



**398/09/PL  
WP 160**

**Opinia 2/2009 w sprawie ochrony danych osobowych dzieci  
(Ogólne wytyczne i szczególny przypadek szkół)**

**Przyjęta dnia 11 lutego 2009 r.**

Grupa robocza została ustanowiona na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określa art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (Sądownictwo Cywilne, Prawa i Obywatelstwo) Dyrekcji Generalnej ds. Sprawiedliwości, Wolności i Bezpieczeństwa Komisji Europejskiej, B-1049 Bruksela, Belgia, Biuro nr LX-46 01/06.

Strona internetowa: [http://ec.europa.eu/justice\\_home/fsj/privacy/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm)

## **Ochrona danych osobowych dzieci**

(Ogólne wytyczne i szczególny przypadek szkół)

### **I - Wprowadzenie**

#### **1) - Opracowanie**

Niniejsza opinia dotyczy ochrony informacji dotyczących dzieci. Jest skierowana przede wszystkim do osób, które zajmują się danymi osobowymi dzieci. W przypadku szkół dotyczy to w szczególności nauczycieli i władz szkolnych. Opinia skierowana jest również do krajowych organów nadzoru nad ochroną danych osobowych, które są odpowiedzialne za monitorowanie przetwarzania takich danych.

Niniejszy dokument należy postrzegać w kontekście ogólnej inicjatywy Komisji Europejskiej opisanej w komunikacie „W kierunku strategii UE na rzecz praw dziecka”. Celem opinii, która stanowi wkład w realizację tego ogólnego zamierzenia, jest wzmocnienie podstawowego prawa dzieci do ochrony danych osobowych.

Temat ten nie jest zupełnie nowy dla Grupy Roboczej Art. 29 ds. Ochrony Danych, która przyjęła już kilka opinii związanych z tą kwestią. Jej opinie w sprawie kodeksu postępowania Federacji Europejskich Stowarzyszeń Marketingu Bezpośredniego FEDMA (Opinia 3/2003), geolokalizacji (Opinia 5/2005) oraz wiz i danych biometrycznych (Opinia 3/2007) zawierają określone zasady lub zalecenia w kwestii ochrony danych osobowych dzieci.

Celem niniejszego dokumentu jest skonsolidowane ujęcie tego zagadnienia w sposób uporządkowany, poprzez określenie obowiązujących podstawowych zasad (część II) i zilustrowanie ich odniesieniami do danych gromadzonych przez szkoły (część III).

Wybór obszaru danych gromadzonych przez szkoły wynika z tego, że szkoła jest jednym z ważniejszych miejsc w życiu dzieci i odbywa się w niej znacząca część ich codziennych czynności.

Znaczenie tego obszaru wynika również ze szczególnie chronionego charakteru większości danych przetwarzanych w instytucjach oświatowych.

#### **2) – Cel i zakres**

Celem niniejszego dokumentu jest przeprowadzenie analizy ogólnych zasad związanych z ochroną danych osobowych dzieci oraz wyjaśnienie ich znaczenia w określonej kluczowej dziedzinie, a mianowicie w dziedzinie danych gromadzonych przez szkoły.

Pozwoli to na ogólne określenie kwestii istotnych dla ochrony danych osobowych dzieci oraz na zapewnienie wytycznych osobom pracującym w tej dziedzinie.

Zgodnie z kryteriami określonymi w większości stosownych międzynarodowych aktów prawnych, dziecko jest osobą poniżej osiemnastego roku życia, o ile przed tym wiekiem nie osiągnie pełnoletniości prawnej.<sup>1</sup>

Dziecko jest istotą ludzką w pełnym tego słowa znaczeniu. Z tego względu dziecko musi mieć możliwość korzystania ze wszystkich praw osoby, łącznie z prawem do ochrony jej danych osobowych. Dziecko znajduje się jednak w szczególnej sytuacji, którą należy postrzegać w dwóch perspektywach: statycznej i dynamicznej.

Ze statycznego punktu widzenia dziecko jest osobą, która nie osiągnęła jeszcze dojrzałości fizycznej i psychicznej. Z dynamicznego punktu widzenia dziecko podlega procesowi rozwoju fizycznego i psychicznego, w wyniku którego stanie się osobą dorosłą. Prawa dziecka oraz wykonywanie tych praw – włącznie z prawem ochrony danych – powinny być wyrażone w sposób uwzględniający obie te perspektywy.

Niniejsza opinia jest oparta na przekonaniu, że edukacja i odpowiedzialność są decydującymi narzędziami ochrony danych osobowych dzieci. Zbadano w niej główne zasady istotne dla tej kwestii. Większość z nich dotyczy praw dziecka, ale będą one zbadane w kontekście ochrony danych osobowych.

Wszystkie te zasady są zawarte w najbardziej podstawowych, obowiązujących aktach międzynarodowych. Niektóre z nich dotyczą ogólnych praw człowieka, ale zawierają także szczegółowe przepisy dotyczące dzieci. Najważniejszymi z nich są:

- Powszechna deklaracja praw człowieka z dnia 10 grudnia 1948 r. – art. 25, art. 26 ust. 3;
- europejska Konwencja o ochronie praw człowieka i podstawowych wolności z dnia 4 listopada 1950 r. – art. 8;
- Karta praw podstawowych Unii Europejskiej z dnia 7 grudnia 2000 r. – art. 24<sup>2</sup>.

Innymi dokumentami bezpośrednio dotyczącymi praw dziecka są:

- Genewska deklaracja praw dziecka z 1923 r.;
- Konwencja o prawach dziecka ONZ z dnia 20 listopada 1989 r.;
- Europejska konwencja o wykonywaniu praw dzieci, Rada Europy nr 160 z dnia 25 stycznia 1996 r.;
- rezolucja Parlamentu Europejskiego „W kierunku strategii UE na rzecz praw dziecka” z dnia 16 stycznia 2008 r.

<sup>1</sup> - Przede wszystkim art. 1 Konwencji o prawach dziecka ONZ z dnia 20 listopada 1989 r.

<sup>2</sup> - A także:

- Deklaracja helsińska, czerwiec 1964 r., cz. I-11,
- Międzynarodowy pakt praw gospodarczych, społecznych i kulturalnych z dnia 16 grudnia 1966 r., art. 10 ust. 3;
- Międzynarodowy pakt praw obywatelskich i politycznych z dnia 16 grudnia 1966 r., art. 16, 24,
- Protokół fakultatywny z dnia 16 grudnia 1966 r.

Oczywiście zawsze należy uwzględniać ogólną perspektywę ochrony danych osobowych, zawartą w dyrektywach dotyczących ochrony danych osobowych (dyrektywa 95/46/WE z dnia 24 października 1995 r. i dyrektywa 2002/58/WE z dnia 12 lipca 2002 r.), a częściowo również w innych aktach prawnych<sup>3</sup>.

## **II – Zasady podstawowe**

### **A – Ujęcie ogólne**

#### **1) – Najlepiej pojęty interes dziecka**

Główną zasadą prawną jest najlepsze zabezpieczenie interesów dziecka<sup>4</sup>.

