

Warszawa, 12.05.2021 r.

“ICO z tym internetem dzieci?” - Część II. Standardy 1 - 3

(1 - Najlepszy interes dziecka, 2 - Ocena skutków dla ochrony danych, 3 - Dostosowanie do wieku)

Po omówieniu ogólnych informacji na temat wytycznych ICO w tekście “ICO z tym internetem dzieci?” - Część I. Kodeks¹, przyszedł czas na dokładne omówienie każdego z 15 standardów, które należy brać pod uwagę przy projektowaniu narzędzi i usług skierowanych do dzieci lub którymi dzieci mogą się zainteresować i ich używać.

Standard nr 1 - Najlepszy interes dziecka

Pierwszy standard to tak naprawdę ustalenie pryncypiów. ICO wskazuje, że narzędzie i usługi skierowane do dzieci powinny być projektowane w ich najlepszym interesie, zarówno jeśli chodzi o podstawowy cel (dostarczenie konkretnej usługi lub narzędzia), jak i wszelkie praktyki towarzyszące (np. marketing).

Rozumienie najlepszego interesu dziecka według ICO obejmuje następujące zasady:

- chroń dziecko przed wykorzystywaniem reklamowym
- chroń dziecko przed wykorzystywaniem seksualnym
- chroń i wspieraj zdrowie fizyczne i psychiczne
- chroń i wspieraj dobre samopoczucie dziecka
- chroń i wspieraj dochodzenie do własnych poglądów i identyfikacji
- chroń i wspieraj prawo do zrzeszania się (uczestnictwa w grupie) i zabawy
- chroń i wspieraj dzieci z niepełnosprawnościami (a także wspieraj szeroko rozumianą równość).

Najlepszy interes dziecka nie jest oczywiście zawieszony w próżni i należy go konfrontować z innymi interesami, także biznesowymi, ale organ przestrzega przed dowolnością tych ocen wskazując np. że “jest mało prawdopodobne, aby cel marketingowy stał ponad dobrem dziecka”.

Standard nr 2 - Ocena skutków dla ochrony danych osobowych (DPIA)

Drugi ze standardów to zalecenie wykonywania oceny skutków dla ochrony danych osobowych (*ang. Data Protection Impact Assessment - DPIA*), czyli używanie dobrze znanego w RODO mechanizmu oceny projektowanego procesu.

Ocena ta ma pomóc określić, czy i w jakim zakresie wytyczne ICO powinny być stosowane w przypadku konkretnego narzędzia/usługi, a także zidentyfikować ryzyka dla sfery praw i wolności dziecka i dobrać odpowiednie środki, które te ryzyka naruszenia praw zmniejszą.

W sytuacji, gdy narzędzie lub usługa są projektowane dla dzieci lub wiadomo, że dzieci będą jej odbiorcami (np. gry komputerowe, social media), brytyjski organ nadzorczy zaleca przeprowadzenie uprzednich konsultacji z dziećmi, rodzicami, oraz specjalistkami/specjalistami od praw dziecka, aby uwzględnić w ocenie nie tylko spojrzenie biznesowe, ale także odbiór zainteresowanych.

¹ <https://www.isecure.pl/blog/ico-z-tym-internetem-dzieci-czesc-i-kodeks/>

ICO wymienia także ryzyka, na które należy szczególnie zwrócić uwagę:

- obniżenie samopoczucia dziecka, brak akceptacji
- nękanie seksualne
- depresja, lęk przed interakcjami społecznymi
- nieprawidłowe nawyki zdrowotne np. złe nawyki żywieniowe czy złe zachowanie
- zaburzenia snu
- podważanie autorytetu rodziców i ich obowiązków
- nadmierna ekspozycja na reklamy i wykorzystywanie ekonomiczne

Pomocą przy dotrzymywaniu tego standardu ma być arkusz oceny, czy projektowanego narzędzia/usługi dotyczą niniejsze wytyczne (*Annex A: Services covered by the code flowchart* - dostępny w wersji anglojęzycznej²) oraz formularz oceny skutków dla ochrony danych osobowych (*Annex D: DPIA template* - dostępny w wersji anglojęzycznej³).

