

### ***T-Phone3: zgodność z ustawą UE o danych (rozporządzenie (UE) 2023/2854)***

**Opierając się na konstrukcji systemu operacyjnego Android i związanym z zasadami bezpieczeństwa Google, Luxshare nie ma uprawnień do generowania ani dostępu do danych użytkownika. Od momentu zalogowania się użytkownika za pomocą identyfikatora Google ID i udzielenia autoryzacji, Google działa jako posiadacz danych. W przypadku innych aplikacji stron trzecich, gdy użytkownik udzieli autoryzacji, dostawcy usług stron trzecich stają się również właścicielami danych.**

Polityka bezpieczeństwa Androida jest egzekwowana przez Google i obejmuje funkcje takie jak sandboxing aplikacji, zarządzanie uprawnieniami, szyfrowanie i bezpieczne uruchamianie, które wpływają na sposób dostępu do danych, przechowywania ich i udostępniania.

#### ***1. Przejrzystość przedumowna (art. 3 ust. 2)***

*· Rodzaj i objętość danych, które produkt będzie generował.*

Smartfony z systemem Android generują różne rodzaje „danych o produkcie”, które obejmują informacje o wydajności urządzenia, użyciu i środowisku. Dane te gromadzone są za pośrednictwem czujników, aplikacji i operacji systemowych. Poniżej znajdują się przykłady oparte na możliwościach Androida:

- **Rodzaje danych:**

- **Dane czujnika:** Obejmuje lokalizację (współrzędne GPS), ruch (akcelerometr, odczyty żyroskopu), środowisko (czujnik P, światło) i związane ze zdrowiem (kroki).
- **Dane dotyczące użytkownika i wydajności:** Statystyki korzystania z aplikacji (np. czas spędzony w aplikacjach, zużycie baterii na aplikację).
- **Dane medialne i treści:** Zdjęcia, filmy, nagrania dźwiękowe i dokumenty utworzone lub przechowywane na urządzeniu.

- **Formaty:**

- Dane czujnika: są to dane w czasie rzeczywistym i nie będą przechowywane w telefonie. Jeśli aplikacja zewnętrzna chce ją zebrać, po uzyskaniu autoryzacji użytkownika zostanie ona przesłana do aplikacji w formacie binarnym (dla wyjść surowych czujników).

- Dane multimedialne: JPEG/PNG dla obrazów, MP4 dla filmów, MP3/WAV dla dźwięku.

- **Szacowane objętości:**

- Dane czujnika: śledzenie lokalizacji może generować 1-5 MB dziennie przy ciągłym użyciu; czujniki ruchu mogą dodać 500 KB-2 MB dziennie.
- Dane medialne: bardzo zmienne; pojedyncze zdjęcie może wynosić 2-5 MB, filmy 100 MB+ na minutę.
- Ogólnie rzecz biorąc: codzienna generacja może wynosić od 10 MB (lekkie użycie) do kilku GB (tworzenie ciężkich mediów), w zależności od ustawień i aplikacji. Szacunki te są zgodne z wymogiem ustawy o danych dotyczącym producentów ujawniania wielkości przed zakupem.

*Niezależnie od tego, czy dane są generowane ciągle lub w czasie rzeczywistym.*

Smartfony oparte na Androidzie są w stanie generować dane ciągle i w czasie rzeczywistym. Ta możliwość jest włączona przez architekturę Androida, w tym interfejsy API dla czujników i usług tła, z zastrzeżeniem zasad bezpieczeństwa systemu operacyjnego, takich jak kontrola uprawnień (np. uprawnień LOCATION) i optymalizacja baterii.

- **ciągłej generacji:** Jeśli uprawnienia są udzielane przez użytkownika na poziomie aplikacji, dane, takie jak lokalizacja, ruch lub stan baterii, mogą być zbierane w tle, nawet gdy urządzenie jest w bezczynności lub w trybie gotowości. Na przykład aplikacje fitness używają ciągłego monitorowania czujników do liczenia kroków.
- **Generacja w czasie rzeczywistym:** Android obsługuje strumienie danych w czasie rzeczywistym za pośrednictwem bibliotek, takich jak Kotlin Flow lub interfejsów API, takich jak SensorManager, umożliwiając natychmiastowe przechwytywanie i przetwarzanie (np. aktualizacje GPS na żywo do nawigacji lub interakcje głosowe w czasie rzeczywistym z Asystentem Google). Jest to technicznie wykonalne bez utrudniania funkcji urządzenia, chociaż użytkownicy mogą go wyłączyć za pośrednictwem ustawień, aby zaoszczędzić zasoby.

