Prywatność dziecka w cyberprzestrzeni – prawa i obowiązki

Maciej Groń

Pierwsze spotkanie rodziców w przedszkolu lub w szkole. Nauczyciel wręcza Ci do podpisania plik dokumentów często zwany „no bo RODO", który dotyczy zgody na wykorzystanie wizerunku i innych danych osobowych dziecka: w mediach społecznościowych, na oficjalnej stronie placówki lub podczas ciekawego projektu edukacyjnego itp. Większość rodziców automatycznie wyraża na nie zgodę, ponieważ chce, by ich dzieci dobrze się integrowały z nową grupą, a także by miały pamiątki z wycieczek, balów i przedstawień. Ty masz wątpliwości, czy to jest rozważne i nie masz pewności, do czego dane osobowe Twojego dziecka będą wykorzystane. Na co w takiej sytuacji zwrócić uwagę? Kiedy zgoda nie jest wymagana i na czym polega ochrona danych osobowych?

Zdjęcia dzieci z przedszkola i szkoły to wspaniała pamiątka i trudno się dziwić, że prawie każdy rodzic chce, by debiuty ich pociech w teatrzyku czy pierwsze samodzielne wycieczki były solidnie udokumentowane. Jednak to, co w XX wieku było utrwalane na papierze i przechowywane w rodzinnym albumie, a czasami w gazetkach ściennych szkoły lub przedszkola, dzisiaj jest umieszczane w internecie, najczęściej w mediach społecznościowych szkoły, zaraz później na profilach rodziców, uczniów, aż w końcu wymyka się spod kontroli. Bardzo często zdjęcia i filmy przekazywane są za pomocą komunikatorów internetowych – niestety nadzór nad ich swobodnym rozsyłaniem wśród dalszych znajomych nie jest możliwy.

W związku z tym, zanim rodzice lub opiekunowie wyrażą zgodę na przetwarzanie danych osobowych swoich dzieci (w tym także ich wizerunku), powinni podjąć co najmniej **kilka podstawowych kroków**:

1. Zrozumieć, jakie dane są zbierane i w jakim celu

a. **Dokładnie przeczytać politykę prywatności:** poświęcić czas na zapoznanie się z dokumentem, w którym opisano, jakie dane są zbierane, w jaki sposób mogą być wykorzystywane i komu udostępniane.

b. **Zwrócić uwagę na rodzaj danych:** sprawdzić, czy są to tylko podstawowe dane identyfikacyjne (imię, nazwisko, wiek), czy też bardziej wrażliwe informacje, takie jak adres zamieszkania, numer PESEL, dane dotyczące zdrowia czy preferencji.

c. **Zrozumieć cel przetwarzania danych:** czy dane są zbierane w celu świadczenia usług, personalizacji treści, marketingu, czy też w innych celach.

2. Ocenić, czy przetwarzanie danych jest konieczne i proporcjonalne

a. **Zastanowić się, czy cel przetwarzania danych jest uzasadniony:** czy usługa lub aplikacja, z której dziecko korzysta, rzeczywiście potrzebuje tych danych, aby działać poprawnie (nie zawsze jest to konieczne).

b. **Sprawdzić, czy nie ma alternatywnego rozwiązania:** często istnieją inne aplikacje lub usługi, które nie wymagają podawania tak wielu danych osobowych.

3. Pamiętać o prawach dotyczących ochrony danych osobowych, które przysługują zarówno dziecku, jak i rodzicowi w jego imieniu

a. **Prawo dostępu do swoich danych:** należy wiedzieć, w jaki sposób można je sprawdzić oraz jakie dane na temat dziecka są przetwarzane.

b. **Prawo do sprostowania danych:** jeśli dane są nieprawidłowe lub niekompletne, dziecko (lub rodzic w jego imieniu) ma prawo do ich poprawienia.

c. **Prawo do bycia zapomnianym:** w niektórych sytuacjach można zażądać usunięcia danych osobowych dziecka (lub swoich).

d. **Prawo do wycofania zgody w dowolnym momencie:** rodzice mają prawo zmienić zdanie i jeśli w przyszłości uznają, że przetwarzanie danych dziecka jest niekorzystne, mogą wycofać swoją zgodę.