Podstawą tej zasady jest przekonanie, że osoba, która nie osiągnęła jeszcze dojrzałości fizycznej i psychicznej, potrzebuje większej ochrony niż inne osoby. Zasada ma na celu poprawę warunków, w jakich żyje dziecko, i zmierza do wzmocnienia prawa dziecka do rozwoju jego osobowości. Zasady tej muszą przestrzegać wszystkie podmioty, publiczne lub prywatne, które podejmują decyzje dotyczące dzieci. Ma ona zastosowanie również w odniesieniu do rodziców i innych przedstawicieli prawnych dzieci, jeżeli interesy każdej ze stron są sprzeczne lub gdy w imieniu dziecka występuje przedstawiciel. Zazwyczaj zasadę tę powinien stosować przedstawiciel dziecka, jednak jeżeli zaistnieje konflikt interesów między dziećmi a ich przedstawicielami prawnymi, decyzję powinien podjąć sąd lub w stosownych przypadkach organ ochrony danych.

#### **2) – Ochrona i opieka niezbędne dla dobra dzieci**

Zasada najlepiej pojętego interesu dziecka wymaga odpowiedniej oceny sytuacji dziecka. Wymaga to uświadomienia sobie dwóch kwestii. Po pierwsze, niedojrzałość dzieci sprawia, że są one wrażliwe, i ten fakt należy zrekompensować właściwą ochroną i opieką. Po drugie, prawo dziecka do rozwoju może być realizowane w pełni jedynie przy pomocy lub poprzez ochronę innych podmiotów lub osób<sup>5</sup>.

Obowiązek ochrony spoczywa na rodzinie, społeczeństwie i państwie.

Należy zwrócić uwagę na fakt, że w celu osiągnięcia odpowiedniego poziomu opieki nad dziećmi niekiedy konieczne będzie obszerne przetwarzanie ich danych osobowych przez różne strony. Będzie to dotyczyło głównie obszarów opieki społecznej: edukacji, zabezpieczenia społecznego, opieki zdrowotnej itp. Nie jest to jednak niespójne z

<sup>3</sup> - Wytyczne OECD z dnia 23 września 1980 r.,  
- Konwencja nr 108 Rady Europy z dnia 28 stycznia 1981 r. oraz Protokół dodatkowy z dnia 8 listopada 2001r.,  
- Wytyczne ONZ z dnia 14 grudnia 1990 r.

<sup>4</sup> Zasada ta została zagwarantowana w Konwencji o prawach dziecka ONZ (art. 3), a następnie potwierdzona w Konwencji nr 192 Rady Europy (art. 6) oraz w Karcie praw podstawowych Unii Europejskiej (art. 24 ust. 2).

<sup>5</sup> Prawo do ochrony jest prawem podstawowym i jako takie zostało zawarte w Powszechnej deklaracji praw człowieka (art.25) oraz zostało potwierdzone w Międzynarodowym pakcie praw obywatelskich i politycznych (art. 24), Międzynarodowym pakcie praw gospodarczych, społecznych i kulturalnych (art. 10 ust. 3), oraz ostatnio w Karcie praw podstawowych Unii Europejskiej (art. 24).

odpowiednią i wzmocnioną ochroną danych osobowych w tych sektorach społecznych, chociaż w przypadku wymiany danych dotyczących dzieci należy zachować szczególną ostrożność. Taka wymiana może przesłonić zasadę celowości (ograniczenie celu) i nieść ze sobą ryzyko, że profile będą tworzone bez odniesienia się do zasady proporcjonalności.

### **3) – Prawo do prywatności**

Dziecko, jako istota ludzka, ma prawo do prywatności.

Artykuł 16 Konwencji o prawach dziecka ONZ stanowi, że żadne dziecko nie będzie podlegało arbitralnej lub bezprawnej ingerencji w sferę jego życia prywatnego, rodzinnego lub domowego czy w korespondencję ani bezprawnym zamachom na jego honor i reputację<sup>6</sup>.

Tego prawa musi przestrzegać każdy, nawet przedstawiciel prawny dziecka.

### **4) - Przedstawicielstwo**

Aby móc korzystać z większości swoich praw, dzieci potrzebują przedstawicielstwa prawnego. Nie oznacza to jednak, że status przedstawiciela prawnego ma bezwzględne lub bezwarunkowe pierwszeństwo nad statusem dziecka, ponieważ w związku z najlepiej pojętym interesem dziecka mogą oni czasem uzyskiwać prawa dotyczące ochrony danych osobowych, które mogą być nadrzędne względem życzeń rodziców lub innych przedstawicieli prawnych. Konieczność wyznaczenia przedstawicielstwa prawnego nie oznacza też, że nie należy z dziećmi, które osiągnęły określony wiek, konsultować spraw z nimi związanych.

Jeżeli przetwarzanie danych osobowych dziecka rozpoczęło się bez zgody prawnego przedstawiciela, zainteresowane dziecko może po osiągnięciu pełnoletniości wycofać zgodę. Jeżeli jednak chce, by przetwarzanie danych było kontynuowane, osoba, której te dane dotyczą, powinna wydać wyraźną zgodę, gdy tylko zaistnieje taka potrzeba.

Na przykład jeżeli prawny przedstawiciel wydał wyraźną zgodę na włączenie jego dziecka (osoby, której dotyczą dane) do badania klinicznego, po uzyskaniu przez dziecko zdolności do odpowiednich czynności administrator danych powinien upewnić się, że nadal ma podstawę do przetwarzania danych osobowych osoby, której te dane dotyczą. Ponieważ chodzi tu o szczególnie chronione dane, aby kontynuować badanie, kontroler powinien rozważyć przede wszystkim uzyskanie wyraźnej zgody od samej osoby, której dotyczą dane.

Przy tej kwestii należy pamiętać, że prawa do ochrony danych osobowych przysługują dziecku, a nie jego przedstawicielom prawnym, którzy jedynie je wykonują.

---

<sup>6</sup> To prawo jest potwierdzeniem ogólnego prawa do prywatności zagwarantowanego w art. 12 powszechnej deklaracji, art. 17 Międzynarodowego paktu praw obywatelskich i politycznych oraz w art. 8 Europejskiej konwencji o ochronie praw człowieka.

## **5) – Konkurencyjne interesy: prywatność i najlepiej pojęty interes dziecka**

Zasada najlepiej pojętego interesu dziecka może odgrywać podwójną rolę. Na pierwszy rzut oka, zasada wymaga chronienia prywatności dziecka w najlepszy możliwy sposób przez wprowadzenie w życie w jak najszerszym zakresie prawa ochrony danych osobowych dziecka, którego te dane dotyczą. Mogą jednak zaistnieć sytuacje, w których najlepiej pojęty interes dziecka oraz jego prawo do prywatności wydają się konkurować. W takich przypadkach zasada najlepiej pojętego interesu dziecka może być nadrzędna wobec praw ochrony danych osobowych.

Ma to miejsce szczególnie w przypadku danych medycznych, gdy na przykład ośrodki pomocy dzieciom może zażądać stosownych informacji w przypadkach zaniedbania lub wykorzystania dziecka. Podobnie nauczyciel może ujawnić dane osobowe dziecka pracownikowi socjalnemu w celu zapewnienia dziecku ochrony, czy to fizycznej, czy to psychologicznej.

W skrajnych przypadkach zasada najlepiej pojętego interesu dziecka może również być sprzeczna z wymogiem wydania zgody przez jego prawnych przedstawicieli. Najlepiej pojęty interes dziecka również w tej sytuacji musi być nadrzędny, jeżeli na przykład zagrożona jest nienaruszalność fizyczna lub psychiczna dziecka.

