybutu („uczeń tej szkoły").

7.5.7. Ocena ryzyka przed przetwarzaniem musi również ocenić, czy dane są chronione przed nieuprawnionym dostępem, modyfikacją i usunięciem / zniszczeniem. Jeśli dane są przetwarzane poza siedzibą (na przykład przez usługodawców będących stronami trzecimi), dostawcy usług edukacyjnych muszą mieć świadomość swoich bieżących obowiązków jako administratorów danych. Należy dołożyć należytej staranności w celu ustalenia zdolności strony trzeciej do odpowiedniej ochrony danych osobowych, w tym poufności, integralności i dostępności.

7.5.8. Podobne pytania należy zadać w odniesieniu do danych cyfrowych, które są przechowywane do celów tworzenia kopii zapasowych i / lub archiwizacji, zwłaszcza jeśli usługi te są świadczone przez strony trzecie - bezpośrednio (np. w przypadku usług archiwalnych objętych umową) lub pośrednio, jako część dostępności danych zabezpieczenia oferowane przez e-learningową usługę administracyjną.

7.5.9. Państwa-Strony nie powinny zakazywać prawnie ani praktykować stosowania technologii szyfrowania dla dzieci.[18] W przypadku gdy szyfrowanie nie jest zintegrowane z aplikacją lub usługą, może być pożądane szyfrowanie danych „ręcznie" jako samodzielny środek ochronny.

7.5.10. Można zastosować wiele poziomów ochrony (a nawet je połączyć). Zaszyfrowanymi danymi należy zarządzać w podobny sposób, jak danymi kopii zapasowych / archiwalnymi. Oznacza to, że proces odzyskiwania danych (ze stanu zaszyfrowanego lub z kopii zapasowej lub archiwum) powinien

18 Zalecenie CM/Rec (2018)7 Komitetu Ministrów dla państw członkowskich w sprawie Wytycznych dotyczących poszanowania, ochrony i wypełniania praw dziecka w środowisku cyfrowym: https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

być regularnie testowany. Należy wziąć pod uwagę procedury awaryjne na wypadek, gdyby główna odpowiedzialna osoba nie mogła wykonać tego zadania.

7.5.11. Wszelkie wprowadzone środki powinny być regularnie testowane, jak określono w art. 7 Konwencji 108+, i uwzględniać zmieniające się metody i techniki bezpieczeństwa danych oraz zagrożenia, a także podlegać regularnym przeglądom i aktualizacjom w razie potrzeby.

7.6. Zautomatyzowane decyzje i profilowanie

7.6.1. Każda osoba ma prawo nie podlegać decyzji, która ma na nią istotny wpływ, opartej wyłącznie na zautomatyzowanym przetwarzaniu danych bez uwzględnienia jej opinii zgodnie z art. 9 ust. 1 lit. a) i art. 9 ust. 1 lit. c) Konwencji 108+. Znajomość powodów leżących u podstaw przetwarzania danych w przypadku, gdy wyniki mają zastosowanie w odniesieniu do osoby, której dane dotyczą, powinna być łatwo dostępna.

7.6.2. Profilowanie dzieci powinno być prawnie zabronione. W wyjątkowych okolicznościach Państwa mogą znieść to ograniczenie, gdy leży to w najlepszym interesie dziecka lub gdy istnieje nadrzędny interes publiczny, pod warunkiem że odpowiednie gwarancje są przewidziane przez prawo (zgodnie z pkt 37 Wytycznych dotyczących dzieci w środowisku cyfrowym).

7.6.3. Osiągnięcia dzieci nie powinny być rutynowo profilowane w celu pomiaru systemów, na przykład do mierzenia zarządzania wynikami szkoły lub nauczycieli na podstawie tego, że nie jest to uzasadnione nadrzędnym interesem publicznym.

7.6.4. Wytyczne dotyczące sztucznej inteligencji i ochrony danych[19] powinny być przestrzegane w placówkach edukacyjnych w odniesieniu do automatycznego przetwarzania danych osobowych, aby zapewnić, że zastosowania sztucznej inteligencji nie naruszają godności człowieka, praw człowieka i podstawowych wolności każdego dziecka, niezależnie od tego czy jako osoby fizycznej, czy jako społeczności, w szczególności w odniesieniu do prawa do niedyskryminacji.