4. Pamiętać o długotrwałych konsekwencjach udostępnienia danych

a. **W internecie nic nie ginie:** niewłaściwe wykorzystanie danych dziecka może mieć skutki wykraczające poza okres dzieciństwa, m.in. wpłynąć na jego przyszłe możliwości edukacyjne, zawodowe czy finansowe. Zdjęcie dziecka w kompromitującej sytuacji (np. w niecodziennym stroju, mówiącego kontrowersyjne teksty) może zostać udostępnione w internecie i stać się obiektem drwin i szykanowania, nawet po wielu latach, np. kiedy już jako osoba dorosła zechce zajmować stanowisko wymagające wyższych standardów zaufania, np. radnego, sędziego, nauczyciela, dziennikarza itp.

b. **Zagrożenia prywatności i bezpieczeństwa:** dane dzieci mogą być wykorzystywane przez osoby niepowołane do nieetycznych celów, takich jak cyberprzemoc, kradzież tożsamości, oszustwa, grooming (nawiązywanie relacji w celu wykorzystania dziecka) czy stalking (śledzenie, naprzykrzanie się).

c. **Podatność na manipulację:** dzieci mogą łatwiej ulec wpływowi reklam, fałszywych informacji czy technik marketingowych wykorzystujących ich dane do profilowania i personalizacji treści.

By rozwiać wątpliwości poniżej bardziej szczegółowo przedstawiamy podstawowe prawa dzieci i obowiązki ich opiekunów związane z dbaniem o ochronę prywatności swoich i innych dzieci. Tłumaczymy także podstawowe pojęcia i odczarowujemy magię RODO – Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych).

Ochrona prywatności – podstawowe pojęcia prawne

Pojęcie ochrony danych osobowych i RODO pojawia się bardzo często, zarówno w oficjalnych sprawach związanych ze szkołą, zdrowiem czy pracą, jak i w internecie, w szczególności podczas instalowania nowych aplikacji czy programów na telefonie lub komputerze. Niektóre pojęcia używane w formularzach RODO mają prawne znaczenie trochę inne od tego znanego z naszego codziennego języka, dlatego wyjaśniamy najważniejsze z nich.

Dane osobowe (art. 4 pkt 1 RODO) oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

W praktyce oznacza to, że do danych osobowych należy zaliczyć każdą informację umożliwiającą identyfikację człowieka oraz że dużo zależy od kontekstów, w jakich te informacje są umieszczone. Dane osobowe to oczywiście imię i nazwisko, ale w pewnych sytuacjach i zbiorach danych także cecha lub rzecz wyróżniająca

człowieka, np. charakterystyczny wzrost, kolor włosów lub nawet element ubioru taki jak muszka, kapelusz, okulary itp.

Przetwarzanie (art. 4 pkt 2 RODO) oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Definicja ta jest często mylona z „profilowaniem" (opisanym niżej). Trzeba pamiętać, że ustawowe znaczenie słowa „przetwarzanie" jest znacznie szersze niż powszechne rozumienie wyrazu „przetwarzać", którego synonimem najczęściej jest „wytwarzać", „zmieniać", „przerabiać", ale prawie nigdy „przechowywać", czy „porządkować". Z tego powodu należy zwrócić uwagę, że przetwarzanie danych osobowych zgodnie z RODO zaczyna się już od ich pobierania i przechowywania, a częste zapewnienie „mam Twoje dane, ale nie będę ich przetwarzać" jest praktycznie niemożliwe do spełnienia.

