Warszawa, 24.06.2021 r.

"ICO z tym internetem dzieci?" - Część III. Standardy 4 - 6

(4 - Przejrzystość, 5 - Szkodliwe wykorzystywanie danych, 6 - Polityki i standardy społeczności)

Pierwsze dwie publikacje dotyczące wytycznych *Information Commissioner's Office* (ICO) w zakresie projektowania produktów i usług (*Age Appriopriate Design Code*) skupiały się na zarysowaniu idei dokumentu wydanego przez ICO (Część I dostępna we wpisie na naszym blogu[1]) oraz na pierwszych trzech standardach (Część II dostępna we wpisie na naszym blogu[2]). Niniejszy tekst stanowi kontynuację tego omówienia.

Standard nr 4 - Przejrzystość

Każda osoba, której dane są przetwarzane, ma prawo uzyskać informacje o tym przetwarzaniu od administratora danych i powinny być one podane w sposób przejrzysty i zrozumiały. Nie inaczej jest w przypadku dzieci korzystających z usług sieciowych i innych cyfrowych produktów, jednakże tutaj ICO zwraca uwagę na kilka istotnych elementów:

- Informacja skierowana do dzieci powinna zachęcać do kontaktu czy konsultacji z osobą dorosłą.
- Administrator powinien upewnić się, że treść informacji jest zrozumiała przed umożliwieniem korzystania przez dziecko z produktu/usługi.
- Informacja powinna zachęcić dziecko do zapoznania się, czyli przyjmować formę, która jest atrakcyjna w odbiorze np. krótki filmik, nagranie dźwiękowe, komiks, rysunki z opisem.
- Informacji skierowanej do dziecka powinna towarzyszyć pełna informacja, z którą może zapoznać się rodzic/opiekun kiedy będzie pomagał dziecku w rozpoczęciu korzystania z produktu/usługi.

Brytyjski organ w swoich wytycznych proponuje następujące sposoby przygotowane w oparciu o podział niepełnoletnich użytkowników na różne kategorie wiekowe:

<u>0-5: niemowlęta i dzieci dopiero zaczynające mówić i czytać:</u>
W przypadku dzieci w tym wieku powinien być bezwzględnie stosowany najwyższy standard ochrony prywatności i powinny być gromadzone wyłącznie niezbędne dla usługi dane.
Przy rozpoczynaniu korzystania z produktu/usługi należy przygotować pełną informację dla rodziców oraz materiał audio/wideo dla dziecka (bez wersji komiksowych ani tekstowych, bo w tym wieku dzieci mogą jeszcze nie umieć czytać), w szczególności należy w nim podkreślić, żeby nie zmieniało nic w ustawieniach prywatności bez rodzica/opiekuna.

<u>6-9: dzieci w czasie nauczania podstawowego:</u>
Najwyższy standard ochrony bezpieczeństwa, pełna informacja dla rodziców/opiekunów, materiał dla dziecka w formie audio/video lub komiksowej. Przy próbie zmiany przez dziecko ustawień prywatności powinna pojawiać się dodatkowa informacja audio/video/komiksowa przedstawiająca skutki takiej zmiany i zachęcająca do kontaktu z osobą dorosłą.

[1] https://www.isecure.pl/blog/ico-z-tym-internetem-dzieci-czesc-i-kodeks/
[2] https://www.isecure.pl/blog/ico-z-tym-internetem-dzieci-czesc-ii-standardy-1-3/

10-12: okres przejściowy:
Pełna informacja dla dorosłych oraz informacja dla dzieci do wyboru, czy audio/wideo, czy wersja do czytania, zapewnienie możliwości zmiany szczegółowości informacji w górę (na prostsze i bardziej zrozumiałe) lub w dół (na bardziej dokładne i obszerne), tak żeby dziecko mogło wybrać informację odpowiednią do swojego poziomu pojmowania. Przy próbie zmiany ustawień dodatkowa informacja audio/video/rysunek o konsekwencjach i zachęcanie do kontaktu z osobą dorosłą.

13-15: wczesne nastolatki:
Pełna informacja dla dorosłych oraz informacja dla dzieci do wyboru - czy audio/wideo, czy wersja do czytania, pozostawienie możliwości zmiany szczegółowości informacji w górę lub w dół, tak żeby dziecko mogło dobrać szczegółowość informacji do poziomu swojego pojmowania. Przy próbie zmiany ustawień dodatkowa informacja audio/video/rysunkowa lub pisemna o konsekwencjach i zachęcanie do kontaktu z osobą dorosłą, jeśli nie rozumieją lub nie są pewni treści.

