CONTROLLER BINDING CORPORATE RULES

Abstract

This Group Directive is a set of Controller Binding Corporate Rules (hereafter referred to as the "**C-BCRs**"), that governs all international transfers of Personal Data between Ericsson Companies that are BCR Members.

Integrity, transparency, and responsibility characterize the way the Ericsson Group conducts its business. We recognize our responsibility to respect data protection rights and to put in place appropriate standards of data protection when processing Personal Data.

The requirements laid out in the C-BCRs are designed to help the Ericsson Group to comply with the requirements under the EU General Data Protection Regulation 2016/679 (GDPR) and to provide appropriate safeguards to transfers of Personal Data between all BCR Members globally.

Application

The C-BCRs apply to all BCR Members, including their Employees and External Workforce involved in the processing of Personal Data or in the development of internal tools or services used to process Personal Data where a BCR Member acts as Controller (separately or jointly with another BCR Member) or as Processor to another BCR Member (internal Processors).

These rules are applicable to the processing of Personal Data by wholly or partly automated means, or when it forms (or is intended to form) part of a filing system.

Purpose

Protecting privacy and ensuring the secure processing of Personal Data, particularly in connection with global transfers of Personal Data, is of utmost importance to the Ericsson Group.

Promote the right to privacy and freedom of expression

In accordance with Ericsson Code of Business Ethics, Ericsson respects and promotes human rights throughout our work, including by providing access to communication and information around the world.

Ericsson fundamentally believes that our hardware, software, services and solutions bring positive change to people. At the same time, Ericsson works to mitigate and minimize the risk of potential misuse of our technology.

Ericsson does this by conducting human rights due diligence in sales engagements, to assess, prevent and mitigate potential negative impacts on human rights.

Ericsson also advocates strongly for freedom of expression and privacy protections. This includes raising concerns about new legislative, administrative, license or law enforcement rules if they may negatively impact individuals' freedom of expression or their right to privacy.

As part of its commitment to respecting privacy and security, the Ericsson Group carries out its business in compliance with applicable data protection laws and regulations. The C-BCRs help to clearly define the rules applicable to all BCR Members for processing Personal Data in order to ensure a consistent and high level of protection for Personal Data in connection with transfers between BCR Members.

Contents

1. Directive

1.1 Introduction

Data protection terms in the C-BCRs shall have the same meaning as they do in the GDPR. The terminology table in Section 11 contains definitions of the main terms.

The GDPR requires transfers of Personal Data to countries outside of the EU/EEA that do not afford an adequate level of data protection to be afforded appropriate safeguards for the protection of privacy, fundamental rights and freedoms of individuals, and the exercise of corresponding rights.

Binding Corporate Rules are one way of providing appropriate safeguards. They can be used to legally transfer (including the granting of access) Personal Data between different entities

within the same corporate group. The C-BCRs help to ensure that the same level of protection for Personal Data is applied by all BCR Members.

The Ericsson Group has implemented a groupwide data protection compliance program and has appointed (i) a Group Data Protection Officer ("GDPO") and (ii) a Group Privacy Head/Chief Privacy Officer, whose respective teams are involved in the oversight and to ensure compliance, and implementation of the Ericsson Privacy Policy, respectively.

The Chief Privacy Officer and Privacy Team and the office of the GDPO as it might be the case, are responsible for the oversight of the Ericsson Privacy Policy and reports to the highest management level of Ericsson. The Chief Privacy Officer or GDPO can inform the highest management level if any questions or problems arise during the performance of their duties. In addition, there is a Head of Product Privacy working specifically with Privacy by Design and product privacy questions and dedicated resources working specifically with questions related to Human Resources.

1.2 Binding nature

1.2.1 Duty to respect the C-BCRs

All BCR Members, including their Employees and External Workforce, have a duty to respect the C-BCRs.

Ericsson Group's internal policies highlight the commitment from the Board of Directors and the Executive Management to ensure compliance with the C-BCRs.

