

Warszawa, dn. 14.02.2024 r.

## Jak zabezpieczyć dane osobowe graczy na forum internetowym?

Wiele firm z branży gamedev jest w stałym kontakcie ze społecznością graczy. Często taka relacja zaczyna się na długo przed wydaniem gry, czasami może to być etap beta – testów albo tzw. early access (tu świetnym przykładem może być chyba największy hit 2023 r. czyli Baldur's Gate 3) podczas którego gracze mają możliwość przetestować dany tytuł i podzielić się swoimi uwagami i propozycjami zmian. Intensywne kontakty są również już po wydaniu danego tytułu, bo gracze mogą chcieć dzielić się swoimi opiniami, czasami potrzebują wsparcia ze strony oficjalnego supportu, itd.

Jedną z potencjalnie wspólnych cech występowania takiej relacji będzie... przetwarzanie danych osobowych graczy. W poniższym artykule będę chciał się skupić na społeczności skupionej wokół dedykowanego forum internetowego, ale spokojnie część z zawartych tu porad można wykorzystać w szerszej perspektywie – jako generalne dążenie do zapewnienia zgodności z RODO.

Przy okazji tego tekstu, chciałbym zaprosić wszystkich zainteresowanych na webinar, który planujemy zorganizować w dniu 26 marca 2024 r., którego tematem będzie [„Zarządzanie społecznościami graczy: przewodnik po zgodności z RODO”](#), a zatem – jak widać, coś co częściowo będę omawiał poniżej.

### Case study

Przyjmijmy zatem kilka założeń:

- nasze forum internetowe funkcjonuje jako część oficjalnej strony dedykowanej grze wideo,
- na stronie może zarejestrować się każdy internauta poprzez podanie kilku podstawowych informacji o sobie np. adres e-mail, itp.,
- forum jest moderowane, podzielone na stosowne sekcje zarządzane przez administratorów i moderatorów.

Skoro wiemy już z czym mamy do czynienia, zastanówmy się jakie elementy będą niezbędne, żeby nasze forum było zarządzane zgodnie z RODO, a nade wszystko, żeby dane osobowe graczy dokonujących rejestracji były przetwarzane tak, by nie naruszać przepisów o ochronie danych osobowych.

Cały proces powinniśmy rozpocząć od analizy privacy by design oraz privacy by default. W ten sposób unikniemy np. zbierania nadmiarowych informacji o graczach, ale też ustalimy, jak forum powinno być zabezpieczone.

### Niezbędne dane osobowe

Choć istnieje pokusa gromadzenia większej ilości danych, bo bardzo często mamy różne pomysły na ich wykorzystanie (różne cele np. marketing, statystyka, analityka), podczas tworzenia formularza rejestracyjnego powinniśmy ograniczyć się tylko do tego co rzeczywiście niezbędne do tego, by użytkownik mógł korzystać z forum. Wydaje się, że takimi niezbędnymi informacjami mogą być: nickname, adres e-mail, data urodzenia (zwłaszcza jeśli forum dotyczy gry wideo np. z ratingiem PEGI 16 albo wyższym).

## Podstawa prawna do przetwarzania danych osobowych

Dobór podstawy prawnej to kolejna kluczowa sprawa. Warto zaznaczyć, że często jest ona determinowana poprzez cel, do którego dane osobowe mają być wykorzystywane. W przypadku forum internetowym możemy mówić o swego rodzaju umowie o świadczenie usług drogą elektroniczną, gdzie usługodawcą jest firma z branży gamedev, a usługobiorcami internauci (gracze) rejestrujący się na stronie www. Usługodawca zapewnia dostęp do forum i przewidziane na nim funkcjonalności np. możliwość przesyłania wiadomości prywatnych, udział w dyskusjach, itp., a usługobiorcy zobowiązują się do przestrzegania reguł takiego forum.

Jeśli natomiast już na etapie rejestracji nasz dział marketingu wskazał, że chciałby również wykorzystywać dane użytkowników do działań – nazwijmy je ogólnie – marketingowych, wówczas z dużą dozą pewności niezbędna okaże się również zgoda (bądź zgody) na przetwarzanie danych (stosowny checkbox albo nawet kilka checkboxów). Na temat zbierania zgód pisałem na naszym blogu zarówno ja jak i inni nasi specjaliści – polecam zwłaszcza te dwa wpisy: [„Twoja zgoda nie musi być taka formalna, czyli o sztuce pisania klauzul”](#) oraz [„Zgoda dziecka na przetwarzanie danych osobowych”](#).