*Czas przechowywania danych.*

- **Na urządzeniu:** Nieokreślony czas do czasu usunięcia użytkownika, odinstalowania aplikacji lub resetowania fabrycznego.
- **Zdalne:** Konfigurowalne przez użytkownika, np. Google przechowuje dane aktywności do czasu ich usunięcia, z opcjami automatycznego usunięcia (3, 18 lub 36 miesięcy za pośrednictwem kontroli aktywności). Niektóre

dane (np. kopie zapasowe) są przechowywane do czasu usunięcia konta lub ręcznego usunięcia, zgodnie z zasadami minimalizacji RODO.

*Jak użytkownicy mogą uzyskać dostęp do danych i korzystać z nich.*

**Przechowywanie na urządzeniu (zarządzane przez użytkowników końcowych i zależne od uprawnień użytkownika końcowego):**

- **Przechowywanie wewnętrzne:** Zawsze dostępne, używane do danych prywatnych aplikacji (np. baz danych, preferencji). Pojemność: Zazwyczaj 0-128 GB.
- **Przechowywanie zewnętrzne:** Zawiera rozszerzalne karty SD (jeśli są obsługiwane) do udostępniania mediów i dokumentów. Pojemność: do kilku TB za pośrednictwem kart.
- Dane są szyfrowane i trwają do czasu ręcznego usunięcia lub odinstalowania aplikacji (co usuwa pliki specyficzne dla aplikacji).

**Zdalne przechowywanie serwera (zarządzane przez użytkowników końcowych i zależne od uprawnień użytkownika końcowego):**

- Za pośrednictwem usług stron trzecich (np. Dysk Google, Zdjęcia). Dane takie jak kopie zapasowe, historia lokalizacji lub synchronizowane treści są przesyłane automatycznie po zalogowaniu się do konta Google.
- Jest to opcjonalne i kontrolowane przez ustawienia użytkownika (np. Backup & Sync).

**Jak Użytkownik może uzyskać dostęp, odzyskać lub usunąć dane, w tym środki techniczne, warunki użytkowania i jakość usługi**

Użytkownicy smartfonów z systemem Android mają prawo do łatwego i bezpiecznego bezpłatnego dostępu, odzyskiwania i usuwania danych produktu. Ułatwia to funkcje systemu operacyjnego Android i usługi Google, przestrzegając zasad bezpieczeństwa, takich jak prośby o uprawnienia i szyfrowanie. Dostęp do danych musi być zgodny z RODO w odniesieniu do danych osobowych.

• **Metody dostępu i odzyskiwania:**

- **Na urządzeniu:** Za pośrednictwem aplikacji Ustawienia (np. Przechowywanie > Pliki dla mediów; Aplikacje > Informacje o aplikacji dla danych użytkownika). Środki techniczne: Menedżery plików, połączenie USB z komputerem (przy użyciu protokołu MTP) lub interfejsy API takie jak MediaStore dla programistów.
- **Dane zdalne/chmurowe:** Za pośrednictwem narzędzi konta Google.

- **Dostęp w czasie rzeczywistym:** Za pośrednictwem aplikacji lub interfejsów API (np. Sensor Manager dla danych czujników na żywo).

- **Metody usuwania:**

- **Na urządzeniu:** Usuwanie za pośrednictwem przeglądarki plików, ustawień aplikacji lub resetu fabrycznego (usuwa wszystkie dane, ale kopie zapasowe mogą pozostać zdalne).
- **Zdalne:** Użyj sterowania aktywnością, aby usunąć (np. automatyczne usunięcie po ustalonych okresach) lub poprosić o całkowite usunięcie konta. Środki techniczne: interfejsy internetowe lub ustawienia Androida (Konta > Google > Usuń dane).
- **Bezpieczne usunięcie:** Android używa szyfrowania; reset fabryczny kluczy do ścieerek, dzięki czemu dane są nieodzyskalne bez zaawansowanych narzędzi.

