PRIVACY POLICY

Privacy Notice for Ericsson work force and/or any person ("User") downloading and using Ericsson Device Analytics (EDA)

1 General

We understand that privacy is an important issue for Users of the Ericsson Device Analytics application. The following information is designed to help users understand what information we collect, and how we handle and use personal data collected via the Device Analytics application (‘Application’).

The Application is intended only for authorized enterprise users.

1.1 Who is collecting personal data?

The personal data is being collected by the Ericsson AB, 16480 Stockholm, Sweden (Ericsson) as the Controller.

For more information, rectification, erasure, portability, or complaints to supervisory authorities about the processing of personal data please see under Section 6 (Your rights) or contact an Ericsson Data Protection Officer or HR Direct if you are Ericsson workforce.

1.2 Why is personal data collected and processed (purpose and grounds for processing)?

Such personal data is collected and processed:

(i) to provide Ericsson Device Analytics service (contractual obligation under Terms of Use for this Application)
(ii) to conduct research aiming at improving Ericsson's current and future products and services (legitimate interest)
(iii) because some processing may be necessary in order to comply with legal obligations, usually in relation to national agencies and supervisory authorities (legal obligation)

Any processing of the User's personal data will be in compliance with applicable law. Ericsson confirms that it will not access the content stored on the User's devices for other purposes than

described above. Ericsson will make every reasonable effort to ensure that the information will be maintained in a secure environment.

1.3 What type of personal data is collected or processed?

Personal data being processed may include but is not limited to :

- User's identity Demographic information: company name may be included in activation code
- Location information: location (GPS) - location data that describes the precise geographic location of your device (“Precise Location Data”).
- Internet connection means, such as internet service provider (“ISP”), mobile operator, WiFi connection, International Mobile Subscriber Identity (“IMSI”) and
- International Mobile Equipment Identity (“IMEI”) e.g. Device manufacturer, model, OS version or other software used)
- Sensor information (humidity, light, pressure, temperature)
- Network Cell Signal Information
- Device type and software used
- Log files, which may contain device information (IMEI, Device manufacturer, model, OS version) and mobile traffic data (location, network performance, cell information). Log files are only shared by the enterprise user towards EDA Solution Support team in case of malfunctions or unexpected behavior.

1.4 Does Ericsson collect sensitive data?

As a general rule Ericsson does not process sensitive personal information about racial or ethnic origin, political opinion, philosophical beliefs, religion, sexual orientation, genetic data, health, criminal records or union membership unless required by law. Such data will not be collected via this Application.

1.5 Where does the personal data that’s being processed come from?

The personal data generally originates from data subjects. When downloaded and installed (only after successful activation takes place via a valid activation code) the App will connect to Ericsson's servers and Ericsson's servers will, through the Application, gain access to information about the User and the User's device which may consist of personal data.

Information about the geographical location is obtained from your mobile phone when it is turned on, based on the phone's internal information and/or GPS functionality, including details about your phone model, manufacturer and serial number. The information is time stamped.

The main feature of the Application is the correlation of your current geographical position with network speed test performance, radio and sensor information. The App will still gather the above information even when it is running in the background.

1.6 Is there a way of automated decision making or profiling done in the processing that Ericsson does?

There is no automated decision making nor profiling involved in the processing.

1.7 Who has access to personal data?

Personal data may, depending on category of data, sensitivity, role and geographical area, be viewed by support staff, administrators, IT staff, security personnel and others.[KO10] [AM11] Only Ericsson personnel can access data stored within this Application.

Access will be granted on a need to know basis with geographical and legal limits taken into account.

1.8. What Information we disclose to Third Parties

Ericsson will not knowingly disclose personal data to third parties unless required to do so in order to comply with any valid legal process, such as a search warrant, subpoena, statute, court order, or if necessary or appropriate to address an unlawful or harmful activity.

However, Ericsson may share aggregate (not personally identifiable) information with its business partners or other third parties.

All individuals with access to personal data, including third parties (if any), are required to protect and handle the information in accordance with legal and contractual obligations as well as instructions from Ericsson.

2 Examples of personal data that may be processed without consent.

2.1 Data requested by different government agencies

The processing of data required in conjunction with the exercise of public authority from, for example, the Tax Agencies and the National Insurance Agencies is allowed without consent.

2.2 Incidents

Personal data can be processed in connection with security incident reporting and handling.

3 International data transfers

Your data is stored in a location within the European Union. However, since Ericsson Group is present around the globe personal data may be transferred across international borders to Ericsson entities in other countries. Please click here for a list of Ericsson entities.

