

Blockchain i RODO w Twojej firmie: przewodnik po nowych wytycznych EROD

Jeśli pracujesz w branży gier, fashion lub zajmujesz się kwestiami deweloperskimi, to technologia blockchain przestała być dla Ciebie tylko technologiczną ciekawostką. Ta innowacja, nazywana fachowo technologią rozproszonego rejestru (DLT), obiecuje bezpieczne transakcje bez udziału tradycyjnych pośredników, takich jak banki czy notariusze. Dla dewelopera to wizja błyskawicznych rezerwacji lokali, a dla marki odzieżowej – gwarancja, że luksusowa torebka z drugiej ręki jest oryginalna dzięki cyfrowemu certyfikatowi.

Rozwój technologii blockchain stawia jednak przed przedsiębiorcami nowe wyzwania w zakresie ochrony danych osobowych. Jedną z podstawowych zasad RODO jest możliwość sprostowania lub usunięcia danych osobowych, gdy nie są już niezbędne do celu, w jakim zostały zebrane. Tymczasem blockchain został zaprojektowany jako rejestr o trwałym i co do zasady niezmiennym charakterze, w którym raz zapisane informacje pozostają częścią łańcucha bloków. Powstaje zatem pytanie, w jaki sposób pogodzić specyfikę tej technologii z obowiązkami administratorów wynikającymi z RODO, w szczególności z prawem do usunięcia danych oraz zasadą ograniczenia przechowywania.

[W lipcu 2026 r. Europejska Rada Ochrony Danych \(EROD\) przyjęła ostateczną wersję wytycznych 02/2025 dotyczących przetwarzania danych osobowych z wykorzystaniem technologii blockchain.](#)

Dokument ten stanowi praktyczny zbiór wskazówek dla przedsiębiorców planujących wdrożenie lub wykorzystujących już rozwiązania oparte na blockchainie, pokazując, jak pogodzić innowacyjne technologie z wymaganiami RODO. Poniżej przedstawiamy najważniejsze wnioski oraz rekomendacje wynikające z tych wytycznych, które warto uwzględnić przy projektowaniu i prowadzeniu rozwiązań opartych na technologii blockchain.

Jak EROD rozumie pojęcie blockchain?

Blockchain to technologia rozproszonego rejestru, która umożliwia prowadzenie wspólnej bazy danych bez udziału centralnego podmiotu zarządzającego. Dane są przechowywane i synchronizowane pomiędzy uczestnikami sieci, a wszystkie operacje odbywają się zgodnie z wcześniej ustalonymi zasadami. W zależności od przyjętego modelu z sieci mogą korzystać wszyscy zainteresowani lub wyłącznie podmioty, którym przyznano odpowiednie uprawnienia. Jej głównymi cechami są:

- **Brak pośredników (Dezyntermediacja):** Transakcje odbywają się bezpośrednio między ludźmi, bez banku czy notariusza.
- **Niezmienność i odporność na manipulacje:** Gdy dane trafią do łańcucha, każda próba ich zmiany zostanie wykryta.
- **Przejrzystość:** Zazwyczaj każdy uczestnik sieci może podejrzeć historię transakcji.

Dla RODO te zalety są jednocześnie ryzykami. Skoro danych nie da się łatwo usunąć, to jak skutecznie zrealizować prawo klienta do „bycia zapomnianym”? Albo jak zapewnić odpowiedni poziom zabezpieczeń dla rozproszonych danych?

Twoja tożsamość ukryta w portfelu

Największy mit blockchaina to anonimowość. W swoim poradniku EROD wskazuje wprost: identyfikatory takie jak **adres portfela (wallet address)**, klucze publiczne czy unikalne kody urządzeń to dane osobowe. Dlaczego? Bo przy użyciu dodatkowych informacji (np. z giełdy kryptowalut czy logów serwera) można „wyłowić” konkretnego Kowalskiego z tłumu użytkowników.

Zatem choć na pierwszy rzut oka wyglądają jak przypadkowy ciąg liter i cyfr, w rzeczywistości jest to cyfrowy ślad człowieka.

Dlaczego tak jest? W języku RODO nazywamy to **pseudonimizacją**. Oznacza to, że same dane z portfela nie mówią nam wprost, jak nazywa się użytkownik, ale pozwalają go „wyłowić” z tłumu (tzw. *singling out*). Dzieje się to przy użyciu wcześniej wspomnianych dodatkowych informacji, zebranych np. z giełdy kryptowalut, na której klient kupił środki, czy logów serwera Twojej aplikacji. Dzięki nim można bez trudu połączyć konkretny adres portfela z żywym człowiekiem. W praktyce oznacza to konkretne wyzwania dla Twojej branży.