7.6.5. Uznanie praw dziecka, jako osoby, której dane dotyczą, oraz jego prawnych opiekunów jest konieczne zarówno w kontekście podejmowania decyzji algorytmicznych, związanych z przetwarzaniem danych osobowych z wykorzystaniem sztucznej inteligencji i świadomym przetwarzaniem (patrz Wytyczne dotyczące ochrony danych i sztucznej inteligencji).[20]

7.6.6. Administratorzy danych są odpowiedzialni za przeprowadzanie ocen skutków dla ochrony danych i prywatności. Oceny powinny uwzględniać szczególny wpływ na prawa dziecka[21] i wykazywać, że wyniki zastosowań algorytmicznych leżą w najlepszym interesie dziecka i zapewniać, aby nie miał miejsca niewłaściwy wpływ na rozwój dziecka w nieprzejrzysty sposób.

7.6.7. Personalizacja treści może (ale nie zawsze) stanowić nieodłączny i oczekiwany element niektórych usług online, a zatem może być uznana za niezbędną do wykonania umowy w niektórych

19 Wytyczne dotyczące sztucznej inteligencji i ochrony danych, dokument T-PD (2019) 01, dostępne: https://rm.coe.int/2018-lignes-directrices-sur-l-intelligence-artificielle-et-la-protecti/168098e1b7

20 Tamże

21 Komitet Praw Dziecka, Komentarz ogólny nr 16(2013) dot. obowiązków państwa w zakresie oddziaływania sektora biznesowego na rzecz praw dziecka pkt 77-81, https://www.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf

przypadkach między usługodawcą a środowiskiem edukacyjnym, ale nie w odniesieniu do dziecka, ponieważ nie może ono zawrzeć umowy[22], nawet pod naciskiem środowiska edukacyjnego.

7.6.8. Prognozy dotyczące grup lub osób o wspólnych cechach, oparte na analizie dużych zbiorów danych osobowych, nadal należy traktować jako przetwarzanie danych osobowych, nawet jeśli nie ma zamiaru, aby skutkowało ingerencją w odniesieniu do osoby.

7.6.9. Dystrybucja i używanie oprogramowania lub korzystanie z usług przeznaczonych do obserwowania i monitorowania działań użytkowników na terminalu lub sieci komunikacyjnej tworzących profil zachowania nie powinno być dozwolone, chyba że jest to wyraźnie przewidziane w prawie krajowym i towarzyszą temu odpowiednie zabezpieczenia, jak określono w zasadzie 3.8 zalecenia Rady Europy CM/Rec (2010)13 oraz w uzasadnieniu[23] dotyczącym ochrony osób fizycznych w związku z automatycznym przetwarzaniem danych osobowych w kontekście profilowania.

7.7. Dane biometryczne

7.7.1. Dane biometryczne nie powinny być rutynowo przetwarzane w placówkach edukacyjnych. Wykorzystanie danych biometrycznych w placówkach edukacyjnych w wyjątkowych okolicznościach, takich jak weryfikacja tożsamości, w tym zdalna opieka, jest dozwolone tylko wtedy, gdy nie mniej inwazyjna metoda może osiągnąć ten sam cel, zgodnie z zasadą bezwzględnej konieczności, po przeprowadzeniu oceny skutków dla ochrony danych i przy odpowiednich zabezpieczeniach przewidzianych prawem, zgodnie z art. 6 ust. 1 Konwencji 108+. Powinno to obejmować należyte uwzględnienie zagrożeń, jakie przetwarzanie danych wrażliwych może stwarzać dla praw i podstawowych wolności dziecka, włączając dyskryminację przez całe życie. Należy oferować metody alternatywne bez uszczerbku.