## Polityka prywatności i obowiązek informacyjny

W obecnych czasach polityka prywatności najczęściej kojarzy nam się z plikami cookies, natomiast warto sobie uzmysłowić, że w tego typu dokumencie można, a nawet powinno się zawrzeć zdecydowanie więcej informacji. Jedną z nich będzie tzw. obowiązek informacyjny, czyli – najkrócej rzecz ujmując – zestaw informacji z których będzie jasno wynikało, kto jest administratorem danych, jak można się z nim skontaktować, jakie są cele wykorzystywania danych, jakie prawa przysługują użytkownikowi, itd.

Należy pamiętać, by polityka prywatności była łatwo dostępnym dokumentem. Zadbaj również, by została napisana prostym i zrozumiałym językiem.

Na temat polityki prywatności również już sporo pisaliśmy, odeślę Ci zatem do tych dwóch materiałów: [„Polityka prywatności na stronie www – o czym należy pamiętać?”](#) oraz [„Jak \(nie\) pisać polityki prywatności – dobre praktyki”](#). Sądzę, że ich lektura pomoże Ci w przygotowaniu stosownego dokumentu.

## Bezpieczeństwo danych osobowych

Temat bezpieczeństwa jest dużo bardziej złożony, ponieważ obejmuje szereg różnych obszarów. Spróbujmy je sobie jakoś zidentyfikować:

- Bezpieczne połączenie - upewnij się, że komunikacja między przeglądarką użytkownika a serwerem forum jest szyfrowana za pomocą protokołu HTTPS, co zabezpiecza dane przed nieuprawnionym dostępem.
- Bezpieczne przechowywanie danych – przechowuj zaszyfrowane dane osobowe.
- Regularne aktualizacje oprogramowania – oprogramowanie ma to do siebie, że po jakimś czasie mogą wyjść pewne luki, które w rękach osób nieuprawnionych mogą posłużyć np. do włamania na serwer, a w konsekwencji do kradzieży danych osobowych. Regularne aktualizowanie oprogramowania powinno zminimalizować

ryzyko wystąpienia tego typu luk, ponieważ taka aktualizacja bardzo często usuwa krytyczne błędy, o których tu mowa.

- Monitorowanie aktywności - monitoruj aktywność na forum, aby wykrywać podejrzane działania i potencjalne naruszenia zabezpieczeń. Gdy wystąpią – reaguj natychmiast.
- Regularne audyty bezpieczeństwa - regularnie przeprowadzaj audyty bezpieczeństwa, aby sprawdzić, czy zabezpieczenia są skuteczne i czy nie ma luk w oprogramowaniu strony www służącej jako forum internetowe.
- Ograniczone dostępy – do danych osobowych powinien mieć dostęp tylko niezbędny personel (zasada minimalizacji dostępu).

### O czym jeszcze warto pamiętać?

Poza wszystkim tym o czym napisałem powyżej, warto jeszcze zadbać o następujące obszary:

- Szkolenie personelu – to bardzo uniwersalna porada, ale prawda jest taka, że bez świadomego personelu, ciężko zadbać o to, by dane osobowe były przetwarzane w prawidłowy sposób. Przeszkoleni pracownicy to także nieco mniejsze ryzyko, że dojdzie w przyszłości do incydentu bezpieczeństwa, a nawet jeśli do niego dojdzie, to takie osoby będą wiedziały jak na nie zareagować.
- Reagowanie na incydenty – skoro o incydentach mowa, to istotne jest, by firma z branży gamedev (oczywiście nie tylko, ale tutaj koncentrujemy się na niej) zadbała o opracowanie procedury reagowania na incydenty, tak by szybko i skutecznie móc zadziałać w przypadku wycieku danych lub innych zagrożeń dla bezpieczeństwa. Więcej o naruszeniach poczytać możesz np. w tym wpisie: [„Naruszenie ochrony danych – czym jest i jak sobie z nim poradzić?”](#).
- Komunikacja z użytkownikami - informuj użytkowników o wszelkich zmianach w polityce prywatności, incydentach bezpieczeństwa lub wyciekach danych, zachowując przejrzystość i uczciwość. Pamiętaj, że w wielu przypadkach, gdy dochodzi do naruszenia ochrony danych, istnieje prawny obowiązek poinformowania o tym samego zainteresowanego (a także organu nadzorczego). Tu również odeślę Cię do bardziej szczegółowego artykułu – [„W jaki sposób prawidłowo zawiadomić o naruszeniu podmiot danych?”](#).

Czy podjęcie powyższych działań skutecznie zabezpieczy dane osobowe graczy na forum internetowym? Cóż, odpowiedź nie jest prosta, ale z całą pewnością wdrażając powyższe zalecenia, zminimalizujesz ryzyka - tak prawne - jak i te, które odnoszą się do obszaru związanego z bezpieczeństwem danych, a zatem będziesz na dobrej drodze do tego, by działać zgodnie z RODO.

**Michał Sztąberek** – ekspert ochrony danych osobowych, prezes zarządu iSecure Sp. z o.o.