All BCR Members, including their Employees and External Workforce, have a duty to follow the instructions on data processing given by the BCR Member acting as Controller, including security and confidentiality measures.

1.2.2 Binding effect on BCR Members

In order to be bound by the C-BCRs, the BCR Members have entered into the Intra-Group Agreement. Each change, revision, amendment, or addition to the C-BCRs shall automatically apply to each BCR Member.

No data transfer can be made under the C-BCRs from one Ericsson Company to another until the recipient Ericsson Company has signed the Intra-Group Agreement and become a BCR Member.

1.2.3 Binding effect on Employees and External Workforce

The C-BCRs are binding upon Employees and External Workforce. Everyone working for the Ericsson Group must acknowledge that they have read and understood the Ericsson Code of Business Ethics, to which they must adhere. In addition, Employees and External Workforce must sign individual non-disclosure agreements. The Code of Business Ethics includes an instruction to follow the Ericsson Group's policies, directives and instructions as well as local

directives and instructions, of which the C-BCRs are one. Failure to do so may result in disciplinary action including termination of employment and/or civil and criminal liability.

In accordance with Ericsson Code of Business Ethics, Ericsson protects Personal Data and supports global efforts to safeguard it. Ericsson adheres to global privacy principles and applicable laws, including the GDPR. Ericsson also has these C-BCRs and contractual agreements which regulate how we process and share data.

1.3 Material scope of the C-BCRs

The C-BCRs apply to all transfers of Personal Data between BCR Members, including onward transfers to BCR Members outside the EU/EEA.

The Ericsson Group primarily processes Personal Data relating to Employees, External Workforce, visitors, shareholders, customer representatives, providers, candidates and other business related third parties. Processing takes place across the Ericsson Group by the different Ericsson Companies; including but not limited to internal units, Geographical Organizations, and the following group functions:

(a) Human Resources (People Function)

(b) Finance

(c) Legal and Compliance

(d) Corporate Audit

(e) Security

(f) Sourcing

(g) Sales

(h) Marketing

Information related to the nature of the Personal Data transferred and the processing operations are described in Annex 2.

The Ericsson Group's intra-group data flows are global in nature, reflecting the interconnected and international presence of its business operations. However, the major part of Personal Data is exported by Ericsson AB in Sweden to the Ericsson Group's intra-group support centres located in China, India, Philippines, Mexico, Romania, Spain and the U.S. Transfers are mainly in the form of remote access to servers located in the EEA.

2. Data protection principles

2.1 Lawfulness and fairness

BCR Members shall only process Personal Data in a lawful and fair manner and when permitted to do so in compliance with a legal basis under applicable data protection laws. Below is an exhaustive list of all legal basis for processing that the BCR Members intend to rely upon.

(a) The Data Subject has unambiguously given consent to the processing;

(b) The processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract;

(c) The processing is necessary for compliance with a legal obligation to which the Controller is subject;

(d) The processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;

(e) The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller; or

(f) The processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

2.2 Transparency

BCR Members shall only process Personal Data in a transparent manner and shall inform Data Subjects how their Personal Data will be used. Information will usually be provided by way of a privacy notice.

Where a BCR Member obtains Personal Data from a source other than the Data Subject, the BCR Member shall provide this information to the Data Subject within a reasonable period after obtaining the Personal Data, but at the latest within one month, having regard to the specific circumstances in which the Personal Data are processed or, if the Personal Data are to be used for communication with the Data Subject, at the latest at the time of the first communication to that Data Subject, or, if it is to be disclosed to a third party, no later than the time at which the data is first disclosed. This rule is applicable unless there is a legitimate basis for not doing so, such as legal proceedings, taxation purposes, preventing or detecting a crime, where withholding information is necessary to safeguard national security or defence, or where otherwise permitted by law.

Information to Data Subjects with respect to BCR Members' processing of their Personal Data shall fulfil the requirements of the GDPR.