## **6) – Dostosowanie do stopnia dojrzałości dziecka**

Ponieważ dziecko podlega stałemu rozwojowi, wykonywanie jego praw, włącznie z prawami dotyczącymi ochrony danych osobowych, musi być dostosowane do poziomu jego rozwoju fizycznego i psychicznego. Dzieci nie tylko podlegają procesowi rozwoju, ale mają do tego rozwoju prawo<sup>7</sup>. Sposoby uwzględniania tego procesu przez systemy prawne są różne w poszczególnych państwach, ale we wszystkich społeczeństwach dzieci muszą być traktowane odpowiednio do ich stopnia dojrzałości<sup>8</sup>.

Jeżeli chodzi o wyrażenie zgody, rozwiązania mogą postępować od zwykłej konsultacji z dzieckiem, przez równoległe wyrażenie zgody przez dziecko i przedstawiciela prawnego, nawet po wyłączną zgodę dziecka, jeżeli osiągnęło ono dojrzałość.

## **7) – Prawo do uczestnictwa**

Dzieci stopniowo pozyskują coraz większe możliwości udziału w podejmowaniu decyzji, które ich dotyczą. W miarę jak rosną, powinny coraz bardziej regularnie uczestniczyć w wykonywaniu swoich praw, w tym również praw związanych z ochroną danych osobowych<sup>9</sup>.

Podstawowym poziomem tego prawa jest prawo dziecka do wyrażenia opinii.

<sup>7</sup> Konwencja o prawach dziecka ONZ – art. 7, 27, 29.

<sup>8</sup> Niektóre systemy prawne realizują tę ogólną zasadę, rozróżniając następujące okresy w wieku dziecka: przed 12 rokiem życia, między 12 a 16 rokiem życia oraz od 16 do 18 roku życia.

<sup>9</sup> Konwencja o prawach dziecka ONZ (art. 12), Karta praw podstawowych Unii Europejskiej (art. 24 ust. 1), Konwencja w sprawie kontaktów z dziećmi (art. 6).

Obowiązek konsultacji z dzieckiem obejmuje uwzględnienie własnej opinii dziecka, chociaż niekoniecznie poddawanie się jej<sup>10</sup>.

Kiedy jednak dzieci osiągną zdolność do odpowiednich czynności, ich uczestnictwo można zwiększyć nawet do podejmowania wspólnej lub autonomicznej decyzji.

Prawo do uczestnictwa ma zastosowanie w różnych sprawach, takich jak geolokalizacja, wykorzystanie wizerunku dzieci i inne.

## **B – Ujęcie z perspektywy ochrony danych**

### **1) – Zakres istniejących ram prawnych dotyczących ochrony danych**

Stosowne dyrektywy dotyczące ochrony danych, tj. 95/46/WE i 2002/58/WE, nie wymieniają wyraźnie praw osób nieletnich do prywatności. Te akty prawne mają zastosowanie do wszystkich osób fizycznych, jednak nie istnieją szczególne przepisy dotyczące kwestii właściwych dla dzieci. Nie znaczy to jednak, że dzieci nie mają żadnego prawa do prywatności i że nie są objęte zakresem wymienionych dyrektyw. Zgodnie z brzmieniem samych dyrektyw mają one zastosowanie do wszystkich „osób fizycznych”, a zatem dotyczą również dzieci.

Z uwagi na ograniczony zakres podmiotowy i przedmiotowy dyrektywy, szereg pytań dotyczących ochrony prywatności dzieci w ramach dyrektywy pozostaje nadal otwartych. Ma to miejsce, ponieważ większość przepisów nie uwzględnia bezpośrednio szczególnych aspektów życia dzieci. Pojawiają się problemy dotyczące stopnia indywidualnej dojrzałości dziecka oraz wymogu przedstawicielstwa w związku z podejmowaniem czynności prawnych.

Potrzeba ochrony danych osobowych dzieci musi uwzględniać dwa istotne aspekty. Po pierwsze, zróżnicowany stopień dojrzałości, który decyduje o tym, kiedy dzieci mogą rozpocząć samodzielne dysponowanie własnymi danymi, a po drugie, zakres prawa przedstawicieli do reprezentowania nieletnich w sprawach, w których ujawnienie danych osobowych naruszałoby najlepiej pojęty interes dziecka. Poniżej przedstawiona została kwestia najlepszego zastosowania istniejących przepisów dyrektywy w celu zapewnienia odpowiedniej i skutecznej ochrony prywatności dzieci.

### **2) – Zasady dyrektywy 95/46/WE**

#### **a) Jakość danych**

Ogólne zasady dotyczące jakości danych przewidziane w dyrektywie 95/46/WE należy oczywiście odpowiednio dostosować w przypadku stosowania ich w odniesieniu do dzieci.

<sup>10</sup> Takie kryterium zostało wyraźnie określone w Rekomendacji Komitetu Ministrów Rady Europy dotyczącej ochrony danych medycznych – pkt 5.5 i 6.3 rekomendacji nr R(97)5 z dnia 13 lutego 1997 r., nr 5.5 oraz 6.3.

Oznacza to:

### **a.1) Rzetelność**

Jeżeli obowiązek przetwarzania danych osobowych zgodnie z zasadą rzetelności [art. 6 ust. 1 lit. a)] dotyczy dziecka, należy interpretować go w sposób ścisły. Administrator danych musi zdawać sobie sprawę z tego, że dziecko nie jest jeszcze w pełni dojrzałe, i działać w najlepszej wierze przy przetwarzaniu jego danych.

### **a.2) Proporcjonalność i stosowność danych**

Zasada określona w art. 6 ust. 1 lit. c) dyrektywy 95/46/WE stanowi, że gromadzić i przetwarzać można tylko prawidłowe, stosowne oraz nienadmierne ilościowo dane.

Przy stosowaniu zasad art. 6 ust. 1 lit. c) administratorzy danych powinni zwrócić szczególną uwagę na sytuację dziecka, ponieważ muszą cały czas przestrzegać zasady najlepszego zabezpieczenia jego interesów.

Zgodnie z art. 6 ust. 1 lit. d) dyrektywy 95/46/WE „dane muszą być prawidłowe oraz, w razie konieczności, aktualizowane. Należy podjąć wszelkie uzasadnione działania, aby zapewnić usunięcie lub poprawienie nieprawidłowych lub niekompletnych danych, biorąc pod uwagę cele, dla których zostały zgromadzone lub dla których są dalej przetwarzane”.

Ze względu na stały rozwój dzieci administratorzy danych muszą zwracać szczególną uwagę na obowiązek aktualizacji danych osobowych.

### **a.3) Zatrzymywanie danych**

W tym względzie należy pamiętać o prawie przedawnienia („*droit à l'oubli*”) obejmującym wszystkie osoby, których dotyczą dane, a w szczególności dzieci. Należy odpowiednio stosować art. 6 ust. 1 lit. e) dyrektywy.

Ponieważ dzieci podlegają stałemu rozwojowi, dotyczące ich dane również się zmieniają, dlatego mogą szybko stać się nieaktualne i niestosowne w związku z pierwotnym celem gromadzenia danych. W przypadku zaistnienia takiej sytuacji, danych nie należy dalej przechowywać.

### **b) Legalność**

Dyrektywa 95/46/WE określa podstawowe zasady ochrony danych, które muszą być przestrzegane i realizowane przez państwa członkowskie. W zakresie prawa dzieci do prywatności duże znaczenie mają art. 7 i 8, które określają kryteria legalności przetwarzania danych.



