T-Phone3: Einhaltung des EU-Datengesetzes (Verordnung (EU) 2023/2854)

Aufgrund des Android-Betriebssystems und der Sicherheitsrichtlinien von Google ist Luxshare nicht berechtigt, Benutzerdaten zu generieren oder darauf zuzugreifen. Ab dem Moment, in dem sich ein Nutzer mit seiner Google-ID anmeldt und die Genehmigung erteilt, handelt Google als Dateninhaber. Für andere Drittanbieter-Apps werden, sobald der Benutzer die Berechtigung erteilt hat, auch die Drittanbieter Dateninhaber.

Die Sicherheitsrichtlinien von Android werden von Google durchgesetzt und umfassen Funktionen wie App-Sandboxing, Berechtigungsmanagement, Verschlüsselung und sicheren Boot, die Auswirkungen auf den Zugriff, die Speicherung und die Freigabe von Daten haben.

1. Vorvertragliche Transparenz (Artikel 3 Absatz 2)

Art und Datenmenge, die das Produkt generieren wird.

Android-Smartphones generieren verschiedene Arten von "Produktdaten", die Informationen über Leistung, Nutzung und Umgebung des Geräts umfassen. Diese Daten werden über Sensoren, Apps und Systemvorgänge erfasst. Folgende Beispiele basieren auf den Funktionen von Android:

- **Datenarten:**
    - **Sensordaten**: Enthält Standort (GPS-Koordinaten), Bewegung (Beschleunigungsmesser, Gyroskopmessungen), Umwelt (P-Sensor, Licht) und gesundheitsbezogene (Schritte).
    - **Nutzungs- und Leistungsdaten**: App-Nutzungsstatistiken (z.B. Zeit in Apps, Batterieverbrauch pro App).
    - **Medien- und Inhaltsdaten**: Fotos, Videos, Audioaufnahmen und Dokumente, die auf dem Gerät erstellt oder gespeichert wurden.
- **Formate**:
    - Sensordaten: Es handelt sich um Echtzeitdaten und werden nicht auf dem Telefon gespeichert. Wenn eine Drittanbieter-App sie sammeln möchte, wird sie nach Erhalt der Benutzergenehmigung in binärem Format an die App übertragen (für Rohsensorausgänge).

- Mediendaten: JPEG/PNG für Bilder, MP4 für Videos, MP3/WAV für Audio.

- **Geschätzte Volumen**:
  - Sensordaten: Standortverfolgung kann 1-5 MB pro Tag bei kontinuierlicher Nutzung generieren; Bewegungssensoren können täglich 500 KB-2 MB hinzufügen.
  - Mediendaten: Sehr variable; Ein einzelnes Foto kann 2-5 MB sein, Videos 100 MB+ pro Minute.
  - Insgesamt: Die tägliche Generation kann je nach Einstellungen und Apps von 10 MB (leichte Nutzung) bis zu mehreren GB (schwere Medienerstellung) reichen. Diese Schätzungen entsprechen der Anforderung des Datengesetzes, dass Hersteller Mengen vor dem Kauf offenlegen.

· *Ob Daten kontinuierlich oder in Echtzeit generiert werden.*

Android-basierte Smartphones können Daten kontinuierlich und in Echtzeit generieren. Diese Funktion ist durch die Architektur von Android, einschließlich APIs für Sensoren und Hintergrunddienste, unterliegend den Sicherheitsrichtlinien des Betriebssystems wie Berechtigungskontrollen (z. B. LOCATION-Berechtigung) und der Batterieoptimierung aktiviert.