2.3 Purpose limitation

BCR Members shall only collect Personal Data for specific, explicit, and legitimate purposes and not further process such Personal Data in a manner which is incompatible with those initial purposes.

2.4 Data minimisation and accuracy

BCR Members shall take necessary measures to ensure that Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, and that data are accurate and, where necessary kept up to date. They must take all reasonable steps to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

2.5 Storage limitation

BCR Members must not keep Personal Data in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data are processed and according to the relevant national laws.

2.6 Special Categories of Personal Data

Special Categories of Personal Data are subject to specific legal protection under the GDPR and may only be processed when an exemption to the general prohibition to process such Personal Data applies. When applicable, such categories of Personal Data and appropriate security measures for the processing of such Personal Data shall be specifically described by the relevant BCR Member. Below is an exhaustive list of all exemptions for processing special categories of Personal Data that the BCR Members intend to rely upon.

(a) The Data Subject has given explicit consent to the processing of Special Categories of Personal Data, except where national applicable laws prohibit it;

(b) The processing is necessary for the purposes of carrying out the obligations and specific rights of the Controller in the field of employment and social security and social protection law in so far as it is authorized by EU or member state law or a collective agreement pursuant to member state law providing for adequate safeguards;

(c) The processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving consent;

(d) The processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a

political, philosophical, religious or trade union aim and on the condition that the processing relates solely to the members or to former members of the body or persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed outside that body without the consent of the Data Subjects;

(e) The processing relates to Personal Data which are manifestly made public by the Data Subject;

(f) The processing of Special Categories of Personal Data is necessary for the establishment, exercise or defence of legal claims;

(g) The processing is necessary for reasons of substantial public interest;

(h) The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care, and where the Personal Data is processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy;

(i) The processing is necessary for reasons of public interest in the area of public health; or

(j) The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

BCR Members shall only process Personal Data relating to criminal convictions and offences or related security measures when such processing is authorised by EU or member state law providing for appropriate safeguards for the rights and freedoms of Data Subjects.

2.7 Security, integrity and confidentiality

BCR Members shall adhere to the Ericsson Group standard security measures as set forth in applicable group steering documents, including appropriate technical and organisational measures. Such measures are designed to protect Personal Data against e.g. unauthorised or unlawful processing, accidental loss, destruction, or damage.

Security measures will be designed with due regard for the particular risks presented by the processing. They may include:

(a) The pseudonymization and/or encryption of Personal Data;

(b) Measures that ensure the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;

(c) Measures that ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

(d) Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Access rights to Personal Data are authorized individually on a need-to-have basis according to the Ericsson Privacy Policy. Employees and External Workforce who access Personal Data shall meet confidentiality obligations as specified by applicable non-disclosure agreements.

Ericsson's Information Security Management System is currently globally certified to ISO/IEC 27001.

All data processing activities conducted by external or internal Processors or sub-Processors on behalf of a BCR Member must be subject to a written data processing agreement. Such written agreement shall set out the subject-matter, duration, nature and purpose of the processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of the Controller. The written agreement shall also stipulate, in particular, that the Processor:

(a) processes the Personal Data only on documented instructions from the Controller;

(b) ensures that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required to assess and implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk;

(d) does not engage a sub-Processor without prior written authorisation of the Controller and that the Processor, in case of such authorisation and when engaging a sub-Processor, imposes the same data protection obligations as set out in the written agreement with the Controller on that sub-Processor by way of a contract;

(e) assists the Controller by appropriate technical and organisational measures for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights;

(f) assists the Controller in ensuring compliance with the obligations to (i) assess and implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk; (ii) notify a Data Breach to the Supervisory Authority; (iii) communicate a Data Breach that is likely to result in a high risk to the rights and freedoms of natural persons to Data Subjects; (iv) carry out a Data Protection Impact Assessment; and (v) consult the Supervisory Authority prior to processing where a Data Protection Impact Assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk;

(g) at the choice of the Controller, deletes or returns all Personal Data to the Controller after the end of the provision of services relating to processing; and

(h) makes available to the Controller all information necessary to demonstrate compliance with the obligations laid down in the above items (a)—(g) and allow for, and contribute to, audits conducted, or mandated by, the Controller.