Przede wszystkim, przetwarzanie jest dozwolone, jeżeli dana osoba wyraziła na to jednoznaczną zgodę. Znaczenie słowa „zgoda” zostało wyjaśnione w art. 2 lit. h) dyrektywy.

Innymi słowy, zgoda musi być udzielona w oparciu o znajomość sytuacji i dobrowolna. Zgoda nie jest jednak obowiązkowa we wszystkich przypadkach. Przetwarzanie może również być legalne, jeżeli inne wymogi prawne zostały spełnione zgodnie z art. 7 lit. b) - f), na przykład przetwarzanie jest również dozwolone w przypadku podpisywania umowy.

W przypadkach, w których przedstawiciele prawni naruszają prywatność dzieci, sprzedając lub publikując ich dane, pojawia się pytanie, w jaki sposób można chronić prawo dzieci do prywatności, jeżeli one same nie są świadome przypadków naruszenia tego prawa. Dzieci potrzebują opiekuna prawnego, jednak w sytuacjach takich jak ta, nie mogą wykonywać swoich praw. Jeżeli dzieci są wystarczająco dojrzałe, aby wykryć naruszenie swojego prawa do prywatności, powinny mieć prawo do bycia wysłuchanymi przez właściwe organy, włącznie z organami ochrony danych.

Zasada najlepiej pojętego interesu dziecka oraz zasada przedstawicielstwa muszą być przestrzegane również w przypadku innych warunków określonych w art. 7 dyrektywy, które stanowią o legalności przetwarzania danych. Na przykład w pewnym wieku dzieci mogą zgodnie z prawem wchodzić w zobowiązania umowne, np. w dziedzinie zatrudnienia. Jeżeli wymaga tego prawo, takie umowy są jednak ważne pod warunkiem, że przedstawiciel prawny wyraził na nie zgodę. Przed zawarciem umowy lub w trakcie jej wykonywania osoba trzecia może chcieć gromadzić dane o dziecku jako pracowniku.

Przedstawiciele prawni ułatwiają przetwarzanie danych, wyrażając na to zgodę. Rodzice lub opiekunowie powinni podejmować decyzje, mając na względzie najlepsze zabezpieczenie interesów dziecka. Powinni uwzględniać sytuacje, w których ujawnienie danych może stanowić zagrożenie dla prywatności lub istotnych interesów ich dziecka, na przykład przez nieujawnianie danych medycznych. Istnieją inne dziedziny, w których nawet dzieci mogą podejmować decyzje niezależnie od swoich przedstawicieli prawnych.

W odniesieniu do warunku określonego w art. 7 lit. e) należy zwrócić uwagę na fakt, że zasada najlepiej pojętego interesu dziecka może być również zaklasyfikowana jako interes publiczny. Może to mieć miejsce w przypadku, w którym ośrodek pomocy dzieciom potrzebuje danych osobowych dziecka w celu zapewnienia mu opieki. Przepisy dyrektywy mogą zatem mieć bezpośrednie zastosowanie w takich okolicznościach.

Pojawia się jednak pytanie, czy dzieci, które w określonych przypadkach mogą podejmować czynności prawne bez zgody swoich przedstawicieli prawnych (w przypadkach, w których przysługują im prawa częściowe), mogą również udzielać wiążącej zgody na przetwarzanie własnych danych osobowych.

Zgodnie z obowiązującymi przepisami krajowymi może to mieć miejsce w przypadku małżeństwa, zatrudnienia, spraw religijnych itp. W innych przypadkach zgoda dziecka może być ważna pod warunkiem, że przedstawiciel prawny nie wyrazi sprzeciwu.

Oczywiste jest również, że należy uwzględnić poziom dojrzałości fizycznej i psychicznej dzieci, oraz że od momentu osiągnięcia pewnego wieku dzieci są zdolne do oceny spraw, które ich dotyczą. Może to być istotne w przypadkach, w których przedstawiciel prawny nie zgadza się z dzieckiem, ale dziecko jest wystarczająco dojrzałe, aby podejmować decyzje we własnym interesie, na przykład w kontekście medycznym lub seksualnym. Przypadki, w których najlepiej pojęty interes dziecka ogranicza zasadę przedstawicielstwa lub nawet nad nią przeważa, nie mogą być lekceważone i wymagają dalszego rozważenia.

Najszersza podstawa legalności odnosi się do uzasadnionych interesów administratora danych lub osoby trzeciej [art.7 lit. f)], z wyjątkiem przypadków, w których interesy te są uchylane przez interesy lub podstawowe prawa i wolności osoby, której dotyczą dane. Przy rozważaniu tych kwestii szczególną uwagę należy poświęcić statusowi dzieci jako osób, których dotyczą dane, i kierować się najlepiej pojętym interesem dzieci.

### **c) Bezpieczeństwo danych**

Zgodnie z art. 17 dyrektywy 95/46/WE „państwa członkowskie zapewniają, aby administrator danych wprowadził odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub dostępem” oraz:

„Uwzględniając stan wiedzy w tej dziedzinie oraz koszt realizacji, przyjęte zostaną takie środki, które zapewnią poziom bezpieczeństwa odpowiedni do zagrożeń wynikających z przetwarzania danych oraz charakteru danych objętych ochroną.”

Do danych osobowych dzieci należy podchodzić ze szczególną troską i uwagą. Należy dostosować środki bezpieczeństwa do sytuacji dzieci. Należy zauważyć, że dzieci mogą być mniej świadome zagrożeń, jakie mogą je spotkać, niż osoby dorosłe.

### **d) Prawa osób, których dotyczą dane**

#### **d.1) Prawo do informacji**

Należy podkreślić, że wymóg zgody określony w dyrektywie idzie w parze z obowiązkiem udzielania odpowiednich informacji osobom, których dotyczą dane (art. 10, 11, 14).

Grupa robocza miała już możliwość zajęcia się kwestią wymogów dotyczących udzielania informacji w kilku dokumentach; w szczególności należy uwzględnić Opinię w sprawie dalszej harmonizacji zasad informowania (dokument roboczy 100) i Rekomendację w sprawie określonych minimalnych wymogów w odniesieniu do gromadzenia danych osobowych online w UE (dokument roboczy 43), ponieważ przedstawiono w nich jasne wytyczne.

Jeżeli chodzi o zapewnianie informacji dzieciom lub ich przedstawicielom prawnym, szczególny nacisk należy położyć na to, aby te złożone informacje przekazywane były za pomocą prostego, zwięzłego i pouczającego języka, który będzie łatwy do zrozumienia. Krótsza informacja o prywatności powinna zawierać podstawowe informacje udzielane w przypadku gromadzenia danych bezpośrednio od osoby, której dotyczą dane, lub od osoby trzeciej (art. 10 i 11). Powinna temu towarzyszyć bardziej szczegółowa informacja dostarczana na przykład za pośrednictwem hiperłącza, która będzie zawierać wszystkie istotne szczegóły.

Informacje muszą być (zawsze) przedstawiane przedstawicielom prawnym oraz dzieciom po osiągnięciu przez nie zdolności do odpowiednich czynności.

Do informacji zamieszczanych online zastosowanie mają szczególne wymagania.

Jak stwierdziła grupa robocza w rekomendacji w sprawie przetwarzania danych online, zasadnicze znaczenie ma umieszczanie informacji o prywatności w odpowiednim miejscu i czasie, tj. powinny być one pokazywane bezpośrednio na ekranie przed zgromadzeniem informacji. Jest to zarówno wymóg określony w dyrektywie, jak i szczególnie ważne narzędzie zwiększania świadomości dzieci na temat możliwych zagrożeń i niebezpieczeństw wynikających z działań online. Można nawet uznać, że – w przeciwieństwie do świata rzeczywistego – w środowisku online działanie to stanowi jedyną możliwość poinformowania dzieci o takich zagrożeniach.