Profilowanie (art. 4 pkt 4 RODO) danych osobowych stanowi szczególną kategorię ich zautomatyzowanego przetwarzania, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Z profilowaniem możemy mieć do czynienia np. w projekcie dotyczącym personalizacji treści edukacyjnych, w którym platformy e-learningowe analizują wyniki testów, czas trwania nauki lub wybory dzieci, aby dostosować poziom materiałów lub proponować określone obszary do nauki albo kwalifikować dzieci do odpowiedniej placówki edukacyjnej lub klasy. Z tego powodu należy zachować bardzo dużą ostrożność wyrażając zgodę na profilowanie.

Wizerunek człowieka jest pojęciem często używanym w kontekście ochrony prywatności i może być traktowany także jako dane osobowe. Podlega on ochronie prawnej na podstawie **art. 23 i 24 Kodeksu cywilnego** (Dz. U. z 2024 r., poz. 1061) jako dobro osobiste człowieka, a **art. 81 Ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych** (Dz. U. z 2025 r. poz. 24) warunkuje rozpowszechnianie wizerunku uzyskaniem na to zezwolenia osoby na nim przedstawionej. W polskich przepisach prawa nie ma definicji wizerunku**,** ale na podstawie dorobku doktryny i orzecznictwa przyjmuje się, że jest to **konkretyzacja obrazu fizycznego**, tzn.

rozpoznawalna podobizna człowieka, na którą składają się cechy fizyczne (naturalne oraz sztuczne, np. strój), utrwalona na zdjęciu, portrecie, emisji „na żywo" przekazu internetowego lub telewizyjnego, a także w postaci nagrania.

Zgoda na przetwarzanie danych osobowych dziecka

Zgoda jest najczęstszym warunkiem przetwarzania danych osobowych. Poza wyjątkami opisanymi poniżej (wymienionymi w art. 6 ust. 1 lit. b-f RODO) **bez zgody rodziców lub opiekunów ani ich dane osobowe, ani dane dzieci nie mają prawa być przetwarzane** – tzn. nie powinny być nawet zbierane. Naruszenie tej zasady skutkuje odpowiedzialnością prawną i narażeniem się na wysokie kary.

Wyrażając zgodę na przetwarzanie danych osobowych należy zachować szczególną ostrożność i dokładnie sprawdzić, na co się zgadzamy. Zazwyczaj pierwsze formularze zgody, które wyświetlają się na ekranie telefonu lub komputera, obejmują szeroki zakres czynności przetwarzania. Oprócz oczywistego celu, takiego jak jest np. wykonanie umowy, organizacja wycieczki lub przedstawienia, formularze często proponują zaznaczenie zgody na inne działania, które nie są konieczne i bezpośrednio związane z sytuacją – np. publikację wizerunku, działania marketingowe i promocyjne, a nawet przekazywanie danych innym podmiotom.

Zgoda została formalnie zdefiniowana w RODO (art. 4 pkt 11) i jest skuteczna tylko w sytuacji, gdy stanowi **dobrowolne, konkretne, świadome i jednoznaczne okazanie woli osoby, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego przyzwolenie na przetwarzanie dotyczących jej danych osobowych**. W związku z tym poza wyjątkowymi sytuacjami (o których mowa w art. 6 ust. 1 lit. b-f RODO) zgody nie można domniemywać ani uznać, że nie jest wymagana. Przepisy RODO (motyw 38, 39 i 58) wprowadzają zasadę, że dane osobowe dzieci wymagają szczególnej ochrony, a wszelkie informacje i komunikaty związane z ich przetwarzaniem powinny być łatwo dostępne i zrozumiałe oraz sformułowane tak jasnym i prostym językiem, by dziecko mogło je bez trudu zrozumieć.

