

T-Phone3: usklađenost s Zakonom o podacima EU-a (Uredba (EU) 2023/2854)

Osnovan na dizajn Android OS-a i vezan za Googleove sigurnosne politike, Luxshare nema dozvolu za generiranje ili pristup korisničkim podacima. Od trenutka kada se korisnik prijavi svojim Google ID-om i odobri, Google djeluje kao nositelj podataka. Za druge aplikacije trećih strana, kada korisnik odobri, pružatelji usluga trećih strana također postaju nositelji podataka.

Google provodi sigurnosne politike Androida i uključuju značajke kao što su sandboxing aplikacija, upravljanje dozvolama, enkripcija i sigurno pokretanje, što utječe na način na koji se podacima pristupa, pohranjuje i dijeli.

1. Transparentnost prije ugovora (članak 3. stavak 2.)

- *Vrsta i količina podataka koje će proizvod generirati.*

Android pametni telefoni generiraju različite vrste "podataka o proizvodu", koji uključuju informacije o performansama uređaja, upotrebi i okolišu. Ovi podaci prikupljaju se putem senzora, aplikacija i operacija sustava. Ispod su primjeri temeljeni na mogućnostima Androida:

- **Vrste podataka:**

- **Podaci senzora:** uključuju lokaciju (GPS koordinate), kretanje (akcelerometar, čitanja žiroskopa), okoliš (P-senzor, svjetlo) i zdravlje (koraci).
- **Podaci o korištenju i performansama:** statistika korištenja aplikacija (npr. vrijeme provedeno u aplikacijama, potrošnja baterije po aplikaciji).
- **Podaci o medijima i sadržaju:** fotografije, videozapisi, audio snimke i dokumenti stvoreni ili pohranjeni na uređaju.

- **Formati:**

- Podaci senzora: To su podaci u realnom vremenu i neće se pohranjivati na telefonu. Ako ga aplikacija treće strane želi prikupiti, nakon dobivanja korisničkog odobrenja, bit će prenesena aplikaciji u binarnom formatu (za sirove izlaze senzora).
- Medijski podaci: JPEG/PNG za slike, MP4 za videozapise, MP3/WAV za audio.

- **Procijenjeni volumeni:**

- Podaci senzora: Praćenje lokacije može generirati 1-5 MB dnevno s kontinuiranom upotrebom; Senzori pokreta mogu dodati 500 KB-2 MB dnevno.
- Medijski podaci: vrlo varijabilni; jedna fotografija može biti 2-5 MB, videozapisi 100 MB+ u minuti.
- Ukupno: Dnevna generacija može varirati od 10 MB (lagana upotreba) do nekoliko GB (stvaranje teških medija), ovisno o postavkama i aplikacijama. Ove procjene su u skladu s zahtjevom Zakona o podacima da proizvođači objave količine prije kupnje.

Bilo da se podaci generiraju kontinuirano ili u realnom vremenu.

Pametni telefoni zasnovani na Androidu mogu kontinuirano generirati podatke i u realnom vremenu. Ova mogućnost omogućuje arhitektura Androida, uključujući API-je za senzore i pozadinske usluge, podložne sigurnosnim politikama operativnog sustava kao što su kontrole dozvola (npr. dozvola LOCATION) i optimizacija baterije.

- **Kontinuirano generiranje:** Ako korisnik dodjeljuje dozvole na razini aplikacije, podaci kao što su lokacija, pokret ili status baterije mogu se prikupljati kontinuirano u pozadini, čak i kada je uređaj u mirnom stanju ili u stanju pripravnosti. Na primjer, fitness aplikacije koriste kontinuirano praćenje senzora za brojanje koraka.
- **Generacija u realnom vremenu:** Android podržava protoke podataka u realnom vremenu putem knjižnica kao što su Kotlin Flow ili API-ja kao što je SensorManager, omogućujući odmah snimanje i obradu (npr. ažuriranja GPS-a uživo za navigaciju ili glasovne interakcije u realnom vremenu s Google Asistentom). To je tehnički izvedivo bez ometanja funkcije uređaja, iako ga korisnici mogu onemogućiti putem postavki kako bi uštedjeli resurse.

Trajanje čuvanja podataka.

- **Na uređaju:** Neograničeno do brisanja korisnika, deinstalacije aplikacije ili tvorničkog resetiranja.
- **Daljinski:** korisnik može konfigurirati, npr. Google zadržava podatke o aktivnosti dok ne izbriše, s opcijama automatskog brisanja (3, 18 ili 36 mjeseci putem kontrole aktivnosti). Neki podaci (npr. sigurnosne kopije) čuvaju se do brisanja računa ili ručnog uklanjanja, u skladu s načelima minimalizacije GDPR-a.

Kako korisnici mogu pristupiti i koristiti podatke.

