

T-Phone3: dodržování zákona EU o údajích (nařízení (EU) 2023/2854)

Spoléhá se na návrh operačního systému Android a je vázána bezpečnostními zásadami společnosti Google, Luxshare nemá oprávnění generovat nebo získat přístup k uživatelským datům. Od okamžiku, kdy se uživatel přihlásí pomocí svého ID Google a udělí oprávnění, Google působí jako držitel dat. U jiných aplikací třetích stran se jakmile uživatel udělí oprávnění, také poskytovatelé služeb třetích stran stanou držiteli dat.

Zásady zabezpečení Androidu vymáhá společnost Google a zahrnují funkce, jako je sandboxování aplikací, správa oprávnění, šifrování a bezpečné spuštění, které ovlivňují způsob přístupu, ukládání a sdílení dat.

1. Předmluvní transparentnost (čl. 3 odst. 2)

Typ a objem dat, které produkt vytvoří.

Smartphony s Androidem vytvářejí různé typy „produktních dat“, které zahrnují informace o výkonu, používání a prostředí zařízení. Tato data jsou shromažďována prostřednictvím senzorů, aplikací a systémových operací. Níže jsou uvedeny příklady založené na schopnostech Androidu:

- **Typy dat:**

- **Datum senzoru:** Zahrnuje polohu (GPS souřadnice), pohyb (akcelerometer, čtení gyroskopu), životní prostředí (P-senzor, světlo) a zdravotní (kroky).
- **Údaje o použití a výkonu:** Statistiky používání aplikací (např. čas strávený v aplikacích, spotřeba baterie na aplikaci).
- **Média a obsahové údaje:** Fotografie, videa, zvukové nahrávky a dokumenty vytvořené nebo uložené v zařízení.

- **Formáty:**

- Data senzoru: Jedná se o data v reálném čase a nebudou uložena v telefonu. Pokud ji chce aplikace třetí strany shromažďovat, bude po získání uživatelského souhlasu předána aplikaci v binárním formátu (pro surové výstupy senzoru).
- Médiová data: JPEG/PNG pro obrázky, MP4 pro videa, MP3/WAV pro zvuk.

- **Odhadované objemy:**

- Data senzoru: sledování polohy může generovat 1-5 MB denně při nepřetržitém používání; Senzory pohybu mohou přidat 500 KB až 2 MB denně.
- Médiová data: vysoce variabilní; jedna fotografie může být 2-5 MB, videa 100 MB+ za minutu.
- Celkově: Denní generace se může pohybovat od 10 MB (lehké použití) až po několik GB (vytváření těžkých médií) v závislosti na nastavení a aplikacích. Tyto odhady jsou v souladu s požadavkem zákona o údajích, že výrobci zveřejňují objemy před nákupem.

- *At' jsou data generována nepřetržitě nebo v reálném čase.*

Smartphony založené na Androidu jsou schopny vytvářet data nepřetržitě a v reálném čase. Tato možnost je povolena architekturou Androidu, včetně rozhraní API pro senzory a služby na pozadí, podle bezpečnostních zásad operačního systému, jako jsou ovládání oprávnění (např. oprávnění LOCATION) a optimalizace baterie.

- **kontinuální generace:** Pokud uživatel udělí oprávnění na úrovni aplikace, data, jako je poloha, pohyb nebo stav baterie, mohou být shromažďována v pozadí, i když je zařízení v volném provozu nebo v pohotovostním režimu. Například fitness aplikace používají nepřetržité sledování senzorů pro počítání kroků.
- **Generace v reálném čase:** Android podporuje datové toky v reálném čase prostřednictvím knihoven jako je Kotlin Flow nebo API jako je SensorManager, což umožňuje okamžité zachycení a zpracování (např. živé aktualizace GPS pro navigaci nebo hlasové interakce v reálném čase s Asistentem Google). To je technicky proveditelné bez překážky funkce zařízení, ačkoli uživatelé mohou zakázat prostřednictvím nastavení, aby ušetřili zdroje.

- *Doba uchovávání údajů.*

- **Na zařízení:** Neomezeně dlouho do smazání uživatele, odinstalace aplikace nebo továrního resetu.
- **Vzdálený:** Uživatelsky konfigurovatelné, například Google uchovává data o aktivitě až do smazání s možnostmi automatického smazání (3, 18 nebo 36 měsíců prostřednictvím ovládání aktivity). Některá data (např. zálohy) jsou uchovávána až do smazání účtu nebo ručního odstranění v souladu se zásadami minimalizace GDPR.