Zgodę na przetwarzanie danych osobowych dzieci wyrażają ich rodzice lub opiekunowie prawni (art. 6 ust. 1 lit. a RODO). Powinni oni pamiętać, że **władza rodzicielska**, choć nie ma swojej definicji w Kodeksie rodzinnym i opiekuńczym (Dz. U. z 2023 r. poz. 2809), **nie oznacza całkowicie swobodnego rozporządzania losem dziecka i jest zdeterminowana naczelną zasadą prawa** rodzinnego – **dobrem dziecka.** Art. 95 Kodeksu rodzinnego i opiekuńczego obliguje rodziców lub opiekunów prawnych, by przed wyrażeniem zgody **wzięli pod uwagę poszanowanie**

godności i praw dziecka oraz dbałość o jego jak najlepszy interes, a także by chronili je przed potencjalnym zagrożeniem. W ważniejszych sprawach (w szczególności takich jak udostępnienie wizerunku dziecka w miejscu publicznym, reklamie, czy w mediach) powinni z dziećmi porozmawiać i je wysłuchać, a jeżeli stopień dojrzałości na to pozwala, starać się także uwzględnić ich wolę.

Pewnym odstępstwem od tej zasady jest art. 8 ust. 1 RODO dot. **usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku**, stanowiący, że zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Natomiast, jeżeli dziecko nie ukończyło 16 lat, zgodę na przetwarzanie wyrazić powinna osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem. **Nie oznacza to, że dzieci, które ukończyły 16 lat, mogą swobodnie rozporządzać swoimi danymi osobowymi w internecie.** Przesłanka „oferowania usługi bezpośrednio dziecku" nie jest jednoznaczna. W związku z tym, że dzieci wymagają szczególnej ochrony, nie powinna być interpretowana szeroko. Należy zwrócić uwagę, czy dana usługa społeczeństwa informacyjnego (np. platforma edukacyjna, gra) jest oferowana wprost oraz wyłącznie dzieciom i pamiętać, że sama potencjalna dostępność usługi dla dziecka w internecie o tym nie przesądza.

W publikacji pt. „Wizerunek dziecka w internecie. Publikować czy nie?" opracowanej przez Fundację Orange przy wsparciu prawnym Moniki Trzcińskiej, radczyni prawnej i partnera merytorycznego Urzędu Ochrony Danych Osobowych (Fundacja Orange, 2024, s. 8) wskazano, że **zgoda na rozpowszechnianie wizerunku dziecka powinna:**

1. być wyrażona w sposób **dobrowolny**, rodzic/opiekun prawny nie może być przymuszany do jej wyrażenia;

2. **być precyzyjna i przejrzysta**;

3. **wskazywać cel** przetwarzania lub wykorzystania wizerunku, np. promocję działalności organizacji lub placówki, kampanię społeczna;

4. wskazywać szczegółowy **sposób wykorzystywania wizerunku**, np. publikację na profilu w mediach społecznościowych (przy uściśleniu w jakich serwisach), publikację na stronie internetowej organizacji;

5. **określać warunki wykorzystania wizerunku**, np. czy zdjęcie będzie podpisane imieniem dziecka lub opatrzone komentarzem, czy zdjęcie będzie kadrowane, czy zdjęcie będzie poddane edycji;

6. zostać napisana **zrozumiałym językiem** zarówno dla rodzica, jak i starszego dziecka;

7. być wyrażona **na rzecz konkretnego podmiotu**;

8. dotyczyć **oznaczonego czasu,** po którym dane powinny zostać usunięte (dokładny termin – od i do dnia);

9. być wyrażona **przed przetwarzaniem danych lub opublikowaniem** zdjęcia/nagrania.

Jeżeli po przeczytaniu przedstawionych warunków przetwarzania danych osobowych dziecka któryś z ww. punktów będzie niejasny albo go zabraknie, to koniecznie należy poprosić o doprecyzowanie. Zgodnie z RODO (art. 5 ust. 1 lit a) **dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty** dla osoby, której dane dotyczą.

