Aplikacja mobilna zgodna z RODO, czyli jaka?

Nie ulega wątpliwości, że opracowując aplikację mobilną trzeba zadbać o to, by była ona zgodna z przepisami w zakresie ochrony danych osobowych. Na szczęście RODO dostarcza nam odpowiednie narzędzie, które jest w stanie bardzo mocno przysłużyć się takiej zgodności.

Privacy by design, bo o nim właśnie mowa, to podejście zakładające uwzględnianie ochrony danych osobowych w fazie projektowania. Można oczywiście zadać sobie pytanie, o jakie projektowanie chodzi? Otóż chodzi o projektowanie procesu przetwarzania danych (a więc np. opracowanie mobilnej gry na telefon działającej w modelu free to play, gdzie jednym z istotnych założeń może być gromadzenie danych osobowych przy okazji mikrotransakcji) tak, aby od samego początku odbywało się to, najogólniej rzecz ujmując, w zgodzie z unijnym rozporządzeniem.

Takie podejście ma wiele zalet, a wśród nich wskazać można m.in.:

- podjęcie działań mających na celu uprzednią identyfikację potencjalnych problemów związanych z gromadzeniem danych osobowych,
- działanie w oparciu o przepisy – istnieje większa szansa, że nasza aplikacja mobilna od początku będzie zgodna z RODO, co jest zdecydowanie lepszym podejściem niż późniejsze jej „naprawianie", tak by było – mówiąc kolokwialnie - okej,
- minimalizacja ryzyk powiązanych z przetwarzaniem danych osobowych,
- większa świadomość przepisów o ochronie danych osobowych całego zespołu zaangażowanego w proces opracowywania aplikacji mobilnej.

No dobrze, jak w takim razie zapewnić tę zgodność na etapie projektowania? Poniżej kilka istotnych reguł, które niewątpliwie będą pomocne przy tworzeniu aplikacji mobilnych zgodnych z RODO:

1. **Pozyskiwanie zgody albo zapewnienie innej przesłanki uprawniającej do przetwarzania danych**. Warto od razu to sobie wyjaśnić – zgoda na przetwarzanie danych nie zawsze będzie potrzebna (przy aplikacjach mobilnych bardzo często dochodzi o zawarcia umowy o świadczenie usług drogą elektroniczną), ale nie jest wykluczone, że pewne funkcjonalności będą jej wymagały np. zgoda na geolokalizację, np. jeśli Twoja gra będzie czymś w stylu Pokemon Go! (swoją drogą, pamiętacie jeszcze tę niezwykle popularną grę od firmy Niantic?)

2. **Minimalizacja danych**. Właściwie od tego powinienem zacząć tę wyliczankę. To jeden z kluczy do zapewnienia zgodności z RODO. Krótko rzecz ujmując - ogranicz ilość zbieranych danych do niezbędnego minimum. Nie gromadź nadmiernych lub niepotrzebnych informacji. Prosty przykład: jeśli niezbędna jest data urodzenia, bo np. gra ma mieć oznaczenie PEGI 18 i chcesz zminimalizować ryzyko, że sięgną po nią młodsi użytkownicy, zbieraj datę urodzenia, a nie nr PESEL.

3. **Transparentność procesu gromadzenia danych osobowych**. W zasadzie mógłbym napisać prościej – nie zapomnij o obowiązku informacyjnym, czyli klauzuli, w której dostarczysz użytkownikom jasne informacje na temat tego, kto będzie przetwarzał ich dane osobowe, jakie dane, w jaki sposób będą przetwarzane i do jakich celów

zostaną wykorzystane. Idealnym miejscem, gdzie takie informacje możesz umieścić jest polityka prywatności. Tylko proszę – nie chowaj jej jakoś głęboko, to musi być coś co użytkownik z łatwością będzie mógł znaleźć i zapoznać się z zawartymi w niej informacjami.

4. Retencja danych, czyli określenie jak długo będziesz przechowywał dane zebrane dla poszczególnych celów, dla których je pozyskałeś. Tu ważna sprawa – nie jest niczym niezwykłym to, że niektóre dane będziesz mógł przechowywać dłużej np. dane związane z kwestiami rozliczeniowymi, inne krócej np. do czasu wycofania zgody co może nastąpić w dowolnym momencie. Informacje dotyczące retencji danych powinieneś zamieścić w obowiązku informacyjnym. I pamiętaj - nie przechowuj danych dłużej, niż to jest konieczne.

5. **Zabezpiecz dane osobowe**. Niestety to proces dość skomplikowany i potencjalnie generujący koszty. Żeby w ogóle określić jak zabezpieczyć dane osobowe, powinieneś przeprowadzić ocenę ryzyka dla procesu przetwarzania danych. W ten sposób zidentyfikujesz obszary obarczone większym bądź mniejszym ryzykiem. I na tej podstawie będziesz w stanie dobrać odpowiednie (adekwatne) środki bezpieczeństwa. Jako przykłady podrzucę Ci tu m.in. stosowanie bezpiecznych protokołów https oraz technologii szyfrowania. Nie zapominaj też o regularnych aktualizacjach, zwłaszcza tych, które są krytyczne dla bezpieczeństwa danych. Aha – jeszcze jedna sprawa. Zanim wypuścisz swoją mobilkę na rynek, zadbaj o przeprowadzenie testów penetracyjnych. Pomogą Ci one połatać aplikację, a dzięki temu powinna być bezpieczna. Tylko pamiętaj, by takie testy powtarzać co jakiś czas, bo technologia pędzi do przodu, a to oznacza, że i ludzie, którzy żerują na naszych danych osobowych uczą się w tym zakresie i tworzą coraz bardziej wymyślne techniki przejmowania danych osobowych.

6. Zadbaj o **sprawny proces obsługi żądań** zgłaszanych przez użytkowników Twojej aplikacji mobilnej. RODO daje każdemu całkiem pokaźny pakiet uprawnień m.in. możliwość żądania usunięcia danych, dostarczenia ich kopii, itd. Już na etapie projektowania całego procesu zadbaj o dobry kanał komunikacyjny z użytkownikami oraz kompetentne osoby, które będą obsługiwały takie zgłoszenia.

7. **Weryfikacja potencjalnych dostawców usług**. Jeśli dostęp do danych osobowych mają mieć też inne firmy, czyli dostawcy usług, którzy będą Ci pomagali w jej realizacji, po pierwsze musisz zadbać o to, by dobrać ich po uprzednim przeprowadzeniu weryfikacji na okoliczność zgodności z RODO. I od razu mam dla Ciebie złą wiadomość – UODO ostatnimi czasy rekomenduje konkretne audyty potencjalnych procesorów niż przesyłanie im ankiety weryfikacyjnej. Po drugie zaś, pamiętaj o tym, by zadbać o odpowiednie i bezpieczne dla Ciebie zapisy w umowach powierzenia przetwarzania danych, które z nimi będziesz musiał zawrzeć.

Podsumowując – dobrze przeprowadzony proces privacy by design przy tworzeniu aplikacji mobilnej pozwala uniknąć potencjalnych ryzyk związanych z naruszeniem przepisów dotyczących ochrony danych osobowych w przyszłości.

Michał Sztąberek – ekspert ds. ochrony danych osobowych, CEO w iSecure Sp. z o.o.