Pre-contractual information for Connected Products and Related Services
according to Article 3 (2)(3) EU Data Act

In accordance with **Regulation (EU) 2023/2854 (the "EU Data Act")**, we, **Motorola Group**) provide the following information about our Connected Products and Related Services (**"products and services"**). This declaration is intended to give customers and users details about the types of data generated by our products or services, how that data is handled, and how access is enabled. It also outlines the nature, volume, and storage of such data, the purposes for which it is used, and the conditions under which it may be accessed or shared, in accordance with the EU Data Act.

Please note: Depending on the specific customizations, add-ons selected, and additional services selected for the products and services, the types, frequencies and amounts of data gathered and processed may vary.
This pre-contractual information is located at Pre-contractual information. Where information changes during the lifetime of the product or service, this information will be updated at the previously mentioned location.

Covered Products and Services

This declaration applies to:

- Personal and business computing devices (smartphones, IoT ecosystem devices)
- Associated software and cloud-based services (device management tools, data sanitization, software pre-installs, telemetry, remote diagnostics, updates, and (remote) support platforms, AI model adaptation, collaboration connectivity, compatible accessories connectivity)
- For smartphones and IoT ecosystem devices - device activation tracking, device management (incl. country and carrier specific device configuration), hardware and software usage, diagnostics, warranty service and other.

Types of Data Generated

Depending on the product and configuration, data may include:

- Device hardware parameters like battery voltage levels, battery temperature, Wi-Fi and Bluetooth [turned on / off], cellular network type in use [3G, 4G, 5G, etc.]
- Device stability data like force close, application not responding, kernel panic, tombstones
- Android application usage parameters like, which applications are installed, when they are opened and how long they were used and other.

Data Format, Volume, Frequency, and Retention

- Data format used is JSON format.

- Volume of data generated differs by the model type and the number of unique features and apps on the phone. The duration of the phone usage also directly impacts the data volume. On average, this volume typically is around 22Kb per device per day in uncompressed format for a mid-tier device with good device stability and nominal usage.
- Data collection frequency: Data generated by various processes running in the phone will be written to an on-device database [called check in DB]. This check in DB is a circular buffer with a dedicated size of 5 MB. Most of the Motorola developed user applications write the data once a day into this check in DB, typically around midnight local time. Some hardware modules and older Motorola developed user applications write data in real time [like battery level change, temperature change, RAT changes etc.] into this on-device check in database. The data stored in the on device database is uploaded to the cloud once a day around midnight local time.
- Depending on the technical design of the product or service, data may be stored either locally on the device or remotely on a server. Where applicable, the intended duration of retention is determined by the nature of the data, technical feasibility, and contractual or regulatory requirements.
- Typically, data is stored for the duration of the statutory warranty period, as defined by the national laws of the respective EU Member State. In certain cases, the warranty period may be extended based on individual contractual agreements with the User. Retention periods may therefore differ depending on the product or service type, data category, or applicable legal requirement. Additionally, data may be retained for longer periods where necessary, for example, to support research and development activities, to resolve product quality issues, or to comply with statutory retention obligations under commercial or tax law. Where personal data is involved, retention is subject to applicable data protection laws, and data will be deleted once the purpose of processing no longer applies, unless legal obligations require longer storage.

Data Access and Sharing

- **Customers / Users**:

  Access to data generated by the product or service can be provided either **directly** or **indirectly**, depending on the design and technical setup.

  - **Direct Access**

    Users have the technical means to access their data without needing to request it. Depending on the nature of the product or service and relevant technical parameters, Users can:

        - Export device-related data and activity history directly from the device.
        - Access data via management dashboards, APIs, or on-device interfaces.
        - Use authentication systems such as Motorola ID, or their own Single Sign-On (SSO) system to access data.
        - In some cases, users may also be able to retrieve or erase certain data directly, depending on the technical setup and available functionalities.
        - Delete customer-owned device data by removing the device from the TSM Portal.

    - **Indirect Access**

      If the product or service does not support direct access, Users and Customers may request access, retrieval, or erasure of relevant data by contacting Motorola. In such cases, Motorola will process the request in accordance with applicable legal and contractual obligations.

- **Service Providers & Partners** may access relevant diagnostic data directly or indirectly strictly for support and maintenance, under contractual agreements. Sharing data is usually governed by legal requirements, service necessity, or user consent, with safeguards to protect data security. Common examples include:

    - Maintenance & Repair Partners
    - Business Partners for Co-Owned/Co-Delivered services if Motorola offer products or services jointly with other companies, it may share relevant data with these business partners — only to the extent needed to deliver the co-provided service and other.

- **Other third parties**: Data may be shared with global third-party service providers, limited to technical operation and subject to security safeguards.
- **Affiliates**: Motorola share data with its global group companies (e.g., regional subsidiaries or business units in markets like Europe, Asia, or the Americas) to support consistent service delivery, cross-regional device management, and compliance with local regulations.

Where Motorola controls access over data generated by the product or service, it may use readily available data for purposes including fulfilling contractual obligations, complying with legal requirements, improving product quality, supporting research and development, and enhancing customer experience.

If Motorola intends to share data with third parties, this third party is only allowed to use the data for purposes that have been agreed upon with the User.

User Rights

In line with the EU Data Act:

- Users may request access, retrieval, and portability of data in a structured format.
- Users may request erasure of stored data, subject to technical feasibility and contractual obligations.
- Users may request data sharing with a third party or termination of this data sharing where feasible.
- The duration of the contractual relationship between the User and Lenovo as a prospective data holder depends on the nature of the product or service. Users may terminate this relationship in accordance with the applicable terms and conditions.
- Users have a right to lodge a complaint to the designated competent supervisory authority if they believe that any provision of Chapter II of the EU Data Act has been infringed. However, users are encouraged to reach out to us in case of any concerns.

Security and Confidentiality

We apply appropriate technical and organizational safeguards, including encryption, access control, and anonymization where relevant. Proprietary trade secrets are protected, while still ensuring users' rights to access and portability.

Contact

For questions about this Declaration or to exercise data access rights under the EU Data Act, please contact: privacy@motorola.com. You can also contact the Lenovo entity in the country in which you purchased the product or service.