Najczęściej zgoda jest warunkiem koniecznym przetwarzania danych osobowych, ale są **sytuacje, kiedy nie jest konieczna, jeżeli przetwarzanie jest niezbędne do** (art. 6 ust. 1 lit. b-f RODO):

1. **wykonania umowy, której stroną jest osoba** i której dane dotyczą np. zapisanie dziecka na zajęcia dodatkowe w szkole;

2. **wypełnienia obowiązku prawnego ciążącego na administratorze**, np. obowiązku szkolnego – szkoła przekazuje dane dziecka do kuratorium oświaty w celu realizacji obowiązków edukacyjnych;

3. **ochrony żywotnych interesów osoby, której dane dotyczą**, lub innej osoby fizycznej, np. w nagłych przypadkach medycznych, gdy przetwarzanie danych dotyczących dziecka (np. informacja o grupie krwi czy o alergiach) jest konieczne, aby uruchomić pomoc medyczną;

4. **wykonania zadania realizowanego w interesie publicznym** lub w ramach sprawowania władzy publicznej powierzonej administratorowi, np. ewidencja dzieci podlegających obowiązkowi szkolnemu przez organy administracji samorządowej;

5. **celów wynikających z prawnie uzasadnionych interesów** realizowanych przez administratora lub przez stronę trzecią, np. zapewnienia bezpieczeństwa – szkoła instaluje monitoring wizyjny w celu ochrony dzieci oraz swojego mienia.

Ponadto należy podkreślić, że **RODO nie ma zastosowania do** przetwarzania danych osobowych przez osobę fizyczną w ramach **czynności o czysto osobistym lub domowym charakterze** (art. 2 ust. 2 lit. c), czyli np. robienia zdjęć do rodzinnego albumu fotograficznego. Zgodnie z Ustawą o prawie autorskim i prawach pokrewnych (art. 24) nie wymaga zezwolenia rozporządzanie wizerunkiem człowieka, który stanowi jedynie **szczegół obrazu** przedstawiającego obchód, zgromadzenie, krajobraz itp., jak np. twarz dziecka na widowni meczu piłkarskiego.

Warto pamiętać, iż **zgoda na przetwarzanie danych osobowych może być w każdej chwili odwołana** bez podawania przyczyny, bez jakichkolwiek kosztów i bez jakichkolwiek innych trudności, a administrator danych nie może jej zastąpić inną podstawą przetwarzania danych.

Dane anonimowe i spseudonimizowane

Zarówno anonimizacja danych osobowych jak i ich pseudonimizacja są bardzo skutecznymi metodami ochrony, dlatego zachęcamy do ich stosowania. Te dwa podejścia stanowią różne metody zabezpieczania danych i wywołują różne skutki prawne.

Pseudonimizacja oznacza przetworzenie danych osobowych w taki sposób, by nie **można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji**, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Natomiast **anonimizacja danych osobowych polega na takim ich przetworzeniu, które** całkowicie i nieodwracalnie uniemożliwia zidentyfikowanie osób których te dane dotyczyły. **Konsekwencją tego jest wyłączenie zanonimizowanych danych z reżimu RODO.**

Podsumowując, **pseudonimizacja jest procesem odwracalnym** i umożliwia przy wykorzystaniu dodatkowych informacji ponowną identyfikacje danych z osobą, której dotyczą, podczas gdy **anonimizacja danych jest procesem nieodwracalnym** uniemożliwiającym ich ponowne powiązanie z osobą.

Jak reagować na naruszenia?

W sytuacji naruszenia prywatności dziecka w internecie, np. bezprawnej publikacji zdjęć, warto podjąć próbę skontaktowania się z administratorem strony i żądać ich usunięcia. Nie zawsze jest to możliwe i skuteczne, dlatego trzeba skorzystać

z ochrony jaką zapewniają przepisy prawa, przede wszystkim RODO i Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781), ale także Kodeks cywilny oraz Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2025 r. poz. 24).

Zgodnie z art. 4 pkt 12 RODO **naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa** prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

W Polsce organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).

Zgłoszenia można dokonać na 4 sposoby:

1. elektronicznie poprzez wypełnienie formularza elektronicznego dostępnego bezpośrednio na platformie https://www.biznes.gov.pl;

2. elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: /UODO/SkrytkaESP;

3. elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie biznes.gov.pl (Jak znaleźć Urząd w formularzu pisma ogólnego?) lub platformie epuap.gov.pl;

4. tradycyjną pocztą, wysyłając wypełniony formularz na adres Urzędu (ul. Stawki 2, 00-193 Warszawa).