16-17: zbliżający się do pełnoletności:
Pełna informacja dla dorosłych oraz informacja dla dzieci do wyboru - czy audio/wideo, czy wersja do czytania, pozostawienie możliwości zmiany szczegółowości informacji w górę lub w dół, tak żeby dziecko mogło dobrać szczegółowość informacji do poziomu swojego pojmowania. Przy próbie zmiany ustawień dodatkowa informacja audio/video/rysunkowa lub pisemna o konsekwencjach i zachęcanie do kontaktu z osobą dorosłą, jeśli nie rozumieją lub nie są pewni treści.

Standard 5 - Szkodliwe wykorzystanie danych

Produkt lub usługa skierowane do dziecka powinny chronić je przed szkodami dla ich zdrowia i samopoczucia. W wielu przypadkach istnieją mniej lub bardziej sformalizowane branżowe zasady postępowania i wytyczne, które np. zakładają ograniczenie prezentowania określonej treści (np. przemocy, seksu, narkotyków, samobójstw) lub stosowanie środków mających zwiększyć zaangażowanie czasowe lub emocjonalne np. poprzez nagrody za regularne korzystanie, zachęcanie do publikacji lub odbioru treści angażujących emocjonalnie. W tym miejscu ICO jednoznacznie przesądza, że nie powinno być stosowane przetwarzanie danych, o którym wiadomo, że rodzi wysokie ryzyko dla prywatności lub może zagrozić zdrowiu i samopoczuciu dziecka (w szczególności profilowanie na podstawie analizy zachowań, gromadzenie danych geolokalizacyjnych).

Marketing
Brytyjski *The Committee of Advertising Practice* (CAP) opublikował specjalne wytyczne w zakresie marketingu, które mają zapobiec:

- fizycznym, psychicznym i moralnym szkodom dla dzieci
- wykorzystywanie łatwowierności dzieci i wywieranie na nich presji w kierunku jakiegoś działania
- upominaniu dzieci lub podważaniu autorytetu rodzica
- promocjom zachęcającym do kolejnych zakupów.

Z tego powodu CAP zakazuje kierowania do dzieci szkodliwych reklam np. prezentujących produkty z wysokim poziomem tłuszczów, soli i cukru oraz alkohol. Należy także zachować ostrożność w promocji płatnej, dodatkowej treści i płatnych usług.
Dostawcy produktów i usług powinni się wystrzegać w szczególności praktyk wykorzystujących brak doświadczenia dziecka, łatwowierność, wrażliwość, w celu kierowania agresywnych reklam przekonujących do kupienia określonej zawartości/produktu/usługi.

Strategie powiększania zaangażowania użytkownika.

W przypadku niektórych usług oraz gier online ICO krytykuje techniki mające na celu zwiększenie zaangażowania użytkownika. Zaliczają się do nich m. in.:

- dodatkowe nagrody za regularne korzystanie z usługi (w tym regularne granie) - m. in. bonusy dla aktywnych,
- umożliwienie ciągłego "scrollowania" treści bez komunikatów i blokady po pewnym czasie,
- powiadomienia przypominające i zachęcające do dalszego grania (np. w formie wyskakujących powiadomień na urządzeniu (tzw. "*push notifications*"),
- możliwość ustawienia autogry umożliwiającej grę ciągłą,
- zachęcanie do dalszego korzystania z usług lub bycia online poprzez upewnianie się, czy na pewno użytkownik chce opuścić usługę/produkt - takie pytanie powinno być utrzymane w neutralnym tonie i nie sugerować, że użytkownik może przegrać lub coś stracić, jeśli zakończy korzystanie. Powinno się za to udostępnić użytkownikom funkcję pauzy, także z zastrzeżeniem, że przerwa nie spowoduje porażki w grze lub doznania jakiejś straty.

Standard 6 - Polityka i standardy społeczności

Producent powinien nie tylko skupić się na informacjach dotyczących danych osobowych, ale także w sposób wyraźny przedstawić regulamin usługi oraz standardy i zasady korzystania, a następnie się do nich stosować. Jeśli np. usługa zawiera możliwość komunikacji między użytkownikami, to administrator powinien określić dozwolone ramy komunikacji (np. z określeniem, jakie treści są niedopuszczalne, a następnie wyraźnie o nich poinformować (w szczególności, jeśli monitoruje np. forum czy *chat*'y pod kątem treści niedozwolonych).

ICO wskazuje, że brak przejrzystego przedstawienia zasad działania usługi użytkownikowi może spowodować wywołanie u użytkownika, szczególnie dziecka, błędne przekonanie o tej usłudze (np. dziecko nie wie, że wpisy na forum są monitorowane pod kątem treści).

Jeśli w ramach produktu/usługi przetwarzane są dane dzieci, to błędne opisanie (nieczytelne lub niepełne) wpływa na ewentualną decyzję lub zgodę na korzystanie z usługi, a zatem może stanowić naruszenie RODO.

Bartosz Migas, Specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.