- **Kontinuierliche Generation**: Wenn Benutzerberechtigungen auf Anwendungsebene erteilt werden, können Daten wie Standort, Bewegung oder Batteriestatus laufend im Hintergrund erfasst werden, auch wenn das Gerät im Leerlaub oder im Standby-Modus ist. Zum Beispiel verwenden Fitness-Apps eine kontinuierliche Sensorüberwachung zur Schrittzählung.
- **Echtzeit-Generation**: Android unterstützt Echtzeit-Datenströme über Bibliotheken wie Kotlin Flow oder APIs wie SensorManager, die sofortige Erfassung und Verarbeitung ermöglichen (z. B. Live-GPS-Updates für Navigation oder Echtzeit-Sprachinteraktionen mit Google Assistant). Dies ist technisch möglich, ohne die Gerätefunktion zu behindern, obwohl Benutzer es über Einstellungen deaktivieren können, um Ressourcen zu sparen.

· *Dauer der Datenspeicherung.*

- **Auf dem Gerät**: Unbestimmt bis zum Löschen des Benutzers, zum Deinstallieren der App oder zum Werksreset.
- **Fernbedienung**: Nutzerkonfigurierbar, z.B. speichert Google Aktivitätsdaten bis zum Löschen, mit automatischen Löschmöglichkeiten (3, 18 oder 36 Monate über Aktivitätssteuerungen). Einige Daten (z. B.

Backups) werden bis zur Löschung oder manuellen Entfernung des Kontos aufbewahrt, was den Grundsätzen der DSGVO zur Minimierung entspricht.

- *Wie Nutzer auf die Daten zugreifen und nutzen können.*

On-Device Storage (von Endbenutzern verwaltet und abhängig von Endbenutzerberechtigungen):

- **Interne Speicherung**: Immer verfügbar, verwendet für app-private Daten (z.B. Datenbanken, Präferenzen). Kapazität: Typischerweise 0-128 GB.
- **Externe Speicherung**: Enthält erweiterbare SD-Karten (sofern unterstützt) für freigabbare Medien und Dokumente. Kapazität: Bis zu mehreren TB per Karte.
- Die Daten werden verschlüsselt und bestehen bis zum manuellen Löschen oder zum Deinstallieren der App (wodurch appspezifische Dateien entfernt werden).

Remote Server Storage (von Endbenutzern verwaltet und abhängig von Endbenutzerberechtigungen):

- Über Dienste Dritter (z.B. Google Drive, Fotos). Daten wie Backups, Standortverlauf oder synchronisierte Inhalte werden automatisch hochgeladen, wenn Sie sich bei einem Google-Konto anmelden.
- Dies ist optional und gesteuert durch Benutzereinstellungen (z.B. Backup & Sync).

Wie der Benutzer auf die Daten zugreifen, abrufen oder löschen kann, einschließlich technischer Mittel, Nutzungsbedingungen und Dienstleistungsqualität

Benutzer von Android-Smartphones haben das Recht, auf Produktdaten einfach und sicher und kostenlos zuzugreifen, abzurufen und zu löschen. Dies wird durch die Funktionen des Android-Betriebssystems und die Dienste von Google erleichtert, wobei Sicherheitsrichtlinien wie Berechtigungsaufforderungen und Verschlüsselung eingehalten werden. Datenzugriff muss GDPR für personenbezogene Daten entsprechen.

- **Zugriffs- und Abrufmethoden**:
  - **Auf dem Gerät**: Über die Einstellungen-App (z.B. Speicher > Dateien für Medien; Apps > App-Info für Nutzungsdaten). Technische Mittel:

Dateimanager, USB-Verbindung zu einem Computer (mithilfe des MTP-Protokolls) oder APIs wie MediaStore für Entwickler.

- **Remote-/Cloud-Daten**: Über Google Account Tools.
- **Echtzeit-Zugang:** Über Apps oder APIs (z.B. Sensor Manager für Live-Sensordaten).

- **Löschmethoden**:
  - **Auf dem Gerät**: Löschen über Datei-Explorer, App-Einstellungen oder Werksreset (löscht alle Daten, aber Backups können aus der Ferne bestehen).
  - **Fernbedienung**: Verwenden Sie die Aktivitätssteuerungen, um zu löschen (z. B. automatisches Löschen nach festgelegten Perioden) oder die vollständige Löschung des Kontos anzufordern. Technische Mittel: Web-Schnittstellen oder Android-Einstellungen (Konten > Google > Daten löschen).
  - **Sicheres Löschen:** Android verwendet Verschlüsselung; Fabrik zurücksetzen wipes Schlüssel, so dass Daten ohne erweiterte Werkzeuge unwiederherstellbar.

