Warszawa, dn. 09.07.2026 r.

Jak w zgodzie z RODO działać w GameDevie?

Rynek gier i aplikacji rośnie szybciej niż kiedykolwiek wcześniej, co potwierdzają nam liczne raporty biznesowe. Dość powiedzieć, że to branża, która w samym 2025 r. wygenerowała przychody w wysokości prawie 200 miliardów dolarów. Twórcy prześcigają się w nowych mechanikach, personalizacji rozgrywki i wykorzystaniu sztucznej inteligencji. Jednocześnie niemal każda z najnowszych produkcji przetwarza dane swoich użytkowników. Nic więc dziwnego, że oczy regulatorów coraz częściej są zwrócone właśnie na deweloperów.
Przygotowaliśmy tekst oparty na najnowszych wytycznych zawartych w poradniku wydanym przy współpracy hiszpańskiego (AEPD) oraz belgijskiego (GBA) organu ochrony danych. Dodatkowo uwzględniliśmy również porady od francuskiego organu nadzorczego (CNIL) z jego przewodnika po grach hazardowych i aplikacjach mobilnych. W naszym tekście pokażemy Ci, jak projektować gry zgodnie z RODO – od fazy pierwszych szkiców, jej produkcję, wydanie aż wreszcie dalsze utrzymanie jej na rynku. To ważne, bowiem obecnie ochrona danych to nie tylko obowiązek wynikający z przepisów, ale także sposób na budowanie zaufania wśród graczy.

RODO zaczyna się jeszcze przed napisaniem pierwszej linii kodu

Wiele osób kojarzy RODO przede wszystkim z formularzami kontaktowymi, karami administracyjnymi czy też sklepami internetowymi. Mało kto utożsamia je z sektorem rozrywki, jakim niewątpliwie są gry video. Zapewne wielu z nas wydaje się, że twórcy gier muszą martwić się o to dopiero, gdy uda im się wydać ich produkt. W rzeczywistości jednak ochrona danych w tej branży powinna zaczyna się w niej znacznie wcześniej, bowiem już na etapie projektowania gry.
Dlaczego? Bo to wtedy zapadają decyzje dotyczące tego, jakie dane będą zbierane, dlaczego są potrzebne i kto będzie miał do nich dostęp. To wtedy wyznaczane są najczęściej takie obszary jak np.: zakres danych niezbędnych do uczestniczenia w rozgrywce online, z jakich narzędzi i podmiotów zewnętrznych będziemy korzystali czy też jakie są dane niezbędne do zakupu wirtualnej waluty. Im wcześniej uwzględnimy w fazie projektowania kwestie prywatności i ochrony danych, tym łatwiej unikniemy kosztownych zmian na końcowym etapie projektu.
Takie podejście, określane jest jako *Privacy by Design*, polega na projektowaniu modelu ochrony danych od samego początku projektu. Warto również uwzględnić tu zasady *Privacy by Default*, czyli reguł najwyższej ochrony danych. W tym przypadku oznacza to stworzenie gry tak, by jak najlepiej chroniła dane osobowe jej użytkowników.

Twoja gra prawdopodobnie zbiera więcej danych niż myślisz

Dane osobowe w grach to nie tylko imię, nazwisko czy adres e-mail. Głównym zadaniem RODO jest ochrona naszych danych osobowych przed niewłaściwym ich przetwarzaniem. Za dane zaś uważamy wszystkie informacje, które osobno lub w grupie pozwalają na rozpoznanie konkretnej osoby. Jak szeroki jest zaś zakres danych, jakie zbierane są od graczy? Eksperci CNIL wskazali na trzy podstawowe grupy:

- Identyfikatory bezpośrednie: e-mail, nazwa użytkownika czy numer IP.
- Pseudoidentyfikatory: unikalne tokeny sesji czy ID urządzenia, które pozwalają „wyłowić" gracza z tłumu bez znajomości jego nazwiska.
- Metadane: lokalizacja, logi ruchów myszki czy znaczniki czasu.