The data is transferred under both data transfer agreements and binding corporate rules (BCR) which secure an adequate data protection level in accordance with GDPR and other relevant privacy laws. A summary of Ericsson's BCR can be accessed through this link.

Personal data may also be transferred to third parties in countries outside the EU/EEA if it is needed in order for Ericsson to establish, defend and exercise legal claims or Ericsson has entered into the European Commission's Model Contracts for the transfer of personal data to third countries.

4 How long do we keep the data (retention)?

Personal data may not be kept longer than necessary as regards the purpose of processing. Irrelevant or incorrect data may not be saved but must rather be corrected, updated, or erased.

Personal data collected via this Application will be kept for 5 years.

You can, at any time, stop being located and stop providing any other personal data by uninstalling the application. You may exercise your rights to access your data and request deletion of your data by contacting Ericsson at: EDA.solution.support@ericsson.com.

5 Security

Privacy and security are important elements in the products and services delivered by Ericsson, and we align product and business processes to ensure that human rights aspects of privacy are respected throughout our business operations.

The user identity is treated in a secure manner meaning the user identifier is hashed and therefore not easy to retrieve. For further information regarding the process of the User's personal data, please contact Ericsson at EDA.solution.support@ericsson.com.

Encryption at rest and in transit:

- Encryption at rest - data at rest is encrypted. Common forms of encryption at rest include, but are not limited to: database encryption, hard drive encryption, etc. Data are encrypted in Azure (all disks/database in Azure are encrypted)

- Encryption in transit - assurance that data in motion is encrypted. Common encrypted protocols include, but are not limited to: HTTPS, etc. Authentication encryption at login is ensured via https is done.

6 Your rights

You have the right to access and rectification or erasure of the personal data, the right for restriction of processing of personal data as well as the right to data portability. You are also entitled to object to processing of your personal data that is based on Ericsson's legitimate interest. If you object to the processing, we can no longer process your personal data, unless we demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or if processing is needed for the establishment, exercise or defense of legal claims.

Not all personal data that is being processed can be erased, restricted, or made portable.

If you have given your consent to processing of your personal data for an explicit purpose you may always withdraw your consent.

For further information regarding data protection and privacy you can contact an Ericsson Data Protection Officer. Data Subjects who wish to file a request or a complaint pertaining to their Personal Information can send an email to ericsson.group.privacy@ericsson.com

Ericsson staff with direct access to HR Direct who wish to file a complaint or a request pertaining to their Personal Information shall contact HR Direct.

You also have the right to complain about the data processing with your local data protection supervisory authority or the Swedish Data Protection Authority.

8 Q&A

8.1 What is personal data?

All information that can be directly or indirectly linked to a living, natural person is considered personal data. The exact legal meaning can vary from country to country. The information does not necessarily have to consist of text or numbers; rather, it can also consist of photos, videos, images or audio recordings that can be associated with a person.

The terms “personally identifiable information (PII)”, “personal data”, “private information”, “sensitive Personal Information”, “special categories of data” and “legally protected information” are often used interchangeably to refer to information relating to individuals. For the purposes of data privacy at Ericsson, the all-inclusive terms “Personal Information” or “Personal Data” shall be used where appropriate.

8.2 How does Ericsson protect my personal data?

Ericsson has set up a Privacy Framework by adopting and executing a set of privacy related documents. These documents describe 1) Ericsson’s privacy commitments and 2) the rules for handling Personal Information to achieve the privacy commitments (the rules for handling

Personal Information processed by Ericsson or in Ericsson’s custody, including that of partners, employees, customers and end-users such as customer’s subscribers).

Ericsson Security policies and documents ensure that information assets, including Personal Information, are protected according to the sensitivity of the information, available when needed and protected from unauthorized access or modification.

8.3 What are the rules for Ericsson workforce who intend to process personal data?

Most countries have laws that limit how personal data can be collected and used. Such laws also require personal data to be protected from unauthorized disclosure through technical security measures and limitations of access rights. Transfer of personal data to other countries or access to personal data from other countries is often restricted and subject to fulfillment of special conditions.

In addition, usage limitations and security instructions apply through contractual undertakings when Ericsson receives or has access to personal data from business partners or others. Even if there is no legal or contractual limit, Ericsson respects the privacy of individuals and always acts ethically.

Ericsson aligns business processes to ensure that human rights aspects of privacy are respected.