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

7.7.3. Uznając, że definicja danych biometrycznych w Artykule 6 Konwencji służy do jednoznacznej identyfikacji osoby, organy powinny również zwracać uwagę na wrażliwość przetwarzania danych dotyczących ciała i danych behawioralnych dziecka, które może nie służyć weryfikacji tożsamości. Zamiast tego celem takiego przetwarzania danych może być wpływanie na fizyczne lub psychiczne doświadczenia dziecka, na przykład we wciągającej rzeczywistości wirtualnej. Charakterystyka przetwarzania dotycząca głosu, ruchu oczu i chodu; społeczne zdrowie emocjonalne i psychiczne oraz nastrój; i reakcje na neurostymulację, w celu wpływania na zachowanie dziecka lub monitorowania jego zachowania, powinny być wykonywane w oparciu o zasadę ostrożności i traktowane jako dane biometryczne są objęte Konwencją 108+, nawet jeśli nie służą do celów jednoznacznej identyfikacji osoby.

7.7.4. Placówki edukacyjne powinny zwracać szczególną uwagę na to, kiedy korzystanie nie z usługi stanowi umowę, na przykład w przypadku korzystania z oprogramowania do wideokonferencji, aby

22 Personalizacja treści może (ale nie zawsze) stanowić nieodłączny i oczekiwany element niektórych usług online, dlatego w niektórych przypadkach może być uznana za niezbędną do wykonania umowy z usługobiorcą. (EROD, Wytyczne 2/2019)
23 Zalecenie Rady Europy CM/Rec (2010)13 i uzasadnienie (2011) https://rm.coe.int/16807096c3

móc wdrażać programy nauczania na odległość, oraz w których pracownicy mogą wyrazić zgodę na warunki świadczenia usług, które obejmują przetwarzanie i nagrywanie treści, w tym obrazów dzieci i danych głosowych. Pracownicy powinni zapewnić, aby w przypadku gdy przetwarzanie danych odbywało się na podstawie zgody, zgoda ta nie mogła zostać przyjęta przez placówkę edukacyjną i udzielona w imieniu dziecka, ale musi być świadoma i jednoznacznie dobrowolnie wyrażona przez osobę, której dane dotyczą, dziecko, zgodnie z jego ewoluującymi zdolnościami możliwości lub ich prawnego opiekuna, a także zgodnie ze wszystkimi innymi zasadami ochrony danych, w tym zasadą ograniczenia celu.

8. Zalecenia dla branży

Organy nadzorcze, które przekształcają niniejsze wytyczne w kodeksy postępowania, powinny to robić w oparciu o szeroką współpracę z twórcami i branżą, praktykami w dziedzinie edukacji, środowiskiem akademickim, organizacjami reprezentującymi nauczycieli i rodziny oraz ze społeczeństwem obywatelskim i samymi dziećmi. Normy mogą obejmować minimalne kryteria lub jasne wytyczne dotyczące zamówień w odniesieniu do produktów lub usług związanych z przetwarzaniem danych dzieci, w tym produktów lub usług oferowanych bezpłatnie lub po niskich kosztach, a także we wszelkich badaniach produktów i badaniach.

8.1. Normy

8.1.1. W związku z tym, że dzieci zasługują na szczególną ochronę, oczekiwane standardy przetwarzania danych dzieci w sektorze edukacji powinny z założenia stawiać wysoko poprzeczkę, aby spełniać odpowiednie standardy jakości i praworządności, a także zasady ochrony danych w fazie projektowania i domyślnej ochrony danych.

8.1.2. Normy mogą być określone w kodeksach postępowania i certyfikacji, które powinny zostać opracowane na podstawie szerokiej współpracy z twórcami i branżą, praktykami w dziedzinie edukacji, środowiskiem akademickim, organizacjami reprezentującymi nauczycieli, rodziny i dzieci, ze społeczeństwem obywatelskim i samymi dziećmi.

8.1.3. Postanowienia umów w zakresie zgodnego z prawem przetwarzania danych, uzgodnione przy udzielaniu zamówienia, powinny obowiązywać również po nabyciu, połączeniu lub innym przejęciu przez inny podmiot.