Dodatkowo należy wskazać na dane behawioralne, a więc dane wrażliwe. Dzieje się tak np.: poprzez wykorzystanie nowych urządzeń do gier, takich jak np.: słuchawki AR/VR. Te zaś wykorzystują zestawy

czujników do gromadzenia danych o wysokim stopniu wrażliwości, takich jak głos, gesty czy mimika twarzy.
Współcześnie dużym problemem jest coraz częstsze wykorzystywanie sztucznej inteligencji do analizowania zachowania użytkowników. To tzw. wnioskowanie behawioralne, które również należy traktować jako profilowanie. Czym wyróżnia się taki rodzaj operacji względem zwykłego zebrania danych? Otóż tutaj użytkownik nie zawsze podaje wszystkie informacje wprost. Te najczęściej powstają w wyniku analizy jego zachowania. Na ich podstawie zaś algorytm podejmuje odpowiednie jego zdaniem decyzje wobec profilowanego.
Warto w tym miejscu pochylić się nad pojęciem *singling out*, czyli mechanizmu „*wyróżniania*". Dochodzi do niego wówczas, gdy system potrafi „*wyróżnić*" konkretnego gracza spośród innych użytkowników na podstawie posiadanych informacji. W praktyce mogą to być takie dane jak: login gracza, adres IP, identyfikator urządzenia, identyfikator konta czy dane o aktywności w grze. Dlatego już na etapie projektowania i tworzenia gry warto sprawdzić, jakie dane faktycznie są lub będą przetwarzane oraz czy wszystkie są niezbędne do działania naszego produktu. Jeżeli jakieś z nich nie są nam potrzebne, to pamiętajmy, że zwłaszcza w ochronie danych minimalizm jest w modzie. Dlatego nie przetwarzajmy danych nadmiarowych.

Telemetria – co gra wie o użytkowniku?

Wyobraź sobie, że chcesz sprawdzić, dlaczego większość graczy kończy zabawę na trzecim poziomie Twojej gry. Jak możesz zweryfikować, gdzie popełniłeś błąd? Skąd czerpać faktyczną wiedzę o tym co frustruje graczy? Najprostszym rozwiązaniem jest uruchomienie telemetrii. Jest to rodzaj zbierania informacji o zachowaniu użytkownika, poprzez monitorowanie jego rozgrywki. Co istotne zbieranie tych informacji nie następuje bezpośrednio a poprzez wykorzystanie odpowiednich systemów monitorujących. Dzięki niej deweloper może sprawdzić między innymi: ile czasu gracze spędzają na konkretnym etapie, gdzie najczęściej przegrywają, z których funkcji korzystają, jakie błędy pojawiają się podczas gry czy też jak wygląda ich styl rozgrywki.
Problem polega na tym, że takie informacje bardzo często stanowią dane osobowe. Współczesne gry potrafią rejestrować dziesiątki parametrów, praktycznie przez cały czas działania aplikacji. Dane te są później wykorzystywane do poprawy jakości gry, wykrywania oszustw, analizowania błędów czy co istotne do personalizacji rozgrywki, w tym potencjalnego profilowania graczy. Większość z nich często nawet nie zdaje sobie sprawy z zakresu takiego monitorowania! A już na pewno nie wiedzą, że dane te mogą być później wykorzystywane do dalszego profilowania reklam. Jak? Otóż przez tzw. *linkability*, czyli możliwość łączenia różnych informacji o użytkowniku. Gry bowiem bardzo często zachęcają graczy do ich integracji z innymi mediami społecznościowymi. Zwiększa to ryzyko wystąpienia zagrożeń związanych z możliwością połączenia danych. Dodatkowo, granie na urządzeniach mobilnych, takich jak smartfony, stwarza dodatkowe szanse na zbieranie danych i łączenie informacji z gry z zestawami danych od stron trzecich.
Tym samym twórcy gier muszą nie tylko poinformować graczy o zbieraniu przez nich danych. Ich równie ważnym zadaniem jest wprowadzenie mechanik obronnych, które uniemożliwią niechcianą migracje danych poza biblioteki dewelopera.

Rozproszone dane to zagrożenie!