· *Czy produkt współpracuje z powiązanymi usługami i w jaki sposób wpływa to na dostęp do danych.*

**Warunki korzystania i jakość usług (QoS):**

- **Warunki:** Podle Polityki prywatności Google ([policies.google.com/privacy](https://policies.google.com/privacy)) wymagana jest zgoda użytkownika. Użytkownik może bezpłatnie uzyskać dostęp do danych, ich pobieranie lub usunięcie, ale z zastrzeżeniem weryfikacji konta i ograniczeń (np. limitów wielkości eksportu). Używanie jest w celach osobistych; udostępnianie wymaga przestrzegania przepisów ustawy o udostępnianiu danych.
- **QoS:** Bezpieczne (HTTPS, szyfrowanie), kompleksowe (formaty czytelne maszynowo) i terminowe (w czasie rzeczywistym, gdzie to możliwe). Dostępność: 24/7 za pośrednictwem narzędzi online, z potencjalnymi opóźnieniami w przypadku dużego eksportu (godziny do dni). Bezpłatne, ale wymagany internet; Pomoc za pośrednictwem Pomocy Google ([support.google.com](https://support.google.com)).

**2. Wymagania projektowe (obowiązujące od 12 września 2026 r.)**

- *Produkty muszą być zaprojektowane tak, aby dane były domyślnie łatwe, bezpieczne i swobodnie dostępne dla użytkownika.*
- *Jeśli dostęp bezpośredni nie jest możliwy, dane muszą być dostarczane na żądanie w ustrukturyzowanym, powszechnie używanym i czytelnym maszynowo formacie.*

- Użytkownicy smartfonów z systemem Android mają prawo do łatwego i bezpiecznego dostępu, odzyskiwania i usuwania danych produktu, za darmo. Ułatwia to funkcje systemu operacyjnego Androida i usługi Google, przestrzegając zasad bezpieczeństwa, takich jak prośby o uprawnienia i szyfrowanie.
- Zgodnie z projektowaniem systemu operacyjnego Android i podlegającym Polityce prywatności Google ([policies.google.com/privacy](https://policies.google.com/privacy)), do gromadzenia danych wymagana jest zgoda użytkownika. Użytkownicy mogą bezpłatnie uzyskać dostęp do danych, ich pobieranie lub usunięcie, ale z zastrzeżeniem weryfikacji konta i ograniczeń (np. limitów wielkości eksportu).

### **3. Prawa do udostępniania danych**

- *Użytkownicy muszą mieć możliwość żądania udostępnienia danych osobom trzecim (np. usługom naprawy).*
- *Producenci mogą żądać tylko rozsądnego odszkodowania od osób trzecich, a nie od użytkowników.*

Opierając się na projektowaniu systemu operacyjnego Android i związanym z zasadami bezpieczeństwa Google, Luxshare nie ma uprawnień do generowania lub dostępu do danych użytkownika.

Użytkownicy systemu Android mają prawo żądać, aby posiadacz danych (np. Google) udostępniał dane o produkcie i powiązane z nim dane serwisowe osobom trzecim (np. usługom naprawczym).

Mogą one poprosić o udostępnienie poprzez sam dostęp do danych i przekazanie ich stronie trzeciej lub polecenie posiadaczowi danych udostępniania ich bezpośrednio. Jest to zgodne z istniejącymi narzędziami, takimi jak Google Takeout.

Użytkownicy Androida mogą sprawdzić Konto Google ([myaccount.google.com](https://myaccount.google.com)) lub ustawienia urządzenia (Ustawienia > O telefonie > Diagnostyka) w celu uzyskania dostępnych podglądów danych.

Alternatywni użytkownicy Androida mogą eksportować dane za pomocą Google Takeout ([takeout.google.com](https://takeout.google.com)) lub wbudowanych narzędzi eksportowych Androida (np. Ustawienia > Konta > Google > Takeout), a następnie udostępniać je ręcznie stronie trzeciej.