Standard nr 3 - Dostosowanie do wieku

Mówiąc o dzieciach mamy najczęściej na myśli osoby niepełnoletnie. Jednakże w tej kategorii mieszczą się zarówno kilkuletnie dzieci jak i osoby nastoletnie u progu dorosłości. Brytyjski organ nadzorczy nie tylko dostrzega te różnice, ale nakazuje także brać je pod uwagę przy stosowaniu konkretnych rozwiązań w praktyce.

ICO proponuje z ogólnego pojęcia "dzieci" wyodrębnić następujące grupy, różniące się od siebie etapem rozwoju, potrzebami i zdolnościami poznawczymi:

0 - 5 lat, niemowlęta oraz dzieci dopiero zaczynające czytać i pisać

- w tym wieku nie mają świadomości zagrożeń związanych z korzystaniem z szeroko rozumianego internetu, nie umieją czytać lub mają niewielkie zrozumienie czytanego tekstu, więc nie powinno się kierować do nich informacji pisemnych. Często korzystają z urządzeń dostępowych rodziców, które mogą nie mieć odpowiednich ustawień chroniących dzieci, można nimi łatwo manipulować.

6 - 9 lat, dzieci w okresie nauczania podstawowego

- w tym wieku częściej mają własne urządzenia, częściej korzystają z gier oraz aplikacji interaktywnych, a także są odbiorcami vlogów (wideoblogi) i zaczynają interesować się social mediami, otrzymują już pierwsze informacje o zagrożeniach w sieci, ale jeszcze ich do końca nie rozumieją. Choć nadal znajdują się pod największym wpływem rodziny i szkoły to także coraz ważniejsze jest dla nich dopasowanie się do grupy, co może zachęcać je do określonych zachowań.

10 -12 lat, okres przejściowy

- w tym wieku najczęściej posiadają już własne urządzenia, w szczególności smartfony, są bardziej nastawione na poszukiwanie własnej identyfikacji i dopasowaniu do grupy, w szczególności poprzez

² <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/annex-a-services-covered-by-the-code-flowchart/>

³ <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/annex-d-dpia-template/>

korzystanie z social mediów, łatwo mogą znaleźć się pod wpływem influencerów narzucających standardy zachowań i mody, są narażone na strach przed odrzuceniem przez grupę lub strach przed pominięciem jakiegoś wydarzenia lub trendu. Pozostają więc pod presją ciągłego uczestniczenia w grupie i śledzenia wydarzeń, rozumieją podstawowe zasady i zagrożenia związane z cyfrowym światem i potrafią przewidzieć podstawowe konsekwencje, lecz nadal potrzebują pomocy dorosłych i wsparcia. Znacznie lepiej rozumieją informacje tekstowe i sięgają po nie chętniej, choć nadal mogą preferować informacje w formie wideo.

13 - 15 lat, młodsze nastolatki

- w tym wieku odczuwają potrzebę samoidentyfikacji, większej autonomii, przynależności do grupy, zaczynają się dystansować lub kwestionować wartości i zasady rodziców oraz szkoły, znacznie częściej korzystają z urządzeń i usług bez wiedzy i kontroli rodziców, powszechnie używają social mediów i platform streamingowych (muzyka, filmy), często porównują się do standardów grupy, przez co są narażone na skrajne zachowania, zarówno nadmierne przekonanie o wyższości własnych cech, jak i ryzyko popadania w negatywne stany psychiczne w przypadku poczucia odstawania od reszty lub rozpoznania własnych deficytów. W kwestii zagrożeń i problemów w sieci mogą poszukiwać pomocy i wsparcia rodziców, ale często także boją się kontaktu z rodzicami nie chcąc pokazywać swojej aktywności w sieci.

