T-Phone3 and TPhone3 PRO: compliance with EU Data Act (Regulation (EU) 2023/2854)

Reliant on Android OS design and bound by Google security policies, Luxshare do not have permission to generate or access user data. From the moment a user logs in with their Google ID and grants authorization, Google acts as the data holder. For other third-party apps, once the user grants authorization, the third-party service providers also become the data holders.

Android's security policies are enforced by Google and include features like app sandboxing, permission management, encryption, and secure boot, which impact how data is accessed, stored, and shared.

*1. **Pre-Contractual Transparency (Article 3(2))***

· *Type and volume of data the product will generate.*

Android smartphones generate various types of "product data," which includes information about the device's performance, usage, and environment. This data is collected via sensors, apps, and system operations. Below are examples based on Android's capabilities:

- **Types of Data**:
    - **Sensor Data**: Includes location (GPS coordinates), motion (accelerometer, gyroscope readings), environmental (P-sensor, light), and health-related (steps).
    - **Usage and Performance Data**: App usage statistics (e.g., time spent in apps, battery consumption per app)
    - **Media and Content Data**: Photos, videos, audio recordings, and documents created or stored on the device.
- **Formats**:
    - Sensor data： It is real-time data and will not be stored on the phone. If a third-party app wants to collect it, after obtaining user authorization, it will be transmitted to the app in binary format (for raw sensor outputs).
    - Media data: JPEG/PNG for images, MP4 for videos, MP3/WAV for audio.
- **Estimated Volumes**:

- Sensor data: Location tracking can generate 1-5 MB per day with continuous use; motion sensors might add 500 KB-2 MB daily.
- Media data: Highly variable; a single photo might be 2-5 MB, videos 100 MB+ per minute.
- Overall: Daily generation can range from 10 MB (light use) to several GB (heavy media creation), depending on settings and apps. These estimates align with the Data Act's requirement for manufacturers to disclose volumes pre-purchase.

· *Whether data is generated continuously or in real-time*.

Android-based smartphones are capable of generating data continuously and in real-time. This capability is enabled by Android's architecture, including APIs for sensors and background services, subject to OS security policies like permission controls (e.g., LOCATION permission) and battery optimization.

- **Continuous Generation**: If permissions are granted by user on an application level, data such as location, motion, or battery status can be collected ongoing in the background, even when the device is idle or in standby mode. For example, fitness apps use continuous sensor monitoring for step counting.
- **Real-Time Generation**: Android supports real-time data streams via libraries like Kotlin Flow or APIs such as SensorManager, allowing immediate capture and processing (e.g., live GPS updates for navigation or real-time voice interactions with Google Assistant). This is technically feasible without hampering device function, though users can disable it via settings to conserve resources.

· *Duration of data retention*.

- **On-Device**: Indefinite until user deletion, app uninstall, or factory reset.
- **Remote**: User-configurable, e.g., Google retains activity data until deleted, with auto-delete options (3, 18, or 36 months via Activity Controls). Some data (e.g., backups) is kept until account deletion or manual removal, aligning with GDPR minimization principles.

· *How users can access and use the data*.

On-Device Storage (managed by end users and dependent on end user permission):

- **Internal Storage**: Always available, used for app-private data (e.g., databases, preferences). Capacity: Typically 0-128 GB or 0-256GB.
- **External Storage**: Includes expandable SD cards (if supported), for shareable media and documents. Capacity: Up to several TB via cards.
- Data is encrypted and persists until manually deleted or app uninstall (which removes app-specific files).

Remote Server Storage (managed by end users and dependent on end user permission):

- Via third-party services (e.g., Google Drive, Photos). Data like backups, location history, or synced content is uploaded automatically when signed into a Google Account.
- This is optional and controlled by user settings (e.g., Backup & Sync).

How the User May Access, Retrieve, or Erase the Data, Including Technical Means, Terms of Use, and Quality of Service

Users of Android smartphones have rights to access, retrieve, and erase product data easily and securely, free of charge. This is facilitated through Android's OS features and Google services, respecting security policies like permission prompts and encryption. Data access must comply with GDPR for personal data.

- **Access and Retrieval Methods**:
  - **On-Device**: Via Settings app (e.g., Storage > Files for media; Apps > App info for usage data). Technical means: File managers, USB connection to a computer (using MTP protocol), or APIs like MediaStore for developers.
  - **Remote/Cloud Data**: Through Google Account tools.
  - **Real-time access:** Via apps or APIs (e.g., Sensor Manager for live sensor data).
- **Erasure Methods**:
  - **On-Device**: Delete via file explorers, app settings, or factory reset (erases all data, but backups may persist remotely).
  - **Remote**: Use Activity Controls to delete (e.g., auto-delete after set periods) or request full account deletion. Technical means: Web interfaces or Android settings (Accounts > Google > Delete data).