· Ob das Produkt mit verwandten Diensten interagiert und wie sich dies auf den Datenzugriff auswirkt.

Nutzungsbedingungen und Servicequalität (QoS):

- **Bedingungen**: Unter der Datenschutzrichtlinie von Google (policies.google.com/privacy) ist die Zustimmung des Nutzers erforderlich. Der Zugriff/das Abrufen/das Löschen von Daten ist frei, unterliegt jedoch der Kontoverprüfung und den Grenzen (z.B. Exportgrenzen). Nutzung für persönliche Zwecke; Sharing erfordert Einhaltung der Datenaustauschregeln.
- **QoS**: Sicher (HTTPS, Verschlüsselung), umfassend (maschinenlesbare Formate) und zeitnah (Echtzeit, wo möglich). Verfügbarkeit: 24/7 über Online-Tools, mit möglichen Verzögerungen bei großen Exporten (Stunden bis Tage). Kostenlos, aber Internet erforderlich; Unterstützung über Google-Hilfe (support.google.com).

2. Konstruktionsanforderungen (wirksam ab dem 12. September 2026)
· Produkte müssen so gestaltet werden, dass Daten standardmäßig einfach, sicher und frei zugänglich für den Benutzer sind.

· Ist der direkte Zugriff nicht möglich, müssen die Daten auf Anfrage in einem strukturierten, gängigen und maschinenlesbaren Format bereitgestellt werden.

- Benutzer von Android-Smartphones haben das Recht, auf Produktdaten einfach und sicher und kostenlos zuzugreifen, abzurufen und zu löschen. Dies wird durch die Funktionen des Android-Betriebssystems und die Dienste von Google erleichtert, wobei Sicherheitsrichtlinien wie Berechtigungsaufforderungen und Verschlüsselung eingehalten werden.

- Nach dem Android-Betriebssystem-Design und unter den Datenschutzrichtlinien von Google (policies.google.com/privacy) ist die Einwilligung des Benutzers für die Datenerhebung erforderlich. Daten können von Benutzern frei zugegriffen/abgerufen/gelöscht werden, unterliegen jedoch Kontoverifizierung und Beschränkungen (z.B. Exportgrößen).

3. Rechte zur Datenweitergabe

· Nutzer müssen in der Lage sein, die Weitergabe von Daten an Dritte (z.B. Reparaturdienste) zu verlangen.

· Hersteller dürfen nur angemessene Entschädigungen von Dritten verlangen, nicht von Nutzern.

Luxshare ist auf das Design des Android-Betriebssystems angewiesen und an die Sicherheitsrichtlinien von Google gebunden und hat keine Berechtigung, Benutzerdaten zu generieren oder darauf zuzugreifen.

Android-Nutzer haben das Recht zu verlangen, dass der Dateninhaber (wie Google) Produktdaten und damit verbundene Servicedaten mit Dritten (z.B. Reparaturdienste) weitergibt.
Sie können die Weitergabe beantragen, entweder indem sie auf die Daten selbst zugreifen und diese Dritten zur Verfügung stellen oder indem sie den Dateninhaber beauftragen, diese direkt weiterzugeben. Dies ist mit den bestehenden Tools wie Google Takeout ausgerichtet.
Android-Benutzer können Google-Konto (myaccount.google.com) oder Geräteeinstellungen (Einstellungen > Über Telefon > Diagnostik) auf verfügbare Datenvorschauen prüfen.
Alternative Android-Benutzer können Daten mit Google Takeout (takeout.google.com) oder den eingebauten Exportwerkzeugen von Android (z. B. Einstellungen > Konten > Google > Takeout) exportieren und dann manuell mit dem Dritten teilen.