16 - 17, prawie dorośli

- w tym wieku mają już dużą wiedzę na temat funkcjonowania internetu i zagrożeń związanych z upublicznieniem tam danych (np. zdjęć), mają już dobrze rozwinięte zdolności rozumienia i analizowania sytuacji, ale nadal nie można ich traktować jak w pełni dorosłe osoby. Pomoc ze strony rodziców lub osób dorosłych traktują jako ewentualność, najczęściej zupełnie autonomicznie korzystają z urządzeń oraz narzędzi/usług sieciowych i mają już często prawną możliwość udzielenia wiążącej zgody na przetwarzanie danych osobowych (zależy to jednak od kraju).

Szczegółowy opis tych kategorii jest dołączony do wytycznych (*Annex B: Age and developmental stages*- dostępny w wersji anglojęzycznej⁴).

Choć ICO wskazuje, że nie jest to podział obligatoryjny, to jednak zaznacza, że projektując narzędzie/usługę powinno się jednak jakiegoś podziału dokonać, tak żeby dało się go logicznie uzasadnić.

Te kategorie warto zapamiętać, bo ICO wielokrotnie powraca do tego podziału wskazując na różne praktyki realizowania poszczególnych standardów w zależności od kategorii wiekowej odbiorców.

Jak prawidłowo określić wiek?

Dostosowanie rozwiązań do określonych grup wiekowych powinno zostać poprzedzone rozpoznaniem wieku swoich odbiorców.

Jeżeli po przeprowadzonej ocenie nie ma pewności co do wieku odbiorców, ICO wskazuje następujące rozwiązania:

⁴ <https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/annex-b-age-and-developmental-stages/>

- 1 - zmniejszyć ryzyka dla praw i wolności osób w związku z przetwarzaniem ich danych osobowych dla całej swojej usługi;
- 2 - zwiększyć poziom pewności, w jakim wieku są użytkownicy poprzez zastosowanie odpowiednich środków;
- 3 - zastosować wysoki standard ochrony właściwy dla dzieci do wszystkich użytkowników.

Jakie zatem środki na upewnienie się co do wieku użytkowników proponuje ICO?

- deklaracja wieku, bez weryfikacji - może być wystarczająca, gdy ryzyko związane z przetwarzaniem danych jest niewielkie,
- zastosowanie algorytmów i/lub sztucznej inteligencji do wykrycia w jakim wieku są użytkownicy i czy ich zachowanie jest zgodne z wiekiem deklarowanym,
- współpraca z dostawcą usług potwierdzenia wieku - na rynku funkcjonują podmioty, które pozwalają na weryfikację podanych przez użytkownika danych rejestracyjnych (np. adres email, adres zamieszkania, wiek, imię i nazwisko itp.) w oparciu o różne bazy danych, głównie publiczne, w celu potwierdzenia prawdziwości tych danych i wieku osoby, której dotyczą,
- informacja od innego potwierdzonego użytkownika - np. umożliwienie stworzenia potwierdzonego konta osoby dorosłej, która następnie może stworzyć subkonto i potwierdzić wiek dzieci,
- środki techniczne - np. pytanie o wpisanie roku urodzenia zamiast wieku oraz ograniczenie w możliwości zmiany deklarowanego wieku po jego podaniu,
- twarde dowody np. skany dokumentów - tu trzeba wziąć pod uwagę ryzyka związane z przetwarzaniem danych tak, aby nie przetwarzać ich nadmierne.

Brytyjski organ nadzorczy wskazuje w tym miejscu, że dane pozyskane wyłącznie w celu potwierdzenia wieku danej osoby nie mogą być wykorzystywane następnie do innych celów. Np. jeśli przy założeniu konta wymagane jest podanie daty urodzenia w celu weryfikacji wieku, to nie można wykorzystać znajomości tej daty do wysyłania urodzinowych życzeń wraz z ofertą promocyjną.

Reszta standardów wynikających z wytycznych ICO zostanie opisana w kolejnych tekstach publikowanych na naszym blogu.

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