Informacja o przetwarzaniu danych — Pady/Kontrolery do gier (connected product)

> Dokument przygotowany w celu spełnienia obowiązku informacyjnego wynikającego z Rozporządzenia UE „Data Act” (Regulation (EU) 2023/2854) — obowiązek stosowania od 12 września 2025 r.

---

1. Krótkie podsumowanie

Ten dokument wyjaśnia, jakie dane generuje i przetwarza pad/kontroler do gier (dalsze „Urządzenie”), dlaczego są one zbierane, kto jest "data holder" (podmiot przetwarzający/posiadający dostęp do danych), komu dane mogą być udostępniane, jak możesz uzyskać dostęp do tych danych i na jakich zasadach są przechowywane.

2. Zakres i definicje

- **Urządzenie skomunikowane**: pad/kontroler przewodowy lub bezprzewodowy (Bluetooth/RF/Wi-Fi), łączący się z komputerem, konsolą, smartfonem lub hubem, a także wykorzystujący oprogramowanie/sterowniki chmurowe.
- **Usługi powiązane**: aplikacje mobilne/PC do konfiguracji kontrolera, usługi chmurowe do zapisu ustawień, telemetryczne usługi diagnostyczne, subskrypcje z dodatkowymi funkcjami (np. rozszerzone profile gracza, personalizacje, statystyki).
- **Data holder**: zazwyczaj producent lub dostawca usług powiązanych z kontrolerem.

3. Opis typowych danych generowanych przez kontroler

Dane techniczne i operacyjne

- identyfikatory urządzenia: numer seryjny, identyfikator sprzętowy, adres MAC adaptera (jeżeli występuje);
- dane połączeń: informacje o łączeniu Bluetooth/RF (czas, typ połączenia), logi połączeń;
- telemetryczne dane diagnostyczne: informacje o stanie firmware, błędach, aktualizacjach, liczbie godzin działania;
- dane o konfiguracji: mapowanie przycisków, ustawienia triggerów, wibracji, profili, makr, podświetlenia LED;
- dane dotyczące aktualizacji firmware: wersje, historia aktualizacji.

Dane związane z usługami chmurowymi

- statystyki użycia (np. częstotliwość korzystania, ustawienia gier);
- dane konta użytkownika powiązane z usługą producenta (np. email, login);

- dane płatnicze przy subskrypcjach przetwarzane przez zewnętrznych dostawców płatności.

Możliwy zakres danych osobowych

- dane konta użytkownika (adres email, nazwa użytkownika);
- IP adresy i metadane sieciowe w logach usług chmurowych;
- dane interakcji w aplikacjach powiązanych (np. preferencje użytkownika).

4. Cele przetwarzania danych

- zapewnienie podstawowej funkcjonalności kontrolera;
- diagnostyka, serwis i bezpieczeństwo;
- aktualizacje firmware i poprawki zabezpieczeń;
- synchronizacja i przechowywanie profili użytkownika w chmurze;
- analiza statystyk użycia (agregowane, zanonimizowane);
- świadczenie usług subskrypcyjnych i dodatkowych.

5. Podstawa prawna

- Dla danych osobowych: przepisy o ochronie danych (RODO/GDPR) — zgoda użytkownika lub uzasadniony interes;
- Dla danych generowanych przez urządzenie: obowiązki i prawa wynikające z **Data Act** (użytkownik ma prawo do dostępu i udostępniania danych generowanych przez urządzenie).

6. Udostępnianie danych (odbiorcy)

- wewnętrzne działy producenta (R&D, wsparcie);
- dostawcy usług chmurowych (hosting, przetwarzanie telemetryczne);
- procesorzy płatności (dla subskrypcji);
- podmioty trzecie — wyłącznie na podstawie zgody użytkownika lub przepisów prawa.

7. Przekazywanie danych poza UE/EEA

W przypadku transferu danych poza UE/EEA stosowane są mechanizmy prawne zapewniające odpowiedni poziom ochrony (np. standardowe klauzule umowne, decyzje Komisji Europejskiej). Producent musi wskazać, czy i gdzie dane są przekazywane.

8. Okres przechowywania

- Dane techniczne i funkcjonalne: do czasu korzystania z urządzenia/usługi;
- Logi diagnostyczne i telemetryczne: zgodnie z polityką producenta (np. 6–24 miesięcy);
- Dane konta użytkownika: do czasu usunięcia konta lub rezygnacji z usługi.

9. Twoje prawa jako użytkownika

- prawo dostępu do danych i ich pobrania w standardowym formacie (Data Act);
- prawo do sprostowania/usunięcia danych osobowych (RODO);
- prawo do sprzeciwu/ograniczenia przetwarzania (RODO);
- prawo do informacji o odbiorcach i transferach danych;
- prawo do skargi do organu nadzorczego.

10. Jak uzyskać dostęp do danych / jak je udostępnić

- dostęp do danych przez aplikację/portal producenta;
- możliwość eksportu danych (np. w formacie CSV/JSON);
- możliwość przekazania danych do innego dostawcy (Data Act)

11. Bezpieczeństwo

Producenci wdrażają środki ochrony technicznej i organizacyjnej: szyfrowanie transmisji, bezpieczne aktualizacje firmware, kontrolę dostępu do interfejsów, zabezpieczenia kont użytkownika..

Ten dokument jest wzorem informacyjnym. Dokładne szczegóły (np. okresy przechowywania, lista podmiotów przetwarzających, mechanizmy przekazu poza UE) muszą być uzupełnione przez producenta kontrolera lub dystrybutora wprowadzającego produkt na rynek.