Na podstawie art. 24 Kodeksu cywilnego można dochodzić **ochrony naruszonego dobra osobistego jakim jest wizerunek człowieka żądając zaniechania takiego działania, chyba że nie jest ono bezprawne (np. zostało uregulowane umową)**. Choć wizerunek chroniony jest przepisami Ustawy o prawie autorskim i prawach pokrewnych (art. 81 i 83), to nie stanowi on w świetle prawa własności intelektualnej. Osobom uprawnionym, których prawa do wizerunku wymagają ochrony, przysługuje możliwość skierowania roszczeń o:

1. zaniechanie działań grożących naruszeniem prawa do ochrony wizerunku;

2. usunięcie skutków tego naruszenia;

3. zadośćuczynienie pieniężne za doznaną krzywdę lub żądanie zapłacenia sumy pieniężnej na cel społeczny, jeżeli to naruszenie było zawinione (zob. szerzej: Niewęgłowski, 2021).

W powyższych przypadkach dot. ochrony na podstawie Kodeksu cywilnego jak i prawa autorskiego warto rozważyć polubowne rozwiązanie sporu (bezpośrednia rozmowa, formalne pismo wzywające drugą stronę do spełnienia roszczenia w określonym terminie), a dopiero, gdy taki sposób okaże się bezskuteczny, należy wnieść pozew do sądu.

Warto zapamiętać!

- **Edukuj: rozmawiaj** z dzieckiem o tym, dlaczego i jak dbać o prywatność w internecie oraz dlaczego bez zgody nie wolno udostępniać czyichś zdjęć; **naucz** dzieci, aby nie podawały swoich danych osobowych (takich jak imię, nazwisko, adres, numer telefonu) czy haseł na stronach internetowych ani w rozmowach z nieznajomymi; **wyjaśnij**, że nie wszystko, co znajduje się w internecie, jest prawdziwe i nie można ufać każdej osobie poznanej online.

- **Unikaj publikowania zdjęć z danymi osobowymi** – jeśli dziecko pozuje z dyplomem, zakryj jego imię i nazwisko przed publikacją lub użyj edytora graficznego do zamazania tych informacji.

- **Nie oznaczaj lokalizacji na zdjęciach** – zamiast publikować zdjęcie dziecka podczas wakacji i oznaczać miejsce („Jesteśmy teraz w Sopocie!"), lepiej dodać je po powrocie, bez podawania dokładnej lokalizacji.

- **Włącz wysokie standardy prywatności na profilach społecznościowych** – ustawienia prywatności (np. na Facebooku lub Instagramie) pozwalają udostępniać zdjęcia tylko wybranym znajomym, a nie publicznie.

- **Sprawdzaj polityki prywatności** serwisów, w których udostępniasz dane – upewniaj się czy są przechowywane w bezpieczny sposób.

- **Nie udostępniaj kompromitujących materiałów –** zdjęcie dziecka w wannie wydaje się urocze, ale może trafić

w niepowołane ręce. Bezpieczniej jest zachować je w prywatnym albumie rodzinnym.

- **Korzystaj z narzędzi/aplikacji do rozmycia twarzy** – tak udostępnione zdjęcie na przykład z wydarzenia szkolnego uniemożliwi rozpoznania twarzy dziecka.

- **Regularnie sprawdzaj, jakie zdjęcia dziecka są dostępne w internecie – wpisanie imienia i nazwiska dziecka w wyszukiwarkę pozwoli to zweryfikować.**

- **Reaguj na nieautoryzowane wykorzystanie wizerunku dziecka –** jeśli znajdziesz zdjęcie swojego dziecka zamieszczone na stronie internetowej szkoły lub firmy bez zgody, skontaktuj się z administratorem i poproś o jego usunięcie.