Skladište na uređaju (kojim upravljaju krajnji korisnici i ovisno o dozvoli krajnjeg korisnika):

- **Interna pohrana:** Uvijek dostupna, koristi se za privatne podatke aplikacije (npr. baze podataka, preferencije). Kapacitet: Obično 0-128 GB.
- **Vanjsko skladištenje:** uključuje proširene SD kartice (ako su podržane) za dijeljive medije i dokumente. Kapacitet: Do nekoliko TB putem kartica.
- Podaci su šifrirani i ostaju sve dok se ručno ne izbriše ili aplikacija ne deinstalira (što uklanja datoteke specifične za aplikaciju).

Daljinsko skladištenje poslužitelja (kojim upravljaju krajnji korisnici i ovisno o dozvoli krajnjeg korisnika):

- Kroz usluge trećih strana (npr. Google Drive, Fotografije). Podaci kao što su sigurnosne kopije, povijest lokacija ili sinkronizirani sadržaj automatski se učitaju kada se prijavite na Google račun.
- To je opcionalno i kontrolirano korisničkim postavkama (npr. Backup & Sync).

Kako korisnik može pristupiti, preuzeti ili izbrisati podatke, uključujući tehnička sredstva, uvjete korištenja i kvalitetu usluge.

Korisnici Android pametnih telefona imaju pravo pristupa, preuzimanja i brisanja podataka o proizvodu jednostavno i sigurno, besplatno. To se olakšava kroz funkcije Androidovog operativnog sustava i Googleove usluge, poštujući sigurnosne politike kao što su zahtjevi za dozvolu i enkripcija. Pristup podacima mora biti u skladu s GDPR-om za osobne podatke.

• Metode pristupa i preuzimanja:

- **Na uređaju:** putem aplikacije Postavke (npr. Skladište > Datoteke za medije; Aplikacije > Informacije o aplikaciji za podatke o korištenju). Tehnička sredstva: Upravljači datotekama, USB veza na računalo (pomoću MTP protokola) ili API-ja kao što je MediaStore za programere.
- **Daljinski/oblačni podaci:** putem alata Google računa.
- **Pristup u realnom vremenu:** putem aplikacija ili API-ja (npr. Sensor Manager za podatke senzora uživo).

• Metode brisanja:

- **Na uređaju:** brisanje putem istraživača datoteka, postavki aplikacije ili tvorničkog reseta (brisa sve podatke, ali sigurnosne kopije mogu trajati na daljinu).
- **Daljinski:** Koristite kontrole aktivnosti za brisanje (npr. automatsko brisanje nakon određenih razdoblja) ili zatražite potpuno brisanje računa. Tehnička sredstva: Web sučelja ili postavke Androida (Računi > Google > Brisanje podataka).
- **Sigurno brisanje:** Android koristi šifriranje; tvornički reset brisa ključeve, čineći podatke nepovratnim bez naprednih alata.

· *Je li proizvod u interakciji s povezanim uslugama i kako to utječe na pristup podacima.*

Uvjeti korištenja i kvaliteta usluge (QoS)Uvjeti korištenja i kvaliteta usluge (QoS):

- **Uvjeti:** U skladu s Googleovom politikom privatnosti (policies.google.com/privacy), potrebna je suglasnost korisnika. Podaci su korisniku besplatni za pristup/preuzimanje/brisanje, ali podložni provjeri računa i ograničenjima (npr. ograničenjima veličine izvoza). korištenje je u osobne svrhe; Dijeljenje zahtijeva poštovanje pravila Zakona o dijeljenju podataka.
- **QoS:** Sigurno (HTTPS, šifriranje), sveobuhvatno (strojno čitljivi formati) i pravovremeno (u realnom vremenu gdje je to moguće). Dostupnost: 24/7 putem online alata, s potencijalnim kašnjenjima za veliki izvoz (sati do dana). Besplatno, ali internet je potreban; podrška putem Google Pomoći (support.google.com).

2. Zahtjevi za dizajn (na snazi od 12. rujna 2026.)

· *Proizvodi moraju biti dizajnirani tako da su podaci jednostavni, sigurni i slobodno dostupni korisniku po podrazumijevanju.*

· *Ako izravni pristup nije moguć, podaci se moraju dostaviti na zahtjev u strukturiranom, obično korištenom i strojno čitljivom formatu.*

- Korisnici Android pametnih telefona imaju pravo pristupa, preuzimanja i brisanja podataka o proizvodu jednostavno i sigurno, besplatno. To se olakšava kroz funkcije Androidovog operativnog sustava i Googleove usluge, poštujući sigurnosne politike kao što su zahtjevi za dozvolu i enkripcija.
- Prema dizajnu Android OS-a i kojima se uređuje Googleova pravila o privatnosti (policies.google.com/privacy), za prikupljanje podataka potrebna je suglasnost korisnika. Korisnici mogu slobodno

pristupiti/preuzeti/izbrisati podatke, ali podložni su provjeri računa i ograničenjima (npr. ograničenjima veličine izvoza).