- **Secure erasure:** Android uses encryption; factory reset wipes keys, making data irrecoverable without advanced tools.

· *Whether the product interacts with related services and how that affects data access.*

Terms of Use and Quality of Service (QoS):

- **Terms**: Governed by Google's Privacy Policy (policies.google.com/privacy), user consent is required. Data is free for user to access/retrieve/erase, but subject to account verification and limits (e.g., export size caps). Use is for personal purposes; sharing requires compliance with Data Act sharing rules.
- **QoS**: Secure (HTTPS, encryption), comprehensive (machine-readable formats), and timely (real-time where feasible). Availability: 24/7 via online tools, with potential delays for large exports (hours to days). Free of charge, but internet required; support via Google Help (support.google.com).

2. ***Design Requirements (Effective from 12 Sept 2026)***

· *Products must be designed so that data is easily, securely, and freely accessible to the user by default.*

· *If direct access is not possible, data must be provided upon request in a structured, commonly used, and machine-readable format.*

- Users of Android smartphones have rights to access, retrieve, and erase product data easily and securely, free of charge. This is facilitated through Android's OS features and Google services, respecting security policies like permission prompts and encryption.
- Per Android OS design and governed by Google's Privacy Policy (**policies.google.com/privacy**), user consent is required for data collection. Data is free to access/retrieve/erase by users, but subject to account verification and limits (e.g., export size caps).

3. ***Data Sharing Rights***

· *Users must be able to request that data be shared with third parties (e.g., repair services).*

· *Manufacturers may only request reasonable compensation from third parties—not from users.*

Reliant on Android OS design and bound by Google security policies, Luxshare do not have permission to generate or access user data.

Android users have the right to request that data holder (such as Google) share product data and related service data with third parties (ex. repair services).
They can request sharing either by accessing the data themselves and providing it to the third party or by instructing the data holder to share it directly. This is aligned with the existing tools like Google Takeout.
Android users can check Google Account (**myaccount.google.com**) or device settings (Settings > About Phone > Diagnostics) for available data previews.
Alternative Android users can export data using Google Takeout (takeout.google.com) or Android's built-in export tools (e.g., Settings > Accounts > Google > Takeout), then share it manually with the third party.

4. ***Metadata Provision***

· *Metadata necessary to interpret the data must be provided to ensure usability and clarity.*

Reliant on Android OS design and bound by Google security policies, Luxshare do not have permission to generate or access user data.

Android users can access and utilize metadata through data requests to the data holder Google. The process aligns with existing Android/Google tools

Accessing Metadata for Personal Use for Android users :

- **Steps**:
  - Log into your Google Account via the Android Settings app (Settings > Google > Manage your Google Account) or myaccount.google.com.
  - Use **Google Takeout** (takeout.google.com) to export data. Select categories like "Android Device Configuration Service" (for device settings), "Location History," or "My Activity" (for usage data). Exports include metadata in formats like JSON or CSV, such as timestamps, device IDs, and data sources.
  - For on-device data, check Settings > About Phone > Status or use apps like Google's Files app to view file properties (e.g., creation dates, formats).
  - If data is not directly accessible, submit a request via Google's privacy tools (myaccount.google.com/data-and-privacy > Download your data) or support.google.com, specifying the need for interpretable data under the Data Act.

5. ***Contractual Fairness***

· *Contracts must not include unfair terms that restrict data access or sharing.*

· *Unilaterally imposed terms that disadvantage users or SMEs are considered non-binding.*

Reliant on Android OS design and bound by security policies, Luxshare do not have permission to generate or access user data.

Android users interact with contracts from Google (e.g., Google Terms of Service, Privacy Policy) and its terms (at policies.google.com/terms) do not include prohibited restrictions and must comply with the Data Act.

6. ***Security and Confidentiality***

· *Access may be restricted if it compromises product security or trade secrets*.

· *Manufacturers may implement technical and organizational measures to protect sensitive data*.

Reliant on Android OS design and bound by security policies, Luxshare do not have permission to generate or access user data.

Google's Privacy Policy (updated July 1, 2025) emphasizes security (e.g., encryption, restricted access) (https://policies.google.com/privacy).

As the data holder for Android OS data (e.g., via Google Play Services), Google can restrict access under strict conditions to avoid undermining user rights. Example: Google must assess if sharing specific data (e.g., raw OS logs) could expose security flaws (e.g., enabling malware) or trade secrets (e.g., proprietary AI models in Google Assistant) and decide to restrict access to data.