Musi istnieć wystarczająco uczciwy okres na komunikację w sprawie wszelkich zmian warunków i prawa do zmiany nowych warunków lub sprzeciwu wobec nich, rozwiązania umowy i wycofania danych studenta na żądanie.

8.2. Przejrzystość

8.2.1. Twórcy muszą upewnić się, że ich własne rozumienie wszystkich funkcji projektowanych przez nich produktów może być wystarczająco wyjaśnione, aby spełnić wymogi regulacyjne i prawne, oraz

unikać tworzenia dużego ciężaru konieczności sprawdzenia z założenia, nieodpowiedniego dla personelu placówek edukacyjnych i dzieci.

8.2.2. Informacje dotyczące prywatności i inne opublikowane warunki, polityki i standardy społeczności muszą być zwięzłe i napisane jasnym językiem odpowiednim dla dzieci. Przyjazne dziecku metody komunikacji nie muszą osłabiać wyjaśnień, które są konieczne do rzetelnego przetwarzania, ale nie powinny być przesadne i powinny być oddzielone od warunków prawnych i umownych dla opiekunów prawnych i wychowawców. Warstwowe informacje o prywatności mogą pomóc w połączeniu potrzeby kompletnych, ale jednocześnie skutecznych informacji.

8.3. Zaprojektuj funkcje z uwzględnieniem skutków dla ochrony danych i prywatności

8.3.1. Oczekiwania dotyczące poszanowania zasad ochrony danych w fazie projektowania i domyślnej ochrony danych powinny zapobiegać projektowaniu obejmującemu funkcje, które mogą zachęcać dzieci do podawania niepotrzebnych danych osobowych lub obniżania ustawień prywatności.

8.3.2. Przetwarzanie danych osobowych w celu poprawy usług i bezpieczeństwa musi być ściśle niezbędne oraz w granicach świadczenia usługi podstawowej, a także uzasadnionych oczekiwań i dostarczenia użytkownikom zakontraktowanej usługi.

8.3.3. Analizy danych[24] w oparciu o dane osobowe i śledzenie użytkowników nie należy traktować jako formy ulepszania usług lub zwiększania bezpieczeństwa i nie jest niezbędne do wykonania umowy.

8.3.4. Ulepszenia produktu, na przykład te, które mają na celu dodanie nowych funkcji do aplikacji lub poprawę jej wydajności, powinny wymagać nowej akceptacji lub zgody oraz wyrażenia zgody przed zainstalowaniem. W przypadku powołania się na inną podstawę prawną niż umowa, osobę, której dane dotyczą, należy poinformować przed aktualizacjami i zgodnie z podstawą prawną.

8.3.5. Szczególną uwagę należy zwrócić na artykuł 14 Konwencji, aby upewnić się, że transgraniczne przepływy danych osobowych do celów edukacyjnych spełniają warunki artykułu, aby ograniczyć transgraniczne przepływy danych osobowych do celów edukacyjnych oraz zapewnić, że przepływy odbywają się w uznanych ramach ochrony danych.

8.3.6. Śledzenie geolokalizacji w celu zidentyfikowania lokalizacji użytkowania, użytkownika, wskazania funkcji w aplikacji lub do celów profilowania powinno być wdrażane tylko wtedy, gdy jest to niezbędne i zgodnie z odpowiednią podstawą prawną. Usługi powinny zapewniać wskaźnik, kiedy śledzenie lokalizacji jest aktywne i umożliwiać łatwe wyłączanie bez utraty podstawowych funkcji. Takie profile i historia powinny być łatwe do usunięcia po zakończeniu sesji.

8.3.7. Dane dzieci zebrane za pomocą oprogramowania edukacyjnego owych nie powinny być przetwarzane w celu wyświetlania lub kierowania reklam behawioralnych, w przypadku technologii reklamowej w postaci aukcji w czasie rzeczywistym lub reklam w aplikacjach, na potrzeby marketingu skierowanego do dzieci lub rodzin, w celu ulepszania produktów lub dodatkowych produktów kierowanych przez sprzedawców.

24 Wytyczne dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych w świecie Big Data (2017) TPD (2017)01