3. Prava na dijeljenje podataka

- *Korisnici moraju moći zatražiti da se podaci dijele s trećim stranama (npr. uslugama popravka).*
- *Proizvođači mogu zahtijevati razumnu naknadu od trećih strana, a ne od korisnika.*

Osnovan na Android OS dizajn i vezan za Googleove sigurnosne politike, Luxshare nema dozvolu za generiranje ili pristup korisničkim podacima.

Korisnici Androida imaju pravo zatražiti da nositelj podataka (kao što je Google) dijeli podatke o proizvodima i povezane podatke o uslugama s trećim stranama (npr. usluge popravka).

Oni mogu zatražiti dijeljenje bilo pristupom podacima i pružanjem trećoj strani ili upućivanjem nositelju podataka da ih izravno dijeli. To je usklađeno s postojećim alatima kao što je Google Takeout.

Korisnici Androida mogu provjeriti Google račun (**myaccount.google.com**) ili postavke uređaja (Postavke > O telefonu > Dijagnostika) za dostupne preglede podataka.

Alternativni korisnici Androida mogu izvoziti podatke koristeći Google Takeout (takeout.google.com) ili ugrađene alate za izvoz Androida (npr. Postavke > Računi > Google > Takeout), a zatim ih ručno podijeliti s trećom stranom.

4. Pružanje metapodataka

- *Metapodaci potrebni za tumačenje podataka moraju se dostaviti kako bi se osigurala upotrebljivost i jasnoća.*

Osnovan na Android OS dizajn i vezan za Googleove sigurnosne politike, Luxshare nema dozvolu za generiranje ili pristup korisničkim podacima.

Korisnici Androida mogu pristupiti i koristiti metapodatke putem zahtjeva za podacima vlasniku podataka Googleu. Postupak je usklađen s postojećim Android / Google alatima.

Pristup metapodacima za osobnu upotrebu za korisnike Androida:

- **Korak:**
 - Prijavite se na svoj Google račun putem aplikacije Postavke za Android (Postavke > Google > Upravljanje Google računom) ili myaccount.google.com.
 - Koristite Google Takeout (**takeout.google.com**) za izvoz podataka. Odaberite kategorije kao što su "Usluga konfiguracije uređaja za Android" (za postavke uređaja), "Povijest lokacije" ili "Moja aktivnost" (za podatke o korištenju). Izvoz uključuje metapodatke u formatima kao što su JSON ili CSV, kao što su vremenski žigovi, ID uređaja i izvori podataka.

- Za podatke na uređaju, provjerite Postavke > O telefonu > Status ili koristite aplikacije poput aplikacije Google's Files za prikaz svojstva datoteka (npr. datumi stvaranja, formati).
- Ako podaci nisu izravno dostupni, podnesite zahtjev putem Googleovih alata za privatnost (myaccount.google.com/data-and-privacy > Preuzmite podatke) ili support.google.com, navodeći potrebu za tumačivim podacima prema Zakonu o podacima.

5. Ugovorna poštenost

· Ugovori ne smiju uključivati nepoštene uvjete koji ograničavaju pristup podacima ili dijeljenje podataka.

· Jednostrano nametnuti uvjeti koji štete korisnicima ili MSP-ovima smatraju se neobvezavajućim.

Osnovan na dizajn Android OS-a i vezan sigurnosnim politikama, Luxshare nema dozvolu za generiranje ili pristup korisničkim podacima.

Korisnici Androida komuniciraju s Googleovim ugovorima (npr. Googleovi uvjeti korištenja, Politika privatnosti) i njegovi uvjeti (na policies.google.com/terms) ne uključuju zabranjena ograničenja i moraju se pridržavati Zakona o podacima.

6. Sigurnost i povjerljivost

· Pristup može biti ograničen ako ugrožava sigurnost proizvoda ili poslovne tajne.

· Proizvođači mogu provesti tehničke i organizacijske mjere za zaštitu osjetljivih podataka.

Osnovan na dizajn Android OS-a i vezan sigurnosnim politikama, Luxshare nema dozvolu za generiranje ili pristup korisničkim podacima.

Google-ova Politika privatnosti (ažurirana 1. srpnja 2025.) naglašava sigurnost (npr. šifriranje, ograničen pristup) (<https://policies.google.com/privacy>).

Kao vlasnik podataka za podatke o Androidovom sustavu (npr. putem Google Play usluga), Google može ograničiti pristup pod strogim uvjetima kako bi izbjegao narušavanje prava korisnika. Primjer: Google mora procijeniti može li dijeljenje određenih podataka (npr. sirovih operativnih dnevnika) izložiti sigurnosne nedostatke (npr. omogućavanje zlonamjernog softvera) ili poslovne tajne (npr. vlasnički AI modeli u Google Assistantu) i odlučiti ograničiti pristup podacima.