2.8 Duty to cooperate with the Controller

BCR Members acting as internal Processors must comply with intra-group instructions on processing, transfer, security, breach reporting, and termination, and promptly inform Security Function within Ericsson Group and the BCR Member acting as Controller should compliance not be achievable.

BCR Members acting as internal Processors also have a duty to assist BCR Members acting as Controllers to comply and to demonstrate compliance with applicable data protection laws (such as its obligation to respect Data Subject rights, to handle complaints, or to reply to enquiries and/or investigations from the Supervisory Authorities).

2.9 Data Breach notification

BCR Members shall notify a Data Breach as follows:

- without undue delay, to Ericsson AB and the GDPO or the Chief Privacy Officer as it might be the case, as well as to the BCR Member acting as a Controller, and respective DPO, when a BCR Member acting as a Processor becomes aware of a Data Breach. Similarly, BCR Members acting as sub-processors should inform the Processor of a suspected or detected Data Breach;

- without undue delay, and, where feasible, not later than 72 hours after having become aware of the Data Breach to the Competent Supervisory Authority, unless the Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons; and

- without undue delay to Data Subjects, where the Data Breach is likely to result in a high risk to their rights and freedoms.

Data Breaches should be documented (including the facts relating to the Data Breach, its effects and the remedial action taken). Such documentation should be made available to the Competent Supervisory Authority upon request.

The Ericsson Group has implemented processes with mandatory instructions to ensure that security, Data Breaches, and related incidents are properly reported and managed in order to avoid unnecessary damage and cost and to comply with legislation, rules, and contractual obligations.

2.10 Restrictions on transfers and onward transfers to external Processors and Controllers (not members of the Ericsson Group)

BCR Members shall ensure that appropriate safeguards are used for all transfers of Personal Data out of the EU/EEA when required. BCR Members may only transfer Personal Data to external Controllers and Processors outside the EU/EEA if at least one of the following applies:

(a) The destination country has been deemed to afford adequate protection by the European Commission;

(b) The transfer is subject to the EU standard contractual clauses. It is the responsibility of the BCR Member, if needed with the help of the third party, to assess whether the level of protection required by EU law is respected in the third country, in order to determine if the guarantees provided by the EU standard contractual clauses can be complied with in practice. If this is not the case, the third party must implement supplementary measures to ensure an essentially equivalent level of protection as provided in the EU/EEA; or

(c) other appropriate safeguards, such as a legally binding and enforceable instrument between public authorities or bodies, standard data protection clauses adopted by a Supervisory Authority and approved by the Commission, or an approved code of conduct or certification mechanism together with binding and enforceable commitments of the Controller or Processor in the third country to apply the appropriate safeguards, including as regards Data Subjects' rights.

In other limited circumstances, BCR Members may transfer Personal Data to a third party outside the EU/EEA without having to implement the above measures where one of the following conditions is met:

(a) The Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfer for the Data Subject due to the absence of an adequacy decision and appropriate safeguards;

(b) The transfer is necessary for the performance of a contract between the Data Subject and the BCR Member or the implementation of pre-contractual measures taken at the Data Subject's request;

(c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the BCR Member and another natural or legal person;

(d) The transfer is necessary for important reasons of public interest;

(e) The transfer is necessary for the establishment, exercise or defence of legal claims;

(f) The transfer is necessary in order to protect the vital interests of the Data Subject or other persons, where the Data Subject is physically or legally incapable of giving consent; or

(g) The transfer is made from a register which according to the EU or member state law is intended to provide information to the public and which is open to the consultation by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or member state law for consultation are fulfilled in the particular case.