Kolejnym problemem nie jest AI a rozproszenie. W wielu projektach największym wyzwaniem nie jest własny kod, lecz rozwiązania dostarczane przez zewnętrznych partnerów. Silniki analityczne, biblioteki reklamowe, systemy płatności czy narzędzia do raportowania błędów bardzo często przetwarzają dane osobowe użytkowników. Zdarza się, że jedna biblioteka korzysta z usług olbrzymiej liczby dostawców. To właśnie kumuluje tzw. efekt matrioszki dewelopera: choć integruje

on jedno SDK (ang. *Software Development Kit*), to w praktyce dane gracza trafiają do kilku lub kilkunastu kolejnych podmiotów. Czym zaś jest SDK? W skrócie oznacza to zestaw narzędzi niezbędnych w ramach jednej biblioteki do tworzenia gry lub aplikacji.
Dlaczego jest to taki problem? Otóż każdy z kolejnych podmiotów może dobierać się do danych Twoich użytkowników. To zaś rodzi realny problem zapanowania nad dostępami dla wyłącznie uprawnionych podmiotów, zwiększa ryzyko wycieku danych a w konsekwencji naraża administratorów na kary. O jakich tu potencjalnie naruszeniach mówimy? Oto one:

- Brak kontroli nad procesorami: nie jesteś w stanie dokładnie sprawdzić, komu powierzasz dane.
- Brak odpowiednich umów: RODO wymaga, by każda relacja z „lalką" w matrioszce była opisana odpowiednią umową powierzenia.
- Naruszenie zasady rozliczalności: jeśli nie potrafisz udowodnić, gdzie dokładnie trafiają dane Twoich graczy, narażasz się na najwyższy wymiar kary, wynoszący nawet do 20 milionów euro, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu.

Premiera gry nie kończy obowiązków związanych z RODO

Pamiętajmy, że po opublikowaniu gry praca nad ochroną danych wcale się nie kończy. Każda aktualizacja, nowe DLC, sezon, wydarzenie specjalne czy integracja z kolejnym narzędziem może zmienić sposób przetwarzania danych osobowych. Istnieje zatem pokusa, aby wykorzystać już posiadane przez nas dane do tych zmian. Mówimy tu o zjawisku *purpose creep*. Rozumiem przez to wykorzystanie danych zebranych w jednym celu do zupełnie innych działań, np. marketingu lub profilowania. Pamiętajmy, że takie działanie praktycznie zawsze nie jest zgodne z RODO! To zaś może narazić nas na potencjalną odpowiedzialność za naruszenie.
Przed wdrożeniem nowych funkcjonalności, warto więc zadać sobie jedno pytanie: czy zaczynamy wykorzystywać dane użytkowników w nowym celu, choć zebraliśmy je do czegoś innego?
Jeżeli odpowiedź brzmi „*tak*", to zaprzestańmy tego robić! Dodatkowo warto przy tym sprawdzić, czy konieczna jest aktualizacja polityki prywatności, dokumentacji lub podstaw prawnych przetwarzania danych.

Podsumowanie

RODO dla twórców gier i aplikacji nie powinno być traktowane wyłącznie jako obowiązek wynikający z przepisów. Odpowiednio zaprojektowane procesy związane z ochroną danych osobowych ułatwiają rozwój produktu, zwiększają zaufanie użytkowników i pomagają ograniczyć ryzyko kosztownych błędów po premierze. Im wcześniej kwestie prywatności zostaną uwzględnione podczas projektowania gry, tym łatwiej będzie rozwijać kolejne funkcjonalności zgodnie z zasadami RODO i uniknąć konieczności wprowadzania zmian na późniejszym etapie. Dobrze przygotowana polityka prywatności, regularny audyt RODO oraz stosowanie zasad Privacy by Design i Privacy by Default stają się dziś standardem w profesjonalnym procesie tworzenia produktów cyfrowych. Warto pamiętać, że gracze coraz częściej zwracają uwagę nie tylko na jakość rozgrywki, ale również na to, w jaki sposób ich dane są wykorzystywane i chronione. Transparentne podejście do ochrony danych buduje wiarygodność studia, wzmacnia relacje z użytkownikami i może stać się realnym elementem przewagi konkurencyjnej na coraz bardziej wymagającym rynku GameDev.

Aleksander Jarymowicz – specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.