## **d.2) Prawo dostępu do danych**

Prawo dostępu jest zazwyczaj wykonywane przez przedstawiciela prawnego dziecka, jednak zawsze z uwzględnieniem dobra dziecka. W zależności od stopnia dojrzałości dziecka, prawo może być wykonywane w jego imieniu lub razem z nim. W niektórych przypadkach dziecko może być również uprawnione do samodzielnego wykonywania swoich praw.

Jeżeli sprawa dotyczy bardzo osobistych praw (na przykład w dziedzinie zdrowia), dzieci mogą nawet zwrócić się do lekarzy z prośbą o nieujawnianie danych medycznych ich przedstawicielom prawnym.

Może to mieć miejsce w przypadku, w którym osoby nastoletnie udziela lekarzowi lub operatorowi infolinii informacji dotyczących ich życia seksualnego, wyraźnie wyłączając przedstawicieli prawnych z dostępu do takich informacji.

Może to mieć miejsce również w przypadku, w którym dziecko nie ma zaufania do swoich przedstawicieli prawnych i skontaktuje się z ośrodkiem pomocy młodzieży, na przykład w związku z zażywaniem narkotyków lub myślami samobójczymi.

Pojawia się pytanie, czy przedstawiciele prawni mogą mieć dostęp do takich szczegółów i czy dziecko może się temu sprzeciwić. Przy dokonywaniu oceny, czy prawo dziecka do prywatności jest nadrzędne względem prawa przedstawiciela prawnego do dostępu do danych, należy ostrożnie wyważyć interesy wszystkich zainteresowanych stron. Przy dokonywaniu tego wyważenia szczególne znaczenie ma najlepsze zabezpieczenie interesów dziecka.

Jeżeli chodzi o dostęp do danych medycznych, dla dokonania oceny możliwości udostępnienia takich danych przedstawicielom prawnym istotna może okazać się opinia lekarza.

Również doświadczenia krajowe dostarczają użytecznych przykładów: na przykład w Zjednoczonym Królestwie osoby nastoletnie, które ukończyły 12 lat, mogą samodzielnie wykonywać prawo dostępu.

W kilku krajach prawo dostępu przedstawicieli prawnych do danych dotyczących ich nastoletnich córek jest ograniczone w przypadku aborcji.

Ogólnie rzecz ujmując, kryteria dotyczące warunków dostępu obejmują nie tylko wiek dziecka, ale również to, czy przedmiotowe dane zostały dostarczone przez rodziców, czy przez dziecko – co wskazuje również na stopień dojrzałości i samodzielności dziecka.

### **d.3) Prawo do poprawiania, usuwania i blokowania danych**

Prawo dostępu do danych jest ważne i znaczące samo w sobie.

Może jednak również stanowić sposób wykonania prawa do poprawiania, usuwania i blokowania- w odniesieniu do danych, które nie są prawidłowe lub aktualne.

Jeżeli chodzi o wykonywanie tych praw, należy uwzględnić podobne perspektywy, jak opisano powyżej, w odniesieniu do prawa dostępu.

### **d.4) Prawo sprzeciwu**

Artykuł 14 lit. a) stanowi, że osobie, której dane dotyczą, przyznaje się prawo sprzeciwu wobec przetwarzania danych – przynajmniej w przypadkach, o których mowa w art. 7 lit. e) i f) – z ważnych i uzasadnionych przyczyn. Te przyczyny są szczególnie ważne, jeżeli dotyczą dzieci. Należy również przypomnieć, że osoby, których dane dotyczą, mają w każdym razie prawo sprzeciwu wobec przetwarzania ich danych dla potrzeb bezpośredniego obrotu [art. 14 lit. b)].

#### **e) Zawiadomienie**

Ponadto konieczne jest odniesienie się do obowiązku zawiadamiania o przetwarzaniu danych w przypadkach określonych przez prawo.

## **III – W szkole**

W poniższym rozdziale niniejszej opinii zilustrowano sposób, w jaki przypomniane powyżej podstawowe zasady mogą być uszczegółowione w odniesieniu do kontekstu szkolnego. Dziecko w rzeczywistości rozwija się zarówno w szkole, jak i w rodzinie, dlatego naturalne jest pojawienie się różnych pytań związanych z ochroną danych

osobowych w związku ze szkolnym życiem dzieci. Te pytania mają różny charakter i podejmują równie odmienne problemy.

## **1) – Akta ucznia**

### **a) Informacje**

Pytania dotyczące ochrony danych osobowych związane z dziećmi (oraz w niektórych przypadkach z ich rodzinami) mogą się pojawić w związku z aktami uczniów już przy zapisywaniu ich do szkoły. W niektórych krajach prawo zezwala władzom szkoły na wymaganie formularzy zawierających dane osobowe, wypełnianych w celu utworzenia aktu ucznia w formie elektronicznej lub innej.

W przypadku takich formularzy osoby, których dane dotyczą, powinny zostać poinformowane o fakcie gromadzenia i przetwarzania ich danych osobowych, o celu tych działań, o tym kim są administratorzy danych oraz o możliwym sposobie wykonania praw dostępu i poprawek. W stosownych przypadkach osoby te należy również poinformować o tym, komu te dane mogą zostać ujawnione.

### **b) Ograniczenie celu i proporcjonalność**

Dane osobowe mogą być włączane do akt uczniów wyłącznie, jeżeli jest to konieczne dla legalnych celów realizowanych przez szkoły i nie powinny one być wykorzystywane w sposób niezgodny z tymi celami [art. 6 ust. 1 lit. b) dyrektywy].

Wymagane dane nie mogą być nadmierne ilościowo, np. nie zawsze niezbędne są dane o stopniach akademickich rodziców, ich zawodach lub sytuacji na rynku pracy. Administratorzy danych muszą zdecydować, czy są one rzeczywiście potrzebne.

### **c) Niedyskryminacja**

Niektóre dane zamieszczone w tych formularzach mogą przyczynić się do dyskryminacji, na przykład dane dotyczące rasy, statusu imigranta lub niektórych niepełnosprawności.

Informacje te są zazwyczaj gromadzone w celu zagwarantowania, że szkoła będzie wiedziała o uczniach zmagających się z trudnościami kulturowymi (na przykład językowymi) lub ekonomicznymi i poświęci im należyłą uwagę.

Kryteriami przy przetwarzaniu takich informacji powinny być zasady najlepiej pojętego interesu i ścisłego ograniczenia celu.

Przed wszystkim należy zastosować bardzo surowe podejście, jeśli chodzi o rejestrację wyznania uczniów; taką rejestrację można dopuścić wyłącznie, jeżeli uzasadniają to charakter szkoły (szkoła religijna) i cele administracyjne oraz wyłącznie w ścisłym niezbędnym zakresie. Z danych dotyczących wyznania ucznia nie należy wyciągać zbędnych wniosków, jeżeli dane te są potrzebne wyłącznie do celów administracyjnych (np. w następstwie kursu dotyczącego religii lub w celu wskazania preferencji żywieniowych).