- **Unikaj publikowania zdjęć z innymi dziećmi bez zgody ich rodziców.**

- Pamiętaj, że przepisy RODO to nie biurokratyczna przeszkoda, a zestaw zasad i procedur umożliwiających ochronę prywatności.

Kluczowe porady dopasowane do wieku dziecka

0–6 lat

- Ograniczaj ilość udostępnianych danych, w tym wizerunku dziecka do minimum.
- Jako rodzic/opiekun masz pełną kontrolę nad publikacją wizerunku dziecka i to ty wyrażasz zgodę na przetwarzanie danych osobowych w jego imieniu.
- Zawsze zastanów się, czy publikacja jest konieczna i czy nie narusza prywatności dziecka.

7–12 lat

- W tym wieku dziecko nie powinno mieć jeszcze kont na portalach społecznościowych, wyjaśniaj dziecku, dlaczego ważne jest przestrzeganie tego ograniczenia.

- Rozpocznij rozmowy z dzieckiem o ochronie wizerunku i konsekwencjach publikacji zdjęć/filmów.

- Zaproś dziecko do uczestnictwa w procesie podejmowania decyzji dotyczących publikacji jego wizerunku. Wyjaśnij mu znaczenie, jakie ma zgoda osób trzecich na udostępnienie zdjęć i filmów, na których się znajdują – w ten sposób przy okazji będziesz w nim kształtować szacunek do innych.

- Wyjaśnij dziecku, czym są dane osobowe i dlaczego należy je chronić.

- Ucz dziecko ostrożności w podawaniu danych osobowych w internecie, uświadom je, że w tym wieku zgoda rodzica/opiekuna jest wymagana do przetwarzania danych.

13+ lat

- Respektuj prawo nastolatka do prywatności i samodzielnego decydowania o publikacji swojego wizerunku.

- Prowadź otwarte rozmowy o konsekwencjach publikacji zdjęć/filmów w internecie.

- Wyjaśnij, jakie są prawa nastolatka w zakresie ochrony danych osobowych (np. prawo do dostępu, usunięcia danych).

- Ucz nastolatka, jak dbać o swój wizerunek w mediach społecznościowych oraz szanować wizerunek koleżanek i kolegów.

- Ucz nastolatka, jak analizować polityki prywatności i jak korzystać z ustawień prywatności w serwisach i aplikacjach.

Od 16. roku życia:

- Zgodnie z RODO, dzieci powyżej 16. roku życia mogą samodzielnie wyrażać zgodę na przetwarzanie swoich danych osobowych w kontekście usług społeczeństwa informacyjnego, oferowanych bezpośrednio dziecku.

- Oznacza to, że po ukończeniu 16 lat, młoda osoba ma prawo do samodzielnego decydowania o swoich danych osobowych w wielu sytuacjach, np. przy korzystaniu z mediów społecznościowych czy innych usług online.

Maciej Groń, NASK

Bibliografia i literatura polecana

Fajgielski, P. (2021). *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz* (wyd. II). Wolters Kluwer Polska.

Fundacja Orange. (2024). *Wizerunek dziecka w internecie. Publikować czy nie?* https://fundacja.orange.pl/app/uploads/2024/07/Wizerunek_dziecka_w_internecie_BROSZURA_wersja-internet_light.pdf

Lievens, E., van der Hof, S., Liefaard, T., Verdoodt, V., Milkaite, I., Hannema, T. (2019). The child right to protection against economic exploitation in the digital world. *The International Journal of Children's Rights, 28*(4), 833–859. https://doi.org/10.1163/15718182-28040003

Milkaite, I., Lievens, E. (2019). The Internet of Toys: Playing Games with Children's Data? W: M. Giovanna, H. Donell (red.), *The Internet of Toys: Practices, Affordances and the Political Economy of Children's Play* (s. 285-305). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-10898-4_14

Niewęgłowski, A. (2021). *Prawo autorskie. Komentarz.* Wolters Kluwer Polska.