- *Jak mohou uživatelé přistupovat a používat data.*

Úložiště na zařízení (spravované koncovými uživateli a závislé na oprávnění koncového uživatele):

- **Interní úložiště:** Vždy k dispozici, používá se pro soukromá data aplikace (např. databáze, preference). Kapacita: Obvykle 0-128 GB.
- **Externí úložiště:** Zahrnuje rozšiřovatelné SD karty (pokud jsou podporovány) pro sdílená média a dokumenty. Kapacita: až několik TB prostřednictvím karet.
- Data jsou šifrována a přetrvávají až do ručního odstranění nebo odinstalace aplikace (což odstraňuje soubory specifické pro aplikaci).

Vzdálené úložiště serveru (spravované koncovými uživateli a závislé na oprávnění koncového uživatele):

- Prostřednictvím služeb třetích stran (např. Google Drive, Fotky). Data, jako jsou zálohy, historie polohy nebo synchronizovaný obsah, se nahrávají automaticky při přihlášení k účtu Google.
- Je to volitelné a řízeno nastavením uživatele (např. Zálohování a synchronizace).

Jak může uživatel získat přístup k údajům, získat je nebo je vymazat, včetně technických prostředků, podmínek používání a kvality služby

Uživatelé chytrých telefonů s Androidem mají právo snadno a bezpečně získat přístup k datům produktu, získat je a vymazat je zdarma. To je usnadněno prostřednictvím funkcí operačního systému Android a služeb Google, respektujících bezpečnostní zásady, jako jsou výzvy k povolení a šifrování. Přístup k datům musí být v souladu s GDPR pro osobní údaje.

• Metody přístupu a vyhledávání:

- **Na zařízení:** Prostřednictvím aplikace Nastavení (např. Úložiště > Soubory pro média; Aplikace > Informace o aplikaci pro data o používání). Technické prostředky: Správce souborů, připojení USB k počítači (pomocí protokolu MTP) nebo API jako MediaStore pro vývojáře.
- **Vzdálená/cloudová data:** Prostřednictvím nástrojů účtu Google.
- **Přístup v reálném čase:** Prostřednictvím aplikací nebo API (např. Sensor Manager pro živá data senzorů).

• Metody vymazání:

- **Na zařízení:** Odstranit pomocí prohlížeče souborů, nastavení aplikace nebo továrního resetu (vymaže všechna data, ale zálohy mohou přetrvávat vzdáleně).
- **Vzdálený:** Pomocí ovládacích prvků aktivity můžete smazat (např. automaticky smazat po nastavených obdobích) nebo požádat o úplné smazání účtu. Technické prostředky: Webová rozhraní nebo nastavení Androidu (Účty > Google > Smazat data).
- **Bezpečné vymazání:** Android používá šifrování; tovární reset utírá klíče, což dělá data nezvratná bez pokročilých nástrojů.

Zda produkt interaguje s souvisejícími službami a jak to ovlivňuje přístup k datům.

Podmínky používání a kvalita služeb (QoS):

- **Podmínky:** Podle zásad ochrany osobních údajů společnosti Google (policies.google.com/privacy) je vyžadován souhlas uživatele. Údaje mohou uživatel zdarma získat přístup/získat/vymazat, ale podléhají ověření účtu a omezením (např. omezením velikosti exportu). Použití je pro osobní účely; sdílení vyžaduje dodržování pravidel zákona o sdílení dat.
- **služby QoS:** Bezpečné (HTTPS, šifrování), komplexní (strojově čitelné formáty) a včasné (v reálném čase, kde je to možné). Dostupnost: 24 hodin denně prostřednictvím online nástrojů, s potenciálními zpožděním pro velké exporty (hodiny až dny). zdarma, ale vyžaduje internet; podpora prostřednictvím Nápovědy Google (support.google.com).

2. Požadavky na návrh (účinné od 12. září 2026)

Produkty musí být navrženy tak, aby data byla uživateli ve výchozím nastavení snadno, bezpečně a volně přístupná.

Pokud přímý přístup není možný, musí být údaje na vyžádání poskytnuty ve strukturovaném, běžně používaném a strojově čitelném formátu.

- Uživatelé chytrých telefonů s Androidem mají právo snadno a bezpečně získat přístup k datům produktu, získat je a vymazat je zdarma. To je usnadněno prostřednictvím funkcí operačního systému Android a služeb Google, respektujících bezpečnostní zásady, jako jsou výzvy k povolení a šifrování.
- Podle návrhu operačního systému Android a podle zásad ochrany osobních údajů společnosti Google (policies.google.com/privacy) je pro shromažďování dat vyžadován souhlas uživatele. Údaje mohou

uživatelé svobodně získat přístup/získat/vymazat, ale podléhají ověření účtu a omezením (např. omezení velikosti exportu).