Informacje o majątku i dochodach rodziny dziecka również mogą być źródłem dyskryminacji, jednak można je też przetwarzać we własnym interesie dziecka, na przykład jeżeli jego przedstawiciele zwrócą się z prośbą o stypendium lub zmniejszenie czesnego za szkołę.

Wszystkie dane, które mogą prowadzić do dyskryminacji, należy chronić za pomocą odpowiednich środków bezpieczeństwa, takich jak przetwarzanie danych w oddzielnych plikach, przez wykwalifikowane i wyznaczone do tego celu osoby podlegające obowiązkowi zachowania tajemnicy zawodowej oraz innych odpowiednich środków.

Wyrażenie zgody na przetwarzanie danych, które mogą przyczynić się do dyskryminacji, musi być wyraźne i jednoznaczne.

#### **d) Zasada celowości**

##### **d.1) Przekazywanie danych**

Istnieją przypadki, w których władze szkolne udostępniają osobom trzecim nazwiska i adresy swoich uczniów, często do celów marketingowych.

Ma to miejsce na przykład, jeżeli dane są wysyłane do banków lub zakładów ubezpieczeń, które chcą przyciągnąć uczniów jako klientów, lub jeżeli dane uczniów są przekazywane przedstawicielom samorządu lokalnego. Stanowi to naruszenie zasady celowości, ponieważ dane przeznaczone do celów szkolnych zostają wykorzystane niezgodnie z tym przeznaczeniem.

Zgodnie z art. 6 ust. 1 lit b) dyrektywy 95/46WE dane osobowe dotyczące dzieci nie mogą być wykorzystywane w celach niezgodnych z celem, który był powodem gromadzenia tych danych.

Trudności nie stanowi tutaj problem dzieci jako odbiorców działań marketingowych, ale problem ochrony konsumenta. Chodzi tu o wcześniejsze gromadzenie danych osobowych w celu późniejszego wysyłania osobom, których dane dotyczą, informacji marketingowych. Na tego rodzaju przetwarzanie danych muszą wcześniej wyrazić zgodę przedstawiciele (oraz dzieci, w zależności od stopnia ich dojrzałości).

W każdym przypadku, w którym działania marketingowe zostały uznane za uzasadnione i zgodne, przetwarzanie danych należy wykonywać w sposób jak najmniej inwazyjny.

Oprócz warunków wymienionych powyżej, jeżeli osoba trzecia zwraca się o udostępnienie danych rodziców lub uczniów do celów marketingowych, przedstawiciel prawny (oraz dzieci, w zależności od stopnia ich dojrzałości) zawsze musi zostać o tym wcześniej poinformowany oraz wyrazić na to swoją zgodę.

##### **d.2) Dostęp do danych**

Dane zawarte w aktach ucznia muszą podlegać ścisłej poufności zgodnie z ogólną zasadą określoną w art. 16 dyrektywy 95/46/WE.

Przetwarzanie danych o szczególnym charakterze powinno podlegać szczególnym wymogom bezpieczeństwa.

Przykładowe dane tego rodzaju są następujące:

- postępowania dyscyplinarne,
- rejestrowanie przypadków przemocy,
- leczenie w szkole,
- orientacja szkolna,
- kształcenie specjalne dla osób niepełnosprawnych,
- pomoc społeczna dla dzieci z ubogich rodzin.

Dostępu do danych należy udzielić przedstawicielom prawnym uczniów (oraz samym uczniom, jeżeli uzyskali już dojrzałość). Dostęp taki należy ściśle regulować i ograniczyć do władz szkolnych, inspektorów szkolnych, personelu medycznego, pracowników socjalnych i organów ścigania.

### **d.3) Wyniki w nauce**

W różnych krajach istnieją odmienne tradycje w odniesieniu do publikacji wyników w nauce.

Istnieją kraje z od dawna ugruntowaną tradycją publikowania wyników.

Celem tego systemu jest umożliwienie porównania wyników oraz ułatwienie składania możliwych skarg lub odwołań. W tych krajach szkoły powinny ściśle stosować się do przepisów prawa krajowego i publikować jedynie minimalną ilość danych osobowych niezbędnych w tym celu.

W krajach, w których wyniki w nauce podlegają zasadzie poufności, można je ujawnić przedstawicielom prawnym i uczniom, w ramach wykonania ich prawa dostępu.

Publikacja wyników jest zależna od zgody tych przedstawicieli (lub również od zgody uczniów, stosownie do ich zdolności do odpowiednich czynności).

Szczególny problem dotyczy publikacji wyników w nauce w Internecie, co stanowi wygodny sposób przekazywania ich zainteresowanym osobom. Ryzyko nierozzerwalnie związane z tym sposobem komunikacji wymaga, aby dostęp do danych był możliwy wyłącznie z zachowaniem szczególnych środków zabezpieczających. Można to osiągnąć za pomocą zabezpieczonej strony internetowej lub osobistych haseł nadawanych przedstawicielom prawnym lub dzieciom, jeżeli osiągnęły już dojrzałość.

Warunki wykonania prawa dostępu będą się różnić w zależności od stopnia dojrzałości dziecka. Najprawdopodobniej w szkołach podstawowych dostęp będzie umożliwiony głównie przedstawicielom prawnym, natomiast w szkołach średnich uczniowie będą mieli również możliwość samodzielnego dostępu do danych.

#### **d.4) Zatrzymywanie i usuwanie**

Również w tym kontekście ma zastosowanie ogólna zasada, zgodnie z którą żadnych danych nie wolno przechowywać dłużej niż jest to konieczne dla celów, dla których zostały one zgromadzone. Należy zatem uważnie ustalić, które dane z akt szkolnych powinny być przechowywane ze względów edukacyjnych lub zawodowych oraz które dane należy usunąć – na przykład dane dotyczące postępowań dyscyplinarnych i sankcji.

### **2) – Życie szkolne**

Pytania o ochronę danych pojawiają się w niektórych dziedzinach codziennego życia szkolnego.

Istnieją środki kontroli nad społecznością szkolną, w szczególności nad uczniami, które mogą w wyjątkowo inwazyjny sposób naruszać prywatność innych.

Dotyczy to szczególnie gromadzenia danych biometrycznych, telewizji przemysłowej i identyfikacji radiowej.

Przyjęcie takich środków kontroli powinno być zawsze poprzedzone gruntowną dyskusją nauczycieli i rodziców (lub innych przedstawicieli uczniów), z uwzględnieniem określonych celów i stosowności proponowanych środków.

#### **a) Dane biometryczne – dostęp do szkoły i stołówki**

Z biegiem lat zwiększano w szkołach kontrolę dostępu. Kontrola dostępu może polegać na gromadzeniu przy wejściu danych biometrycznych, takich jak odciski palców, obraz tęczówki oka lub geometria dłoni. W niektórych przypadkach środki te są niewspółmierne do celu, co skutkuje nadmierną inwazyjnością nadzoru.

W każdym przypadku przy podejmowaniu takich środków kontroli biometrycznej należy stosować zasadę proporcjonalności.

Gorąco zaleca się, aby przedstawiciele prawni mieli do dyspozycji proste środki sprzeciwu wobec wykorzystania danych biometrycznych ich dzieci. Jeżeli skorzystają z przysługującego im prawa sprzeciwu, ich dzieci powinny otrzymać kartę lub inne środki umożliwiające wstęp do danego obiektu szkolnego.