4. Metadatenbereitstellung

· Metadaten, die zur Interpretation der Daten erforderlich sind, müssen zur Gewährleistung der Benutzerfreundlichkeit und Klarheit bereitgestellt werden.

Aufgrund des Android-Betriebssystems und der Sicherheitsrichtlinien von Google ist Luxshare nicht berechtigt, Benutzerdaten zu generieren oder darauf zuzugreifen.

Android-Nutzer können über Datenanfragen an den Dateninhaber Google auf Metadaten zugreifen und diese nutzen. Der Prozess passt sich an bestehende Android / Google-Tools an.

Zugriff auf Metadaten für den persönlichen Gebrauch für Android-Benutzer:

- **Schritte**:
  - Melden Sie sich über die Android-Einstellungen-App (Einstellungen > Google > Verwalten Ihres Google-Kontos) oder myaccount.google.com an.
  - Verwenden Sie Google Takeout (takeout.google.com), um Daten zu exportieren. Wählen Sie Kategorien wie "Android Device Configuration Service" (für Geräteeinstellungen), "Standortverlauf" oder "Meine Aktivität" (für Nutzungsdaten). Exporte enthalten Metadaten in Formaten wie JSON oder CSV, wie z. B. Zeitstempel, Geräte-IDs und Datenquellen.
  - Wählen Sie für Daten auf dem Gerät Einstellungen > Über das Telefon > Status oder verwenden Sie Apps wie die Dateien-App von Google, um Dateieigenschaften (z. B. Erstellungsdaten, Formate) anzuzeigen.
  - Wenn Daten nicht direkt zugänglich sind, senden Sie eine Anfrage über die Datenschutztools von Google (myaccount.google.com/data-and-privacy > Daten herunterladen) oder support.google.com mit Angabe der Notwendigkeit interpretierbarer Daten gemäß dem Datengesetz.

5. Vertragsgerechtigkeit

· Verträge dürfen keine unfairen Bedingungen enthalten, die den Zugriff oder die Weitergabe von Daten einschränken.

· Einseitig auferlegte Bedingungen, die Nutzer oder KMU benachteiligen, gelten als unverbindlich.

Abhängig vom Android-Betriebssystem-Design und durch Sicherheitsrichtlinien hat Luxshare keine Berechtigung, Benutzerdaten zu generieren oder darauf zuzugreifen.

Android-Nutzer interagieren mit Verträgen von Google (z.B. Google-Nutzungsbedingungen, Datenschutzrichtlinien) und deren Bedingungen (unter policies.google.com/terms) enthalten keine verbotenen Einschränkungen und müssen dem Datengesetz entsprechen.

6. Sicherheit und Vertraulichkeit

· Der Zugang kann eingeschränkt werden, wenn die Produktsicherheit oder Geschäftsgeheimnisse gefährdet werden.
· Hersteller können technische und organisatorische Maßnahmen zum Schutz sensibler Daten ergreifen.

Abhängig vom Android-Betriebssystem-Design und durch Sicherheitsrichtlinien hat Luxshare keine Berechtigung, Benutzerdaten zu generieren oder darauf zuzugreifen.

Die Datenschutzrichtlinie von Google (aktualisiert am 1. Juli 2025) betont die Sicherheit (z. B. Verschlüsselung, eingeschränkter Zugriff) (https://policies.google.com/privacy).

Als Dateninhaber von Android-Betriebssystemdaten (z.B. über Google Play Services) kann Google den Zugriff unter strengen Bedingungen einschränken, um die Nutzerrechte zu vermeiden. Beispiel: Google muss beurteilen, ob die Weitergabe bestimmter Daten (z. B. Roh-OS-Protokolle) Sicherheitslücken (z. B. Aktivierung von Malware) oder Geschäftsgeheimnisse (z. B. proprietäre KI-Modelle in Google Assistant) aufdecken könnte, und beschließen, den Zugriff auf Daten zu beschränken.