### **4. Dostarczanie metadanych**

- *Metadane niezbędne do interpretacji danych muszą być dostarczane w celu zapewnienia użyteczności i jasności.*

Opierając się na projektowaniu systemu operacyjnego Android i związanym z zasadami bezpieczeństwa Google, Luxshare nie ma uprawnień do generowania lub dostępu do danych użytkownika.

Użytkownicy Androida mogą uzyskać dostęp do metadanych i korzystać z nich za pośrednictwem żądań dotyczących danych do właściciela danych Google. Proces jest zgodny z istniejącymi narzędziami Android / Google.

### **Dostęp do metadanych do użytku osobistego dla użytkowników Androida :**

- **Kroki:**
  - Zaloguj się do konta Google za pośrednictwem aplikacji Ustawienia Androida (Ustawienia > Google > Zarządzanie kontem Google) lub [myaccount.google.com](https://myaccount.google.com).
  - Użyj Google Takeout ([takeout.google.com](https://takeout.google.com)) do eksportu danych. Wybierz kategorie takie jak "Usługa konfiguracji urządzenia Android" (dla ustawień urządzenia), "Historia lokalizacji" lub "Moja aktywność" (dla danych o użyciu). Eksport obejmuje metadane w formacie JSON lub CSV, takich jak znaczki czasowe, identyfikatory urządzeń i źródła danych.
  - Aby uzyskać dane na urządzeniu, zaznacz Ustawienia > O telefonie > Status lub użyj aplikacji, takich jak aplikacja Pliki Google, aby wyświetlić właściwości plików (np. daty utworzenia, formaty).
  - Jeśli dane nie są bezpośrednio dostępne, należy złożyć wniosek za pośrednictwem narzędzi prywatności Google ([myaccount.google.com/data-and-privacy](https://myaccount.google.com/data-and-privacy) > Pobierz dane) lub [support.google.com](https://support.google.com), określając potrzebę interpretowalnych danych zgodnie z ustawą o danych.

### **5. Sprawiedliwość umowna**

- *Umowy nie mogą zawierać nieuczciwych warunków ograniczających dostęp do danych lub udostępnianie ich.*
- *Jednostronnie nałożone warunki niekorzystne dla użytkowników lub MŚP są uważane za niewiążące.*

Opierając się na konstrukcji systemu operacyjnego Android i związanych politykami bezpieczeństwa, Luxshare nie ma uprawnień do generowania lub dostępu do danych użytkownika.

Użytkownicy Androida korzystają z umów Google (np. Warunki świadczenia usług Google, Polityka prywatności) i ich warunki (na stronie [policies.google.com/terms](https://policies.google.com/terms)) nie zawierają zabronionych ograniczeń i muszą być zgodne z ustawą o danych osobowych.

### **6. Bezpieczeństwo i poufność**

- *Dostęp może być ograniczony, jeśli narusza bezpieczeństwo produktu lub tajemnice handlowe.*
- *Producenci mogą wdrożyć środki techniczne i organizacyjne w celu ochrony poufnych danych.*

Zależąc od konstrukcji systemu operacyjnego Android i związany polityką bezpieczeństwa, Luxshare nie ma uprawnień do generowania ani dostępu do danych użytkownika.

Polityka prywatności Google (zaktualizowana 1 lipca 2025 r.) podkreśla bezpieczeństwo (np. szyfrowanie, ograniczony dostęp) (<https://policies.google.com/privacy>).

Jako posiadacz danych dotyczących systemu operacyjnego Android (np. za pośrednictwem usług Google Play), Google może ograniczyć dostęp na surowych warunkach, aby uniknąć naruszenia praw użytkownika. Przykład: Google musi ocenić, czy udostępnianie określonych danych (np. surowych dzienników systemu operacyjnego) może ujawnić wady bezpieczeństwa (np. włączenie złośliwego oprogramowania) lub tajemnice handlowe (np. własne modele sztucznej inteligencji w Asystencie Google) i zdecydować się ograniczyć dostęp do danych.