Nawet wykorzystanie zaawansowanych rozwiązań kryptograficznych, takich jak dowody z wiedzą zerową (Zero-Knowledge Proofs, ZKP), nie eliminuje wszystkich obowiązków wynikających z RODO. Jeżeli zastosowane identyfikatory lub dane zastępcze nadal umożliwiają odróżnienie jednego użytkownika od drugiego lub jego identyfikację przy użyciu dodatkowych informacji, mogą zostać uznane za dane osobowe. Dodatkowo należy pamiętać, że przepisy dotyczące przeciwdziałania praniu pieniędzy (AML) oraz regulacje rynku kryptoaktywów (MiCA) nakładają na określone podmioty obowiązek identyfikacji klientów i przechowywania ich danych przez co najmniej pięć lat. W praktyce oznacza to, że całkowita anonimowość użytkowników technologii blockchain często nie jest możliwa do osiągnięcia.

Kto decyduje, ten odpowiada (Role w RODO)

W blockchainie, szczególnie w modelu rozproszonym, ustalenie odpowiedzialności za ochronę danych osobowych jest trudne, ale z punktu widzenia przedsiębiorcy niezbędne. Właściwe określenie ról może bowiem wpłynąć na stopień waszej odpowiedzialności. Oto najważniejsze podmioty związane z przetwarzaniem:

- **Administrator danych (AD):** To „szef” danych. Najczęściej jest to firma, która decyduje „po co” i „jak” przetwarzamy informacje. Przykładem może być deweloper, który buduje system rezerwacji mieszkań oparty na blockchainie.
- **Podmiot przetwarzający (Procesor):** To podmiot, który przetwarza powierzone mu dane osobowe na polecenie administratora, np. firma dostarczająca infrastrukturę węzłów. Najczęściej to administrator będzie odpowiadał za jego błędy. Nie oznacza to jednak, że nie może on zażądać od procesora zwrotu poniesionych kosztów związanych z naruszeniem.

Jak więc najrozsądniej podejść do wyznaczenia ról i odpowiedzialności za przetwarzanie danych w technologii blockchain? W swoim poradniku EROD rekomenduje, aby przedsiębiorcy w pierwszej kolejności wybierali **blockchainy z pozwoleniem (permissioned blockchain)**. W takim modelu dostęp do sieci oraz możliwość dodawania lub modyfikowania danych mają wyłącznie uprawnieni uczestnicy, których zakres uprawnień jest z góry określony. Dzięki temu znacznie łatwiej ustalić, kto odpowiada za przetwarzanie danych osobowych i realizację obowiązków wynikających z RODO, co zwiększa bezpieczeństwo prawne całego projektu. EROD wskazuje również, że zastosowanie innych modeli blockchain powinno być odpowiednio uzasadnione i udokumentowane, a przed ich wdrożeniem warto rozważyć, czy wykorzystanie technologii blockchain jest rzeczywiście niezbędne. Jeżeli ten cel można osiągnąć za pomocą prostszego rozwiązania, organizacja powinna rozważyć zastosowanie innej technologii.

Sytuacja wygląda jednak inaczej w przypadku publicznych sieci blockchain, w których uczestnicy mogą mieć większy wpływ na funkcjonowanie całego systemu. Jeżeli dany uczestnik nie tylko utrzymuje infrastrukturę techniczną, ale również współdecyduje o celach przetwarzania danych lub o kluczowych zasadach działania sieci, może zostać uznany za administratora danych, a w niektórych przypadkach nawet za współadministratora wraz z innymi uczestnikami. Z perspektywy przedsiębiorców oznacza to, że samo korzystanie z technologii blockchain nie przesądza jeszcze o

obowiązkach wynikających z RODO. Kluczowe znaczenie ma rzeczywista rola danego podmiotu w projekcie oraz zakres jego wpływu na sposób przetwarzania danych osobowych. Dlatego każdorazowo warto przeanalizować model działania rozwiązania blockchain przed jego wdrożeniem i prawidłowo określić role poszczególnych uczestników z punktu widzenia przepisów o ochronie danych osobowych.

Techniczne triki: Jak nie wpisywać nazwisk do łańcucha?

Jak więc działać jak najbezpieczniej z danymi? Najważniejsza rada z najnowszych wytycznych brzmi: **unikaj wpisywania danych osobowych bezpośrednio do blockchaina (tzw. on-chain)**. Zamiast tego stosuj metodę **off-chain storage (przechowywanie poza łańcuchem)**.

Oto jak to zrobić bezpiecznie:

- **Haszowanie:** W blockchainie zapisujesz tylko „hasz” (unikalny cyfrowy skrót, który jest jak „odcisk palca” informacji). Same dane osobowe trzymaj w tradycyjnej, bezpiecznej bazie danych znajdującej się poza łańcuchem. Jeśli klient zechce usunąć dane, po prostokasujesz je z bazy a przez to „cyfrowy odcisk palca” w blockchainie staje się bezużyteczny.
- **Szyfrowanie:** Możesz zapisać dane zaszyfrowane, ale pamiętaj: szyfr, który dziś jest nie do złamania, za 10 lat może stać się łatwy do odczytania. Usunięcie klucza szyfrującego jest dobrą praktyką, ale EROD w swoim poradniku zaznacza, że to nie zawsze oznacza pełne usunięcie danych.
- **Zobowiązania kryptograficzne (Commitments):** To nowoczesne rozwiązanie, które pozwala na udowodnienie istnienia pewnych informacji, bez konieczności pokazywania ich wszystkim w sieci. Metoda ta jest to tyle bezpieczna, że również pozwala na przechowywanie danych poza łańcuchem.