3. Práva ke sdílení dat

- *Uživatelé musí mít možnost požádat o sdílení údajů s třetími stranami (např. opravy).*
- *Výrobci mohou požadovat přiměřenou náhradu pouze od třetích stran, nikoli od uživatelů.*

Spoléhá se na návrh operačního systému Android a je vázána bezpečnostními zásadami Google, Luxshare nemá oprávnění generovat nebo přístup k uživatelským datům.

Uživatelé Androidu mají právo požadovat, aby držitel údajů (například Google) sdílel údaje o produktech a související servisní údaje s třetími stranami (např. servisními službami).

Mohou požádat o sdílení buď tím, že získají přístup k údajům sami a poskytnou je třetí straně, nebo tím, že nařídí držiteli údajů, aby je sdíleli přímo. Je to v souladu se stávajícími nástroji, jako je Google Takeout.

Uživatelé Androidu mohou zkontrolovat účet Google (myaccount.google.com) nebo nastavení zařízení (Nastavení > O telefonu > Diagnostika) pro dostupné náhledy dat.

Alternativní uživatelé Androidu mohou exportovat data pomocí služby Google Takeout (takeout.google.com) nebo vestavěných exportních nástrojů Androidu (např. Nastavení > Účty > Google > Takeout) a poté je ručně sdílet s třetí stranou.

4. Poskytování metadat

- *Metadata potřebná k interpretaci údajů musí být poskytnuta pro zajištění použitelnosti a jasnosti.*

Spoléhá se na návrh operačního systému Android a je vázána bezpečnostními zásadami společnosti Google, Luxshare nemá oprávnění generovat nebo získat přístup k uživatelským datům.

Uživatelé Androidu mohou získat přístup a využívat metadata prostřednictvím požadavků na data od držitele dat Google. Proces je v souladu se stávajícími nástroji Android / Google.

Přístup k metadatům pro osobní použití pro uživatele Androidu:

- **Kroky:**
 - Přihlaste se k účtu Google pomocí aplikace Nastavení Androidu (Nastavení > Google > Správa účtu Google) nebo myaccount.google.com.
 - Použití služby Google Takeout (takeout.google.com) pro export dat. Vyberte kategorie jako "Služba konfigurace zařízení Android" (pro

nastavení zařízení), "Historie polohy" nebo "Moje aktivita" (pro data o používání). Exporty zahrnují metadata ve formátech jako JSON nebo CSV, jako jsou časové razítka, ID zařízení a zdroje dat.

- Pro data v zařízení zaškrtněte položku Nastavení > O telefonu > Stav nebo použijte aplikace, jako je aplikace Soubory Google, abyste zobrazili vlastnosti souborů (např. data vytvoření, formáty).
- Pokud nejsou data přímo přístupná, předložte žádost prostřednictvím nástrojů ochrany osobních údajů společnosti Google (myaccount.google.com/data-and-privacy > Stáhněte si data) nebo support.google.com s uvedením potřeby interpretovatelných dat podle zákona o údajích.

5. Smluvní spravedlnost

· *Smlouvy nesmí obsahovat nekalé podmínky, které omezují přístup k datům nebo jejich sdílení.*

· *Jednostranně uložené podmínky, které znevýhodňují uživatele nebo malé a střední podniky, se považují za nezávazné.*

Spoléhá se na návrh operačního systému Android a je vázána bezpečnostními zásadami, Luxshare nemá oprávnění generovat nebo přístup k uživatelským datům.

Uživatelé Androidu spolupracují se smlouvami společnosti Google (např. Podmínky služby Google, Zásady ochrany osobních údajů) a jejich podmínky (na policies.google.com/terms) neobsahují zakázaná omezení a musí dodržovat zákon o údajích.

6. Bezpečnost a důvěrnost

· *Přístup může být omezen, pokud ohrožuje bezpečnost produktu nebo obchodní tajemství.*

· *Výrobci mohou zavést technická a organizační opatření k ochraně citlivých údajů.*

Spoléhá se na návrh operačního systému Android a je vázána bezpečnostními zásadami, Luxshare nemá oprávnění generovat nebo získat přístup k uživatelským datům.

Zásady ochrany osobních údajů společnosti Google (aktualizované 1. července 2025) zdůrazňují bezpečnost (např. šifrování, omezený přístup) (<https://policies.google.com/privacy>).

Jako držitel dat o operačním systému Android (např. prostřednictvím služeb Google Play) může společnost Google omezit přístup za přísných podmínek, aby nedošlo k narušení práv uživatelů. Příklad: Společnost Google musí posoudit, zda sdílení konkrétních dat (např. surových protokolů operačního systému) by mohlo odhalit bezpečnostní chyby (např. umožnění malwaru) nebo obchodní tajemství (např. patentované modely AI v Asistentu Google) a rozhodnout se omezit přístup k datům.