#### **b) Telewizja przemysłowa**

Obserwuje się coraz częstsze stosowanie systemów telewizji przemysłowej w szkołach dla celów bezpieczeństwa. Nie istnieje jedno zalecane rozwiązanie obowiązujące w odniesieniu do wszystkich aspektów życia szkolnego i wszystkich części szkół.

Ze względu na możliwość naruszenia swobód osobistych przez telewizję przemysłową jej instalowanie w szkołach wymaga szczególnej uwagi. Oznacza to, że systemy telewizji przemysłowej należy instalować tylko w razie konieczności lub jeżeli w tym samym celu nie jest możliwe zastosowanie innych, mniej inwazyjnych środków.



Istnieją miejsca, w których bezpieczeństwo jest sprawą najwyższej wagi, co uzasadnia zastosowanie telewizji przemysłowej, np. wejścia do szkoły i wyjścia ze szkoły oraz inne miejsca, w których przemieszczają się ludzie – nie tylko ci, którzy należą do społeczności szkolnej, ale także ci, którzy z jakichś powodów odwiedzają obiekty szkolne.

Rozmieszczenie kamer telewizji przemysłowej powinno być zawsze stosowne, odpowiednie i nienadmierne w stosunku do celu przetwarzania. Na przykład w niektórych krajach uznano stosowanie kamer telewizji przemysłowej po godzinach zajęć szkolnych za odpowiednie w odniesieniu do zasad ochrony danych.

Z drugiej strony, w większości pozostałych części szkoły prawo uczniów (a także nauczycieli i innych pracowników szkoły) do prywatności oraz podstawowa wolność nauczania stanowią wartości nadrzędne wobec potrzeby stałego nadzoru przy pomocy kamer telewizji przemysłowej.

Sytuacja taka ma miejsce szczególnie w salach lekcyjnych, w których nadzór kamerami wideo może stanowić ingerencję nie tylko w wolność uczenia się i wypowiedzi uczniów, ale także w wolność nauczania. To samo dotyczy miejsc, w których uczniowie spędzają czas wolny, a także sal gimnastycznych i szatni, gdzie nadzór może naruszać prawo do prywatności.

Powyższe uwagi opierają się także na prawie do rozwoju osobowości, które posiada każde dziecko. Rozwijające się w nich poczucie własnej wolności może zostać upośledzone, jeżeli już w młodym wieku założą, że podleganie nadzorowi kamer telewizji przemysłowej jest normalne. Jest to tym bardziej prawdziwe, jeżeli w czasie zajęć szkolnych stosuje się metody monitorowania dzieci na odległość, np. za pośrednictwem kamer internetowych i podobnych urządzeń.

W każdym przypadku, w którym zastosowanie telewizji przemysłowej jest uzasadnione, należy poinformować dzieci, pozostałą część społeczności szkolnej oraz przedstawicieli prawnych o istnieniu nadzoru, tożsamości administratora i celach nadzoru. Informacje przekazywane dzieciom powinny być dostosowane do ich poziomu rozumienia.

Nie wolno ponadto zapominać, że należy uwzględnić nie tylko interesy uczniów, lecz także nauczycieli i innych pracowników szkoły. W niektórych krajach istnieją nawet przepisy prawne regulujące stosowanie telewizji przemysłowej w celu kontrolowania pracowników.<sup>(1)</sup>

Władze szkoły powinny regularnie przeprowadzać analizę uzasadnienia i stosowności systemu telewizji przemysłowej i na tej podstawie podejmować decyzję o utrzymaniu lub zaprzestaniu jego stosowania. O podjętych decyzjach należy informować przedstawicieli prawnych dzieci.

---

(1) Zob. także dokument roboczy 89 (Opinia 4/2004 z dnia 11 lutego 2004 r.).

### **c) Stan zdrowia**

Dane dotyczące stanu zdrowia uczniów stanowią dane szczególnie chronione. Dlatego ich przetwarzanie musi się odbywać w ścisłej zgodności z zasadami zawartymi w art. 8 dyrektywy. Dane takie powinni przetwarzać wyłącznie lekarze lub osoby bezpośrednio „opiekujące się” uczniami, takie jak nauczyciele lub inni pracownicy szkoły zobowiązani do przestrzegania zasad etyki w zakresie tajemnicy służbowej.

Możliwość przetwarzania tego typu danych zależy od zgody przedstawicieli prawnych dzieci lub istotnych interesów związanych z życiem szkolnym lub edukacją.

### **d) Strony internetowe szkół**

Coraz więcej szkół tworzy strony internetowe przeznaczone dla uczniów i ich rodzin, które stają się głównym narzędziem komunikacji zewnętrznej. Szkoły powinny mieć świadomość, że rozpowszechnianie danych osobowych pociąga za sobą konieczność bardziej rygorystycznego przestrzegania podstawowych zasad ochrony danych, w szczególności zasady ograniczenia i proporcjonalności danych. Ponadto zaleca się wprowadzenie mechanizmów ograniczonego dostępu w celu zabezpieczenia przedmiotowych danych osobowych (np. logowanie przy pomocy nazwy użytkownika i hasła).

### **e) Zdjęcia dzieci**

Szkoły często ulegają pokusie publikowania zdjęć swoich uczniów (w prasie lub Internecie). Przy umieszczaniu zdjęć uczniów w Internecie należy zachować szczególną uwagę. Konieczne jest każdorazowe dokonanie oceny rodzaju zdjęcia, a także stosowności i celu jego publikacji. Należy także powiadomić dzieci i ich przedstawicieli prawnych o takiej publikacji.

Jeżeli szkoła zamierza opublikować indywidualne zdjęcia poszczególnych uczniów, musi uprzednio uzyskać na to zgodę rodziców lub innych przedstawicieli prawnych (lub dziecka, jeżeli osiągnęło już dojrzałość).

W przypadku zdjęć zbiorowych, takich jak fotografie z wydarzeń szkolnych, szkoła nie musi zwracać się o uprzednią zgodę rodziców, jeżeli zdjęcia nie umożliwiają łatwej identyfikacji uczniów, przy czym powinno się to zawsze odbywać zgodnie z prawodawstwem krajowym. Niemniej jednak w takich przypadkach szkoły muszą poinformować dzieci, rodziców i przedstawicieli prawnych o zamiarze robienia zdjęć i sposobie ich późniejszego wykorzystania.

Dzięki temu mają oni możliwość odmowy wystąpienia na zdjęciu.

### **f) Karty uczniów**

Jeśli chodzi o kontrolę dostępu i monitorowanie zakupów, wiele szkół stosuje karty uczniów nie tylko w celu kontroli dostępu wstępu do szkoły, ale także monitorowania

zakupów dokonywanych przez dzieci. Kwestią sporną jest, czy to ostatnie przeznaczenie kart jest w pełni zgodne z prywatnością dziecka, zwłaszcza dziecka, które osiągnęło pewien wiek.

W każdym razie należy oddzielić te dwie funkcje kart, ponieważ druga z nich może powodować problemy związane z prywatnością.

Jeśli chodzi o lokalizację uczniów<sup>11</sup>, innym środkiem kontroli stosowanym w niektórych szkołach (korzystających lub niekorzystających z kart) jest lokalizacja uczniów przy pomocy plakietek identyfikacji radiowej. W takim przypadku należy uzasadnić zastosowanie takiego systemu w odniesieniu do szczególnych rodzajów ryzyka, o które chodzi, zwłaszcza jeżeli dostępne są alternatywne metody kontroli.