7 złotych zasad bezpiecznego projektu (Topka EROD)

Aby Twoja organizacja działała jak najlepiej i nie narażała się na naruszenia ochrony danych, przygotowaliśmy 7 najważniejszych zasad bezpieczeństwa:

- **Od początku przygotuj odpowiednią dokumentację:** Oprócz dokumentacji związanej z RODO, przygotuj dokument, w którym wykażesz, dlaczego blockchain jest w tym procesie niezbędny i czy tego celu nie dało się osiągnąć prostszą metodą.
- **Domyślne „poza łańcuchem”:** Najbezpieczniejszym rozwiązaniem jest przechowywanie danych osobowych poza łańcuchem bloków, a w samym blockchainie umieszczanie wyłącznie informacji niezbędnych do potwierdzenia transakcji lub jej integralności.
- **Wyjaśnij użytkownikowi jak to działa:** Jeżeli korzystasz z technologii blockchain, opisz to w polityce prywatności prostym i zrozumiałym językiem. Użytkownicy powinni wiedzieć, jakie dane są przetwarzane, gdzie trafiają oraz jakie konsekwencje wiążą się z wykorzystaniem tej technologii.
- **Minimalizacja:** Przetwarzaj wyłącznie te dane, które są rzeczywiście potrzebne do realizacji konkretnego celu. Im mniej danych osobowych trafia do systemu, tym mniejsze ryzyko naruszenia przepisów o ochronie danych.
- **Zaufanie jest ważne:** Bezpieczeństwo projektu zależy nie tylko od samej technologii, ale również od dostawców i infrastruktury. Warto wybierać sprawdzone oprogramowanie oraz partnerów gwarantujących odpowiedni poziom bezpieczeństwa i zgodności z obowiązującymi standardami.
- **Przygotuj plan awaryjny:** Przed uruchomieniem systemu warto opracować procedury postępowania na wypadek błędów w kodzie, awarii lub wykrycia podatności wpływających na bezpieczeństwo danych. Szybka reakcja może znacząco ograniczyć skutki incydentu.

- **Projektuj system zgodnie z zasadą „privacy by design”:** Już na etapie projektowania należy przewidzieć mechanizmy umożliwiające realizację praw osób, których dane dotyczą, w szczególności możliwość skorygowania błędnych informacji lub ograniczenia powiązania danych z konkretną osobą, nawet jeżeli dane zapisane w blockchainie mają charakter trwały.

Największe zagrożenia dla przedsiębiorcy

Wytyczne mają pomóc Ci w uniknięciu zagrożeń, jakie mogą wystąpić przy korzystaniu z blockchaina. Co jednak, gdy dojdzie do naruszenia? Dla firmy oznacza to konkretne konsekwencje:

- **Gigantyczne kary finansowe:** RODO przewiduje w tym przypadku dwa progi kar, a najwyższe z nich mogą wynosić do **20 milionów euro** lub **4% rocznego obrotu** firmy!
- **Efekt skali:** Jedną z cech technologii blockchain jest rozproszone przechowywanie danych – ta sama informacja jest zapisywana na wielu węzłach sieci. Oznacza to, że w przypadku błędnego zapisania danych lub naruszenia ochrony danych osobowych skutki incydentu mogą być znacznie poważniejsze niż w tradycyjnych systemach informatycznych.
- **Blokada biznesu:** Prezes UODO ma prawo na was **zakaz przetwarzania danych**. W branży tech czy retail oznacza to konieczność wyłączenia aplikacji, gry lub sklepu online do czasu naprawienia błędów, o co może oznaczać olbrzymie straty finansowe.
- **Utrata reputacji:** Wyciek z „bezpiecznego” blockchaina to cios wizerunkowy, po którym trudno odzyskać zaufanie klientów.

Podsumowanie

Technologia blockchain otwiera przed przedsiębiorcami nowe możliwości, jednak jej wdrożenie wymaga uwzględnienia obowiązków wynikających z RODO już na etapie projektowania rozwiązania. Najnowsze wytyczne Europejskiej Rady Ochrony Danych pokazują, że kluczowe znaczenie ma właściwe określenie ról uczestników, ograniczenie zakresu przetwarzanych danych oraz wybór rozwiązań zapewniających zgodność z zasadą **privacy by design**. Przed wdrożeniem blockchaina warto również ocenić, czy zastosowanie tej technologii jest rzeczywiście uzasadnione oraz przygotować odpowiednią dokumentację potwierdzającą taki wybór. Dzięki świadomemu podejściu przedsiębiorcy mogą wykorzystać potencjał blockchaina, jednocześnie ograniczając ryzyko prawne i organizacyjne związane z ochroną danych osobowych.

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