### **g) Wideofony w szkołach**

Szkoły mogą odgrywać kluczową rolę w określaniu środków ostrożności w odniesieniu do korzystania z wiadomości MMS, nagrań audio i wideo, w których wykorzystuje się dane osobowe osób trzecich bez wiedzy osób, których dane dotyczą. Szkoły powinny ostrzegać swoich uczniów, że nieograniczony obieg nagrań wideo, audio i zdjęć cyfrowych może skutkować poważnymi naruszeniami prawa do prywatności i ochrony danych osobowych osób, których dotyczą te dane.

### **3) – Szkolne statystyki i inne badania**

W większości przypadków do uzyskania danych statystycznych nie są potrzebne dane osobowe (może się to jednak zdarzyć w pewnych wyjątkowych przypadkach, np. przy prowadzeniu badań statystycznych nad integracją zawodową).

Zgodnie z art. 6 ust 1. lit. e) dyrektywy, wyniki badań statystycznych nie powinny umożliwiać bezpośredniej ani pośredniej identyfikacji osób, których dane dotyczą.

Często prowadzone są badania, w których wykorzystuje się różne dane o uczniach uzyskane dzięki mniej lub bardziej szczegółowym ankietom. Gromadzenie takich danych powinno odbywać się za zgodą przedstawicieli prawnych (zwłaszcza, gdy chodzi o dane szczególnie chronione), którzy powinni zostać poinformowani o celu i odbiorcach badania.

Ponadto, jeżeli możliwe jest przeprowadzanie badań bez identyfikacji dzieci, należy stosować taką procedurę.

---

<sup>11</sup> Zob. dokument roboczy 115 (przyjęty dnia 25 listopada 2005 r.) dotyczący zasad lokalizacji nieletnich.

## **IV – Podsumowanie**

### **1) – Prawo**

Niniejsza opinia wskazuje, że przepisy ustanowione w obecnych ramach prawnych w większości przypadków zapewniają skuteczną ochronę danych dotyczących dzieci.

Wstępnym warunkiem skutecznej ochrony prywatności dzieci jest jednak stosowanie tych przepisów z uwzględnieniem zasady najlepiej pojętego interesu dziecka. Przy ich stosowaniu należy uwzględnić szczególną sytuację nieletnich i ich przedstawicieli. Należy zatem odpowiednio interpretować i stosować przepisy dyrektyw 95/46/WE i 2002/58/WE.

W przypadku konfliktu interesów możliwe jest dążenie do jego rozwiązania przez interpretowanie dyrektyw zgodnie z ogólnymi zasadami Konwencji o prawach dziecka ONZ, a mianowicie z najlepiej pojętym interesem dziecka, oraz przez odwołanie się do innych wspomnianych wyżej aktów prawnych.

Zachęca się państwa członkowskie do podjęcia niezbędnych środków w celu doprowadzenia ich prawa do zgodności ze wspomnianą wyższą interpretacją. Pożądane byłoby również wprowadzenie zaleceń lub innych odpowiednich rozwiązań dotyczących tej kwestii na szczeblu wspólnotowym.

Jak już wcześniej wspomniano, niniejsza opinia zawiera jedynie ogólne zasady ochrony prywatności i danych – odpowiednie w stosunku do danych dotyczących dzieci, a także ich informacje dotyczące ich zastosowania w tak ważnej dziedzinie, jaką jest edukacja. Inne szczególne obszary mogą stać się przedmiotem osobnego badania tej grupy roboczej w przyszłości.

### **2) – Praktyka**

Niniejsza opinia przedstawia ogólne obawy i rozważania powstałe w związku z analizą kwestii ochrony danych i prywatności w odniesieniu do dzieci. Grupa robocza wybrała dziedzinę edukacji jako pierwszy krok w stronę rozwiązania tej kwestii ze względu na istotną rolę edukacji w społeczeństwie. Jak można zauważyć, podejście do ochrony prywatności dzieci opiera się na edukacji – prowadzonej przez rodziny, szkoły, organy ochrony danych, grupy dla dzieci i inne – na temat znaczenia ochrony danych i prywatności oraz konsekwencji ujawniania danych osobowych bez konieczności.

Jeśli nasze społeczeństwa chcą dążyć do rozwinięcia prawdziwej kultury ochrony danych w szczególności i obrony prywatności w ogóle, należy zacząć od dzieci, nie tylko jako grupy wymagającej ochrony lub podmiotów prawa do ochrony, lecz także ze względu na potrzebę uświadomienia im ich obowiązków w zakresie poszanowania danych osobowych innych osób.

Szkoła powinna odgrywać kluczową rolę w dążeniu do realizacji tego celu.

Dzieci i uczniowie powinni być wychowywani na przyszłych samodzielnych obywateli społeczeństwa informacyjnego. Dlatego też istotne jest, aby od najmłodszych lat uczyli się o tym, jak ważna jest ochrona prywatności i danych. Pozwoli im to na podejmowanie w przyszłości świadomych decyzji w odniesieniu do tego, jakie informacje chcą ujawnić, komu i na jakich warunkach. Ochrona danych powinna być systematycznie włączana do planów zajęć w szkołach, stosownie do wieku uczniów i charakteru nauczanych przedmiotów.

Nigdy nie powinna mieć miejsca sytuacja, w której ze względów bezpieczeństwa dzieci stają się przedmiotem nadmiernego nadzoru ograniczającego ich niezależność. W związku z tym należy znaleźć równowagę między ochroną intymności i prywatności dzieci a ich bezpieczeństwem.

Prawodawcy, przywódcy polityczni i organizacje edukacyjne powinny – w ramach swoich odpowiednich kompetencji – podjąć skuteczne środki w celu podjęcia tych kwestii.

Jak już wielokrotnie wspomniano w niniejszym dokumencie, edukacja i odpowiedzialność są głównymi narzędziami ochrony danych dotyczących dzieci. Zasadnicze znaczenie dla skuteczniejszej ochrony danych osobowych nieletnich ma to, aby osoby bezpośrednio zajmujące się edukacją dzieci przeszły uprzednio kompleksowe szkolenia w zakresie zasad ochrony danych.

Rola organów ochrony danych zawiera się w czterech następujących zadaniach: edukowanie i informowanie, zwłaszcza dzieci i organów odpowiedzialnych za dobro młodzieży; wpływanie na decydentów politycznych, tak aby podejmowali oni właściwe decyzje dotyczące dzieci i prywatności; uświadamianie administratorom danych ciążących na nich obowiązków; oraz korzystanie z ich uprawnień w działaniach skierowanych przeciw osobom, które nie uwzględniają prawodawstwa albo nie przestrzegają kodeksów postępowania lub najlepszych praktyk istniejących w tym obszarze

Skuteczną strategią w tym kontekście może być stworzenie porozumień między organami ochrony danych, ministrami edukacji oraz innymi odpowiedzialnymi organami, które określałyby jasne i praktyczne warunki wzajemnej współpracy w tej dziedzinie w celu rozwoju świadomości, że ochrona danych jest prawem podstawowym.

Należy w szczególności uświadomić dzieciom, że to właśnie one powinny w pierwszej kolejności stać na straży własnych danych osobowych. Zgodnie z tym kryterium należy stopniowo zwiększać udział dzieci w ochronie ich danych osobowych (od konsultacji do decyzji). Jest to dziedzina, w której można wykazać skuteczność upodmiotowienia.

Sporządzono w Brukseli dnia 11  
lutego 2009 r.

*W imieniu Grupy Roboczej  
Przewodniczący  
Alex TÜRK*