In addition, where a transfer could not be based on any of the conditions set out above, a transfer to a third country may take place only if the transfer is not repetitive, concerns only a limited number of Data Subjects, is necessary for the purposes of compelling legitimate interests pursued by the BCR Member which are not overridden by the interests or rights and freedoms of the Data Subject, and the BCR Member has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of Personal Data. The BCR Member acting as Controller shall, in such case, inform the Supervisory Authority of the transfer and inform the Data Subject of the transfer and on the compelling legitimate interests pursued.

2.11 Restrictions on transfers to BCR Members

The BCR Members will use the C-BCRs as a tool for transfers only where they have assessed that the law and practices in the third country of destination applicable to the processing of the Personal Data by the BCR Member acting as Data Importer, including any requirements to disclose Personal Data or measures authorising access by public authorities, do not prevent it from fulfilling its obligations under these C-BCRs. If necessary, supplementary contractual, technical or organisational safeguards must be implemented by the BCR Member in a third country to ensure an essentially equivalent level of protection as provided in the EU/EEA. Where any safeguards, in addition to those envisaged under the C-BCRs should be put in place, Ericsson AB, as liable entity and the GDPO, the Chief Privacy Officer, local DPOs, Privacy managers and any other function to work for putting it in place will be informed and involved in such assessment.

In assessing the laws and practices of the third country which may affect the respect of the commitments contained in the C-BCRs, the BCR Members will have taken due account, in particular, of the following elements:

(a) The specific circumstances of the transfers or set of transfers, and of any envisaged onward transfers within the same third country or to another third country, including:

(i) purposes for which the Personal Data are transferred and processed;

(ii) types of entities involved in the processing (the Data Importer and any further recipient of any onward transfer);

(iii) economic sector in which the transfer or set of transfers occur;

(iv) categories and format of the Personal Data transferred;

(v) location of the processing, including storage; and transmission channels used; and

(vi) transmission channels used.

(b) The laws and practices of the third country of destination relevant in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorising access by such authorities and those providing for access to these data during the transit between the country of the Data Exporter and the country of the Data Importer, as well as the applicable limitations and safeguards.

(c) Any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under the C-BCRs, including measures applied during the transmission and to the processing of the Personal Data in the country of destination.

The assessment above is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR, are not in contradiction with the C-BCRs.

Where effective supplementary measures could not be put in place, the transfers at stake will be suspended or ended.

The BCR Members must document appropriately the assessment, as well as supplementary measures selected and implemented, and make it available to the Competent Supervisory Authority on request. Provisions established by the Ericsson Group for performing this assessment (such as tools, instructions on the performance of and evaluation) must be observed.

3. Data Subjects' rights

Data Subjects whose Personal Data is processed by BCR Members have certain data protection rights which they may exercise on request. These include:

(a) The right to be ***informed*** by the Controller of the processing of their Personal Data, including about the categories of Personal Data; the purposes of and legal basis for the processing of the Personal Data; the recipients or categories of recipients of the Personal Data; that the Personal Data is to be transferred to a third country or international organisation and the basis for such transfer; the period or criteria used to determine the period for which the Personal Data will be stored; the rights of Data Subjects; the existence of, and the significance and the envisaged consequences of any automated decision-making; whether the Data Subject is obliged to provide the Personal Data; and, when the Personal Data have not been obtained from the Data Subject, from which source it originates. The information

shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language;

(b) The right to obtain from the Controller ***confirmation*** as to whether or nor not their Personal Data are being processed, and where that is the case ***access*** to their Personal Data by a copy of the Personal Data undergoing processing, together with information about the purposes of the processing; the categories of Personal Data concerned; the recipients or categories of recipients of the Personal Data; the period or criteria used to determine the period for which the Personal Data will be stored; the rights of Data Subjects; when the Personal Data have not been obtained from the Data Subject, from which source it originates; the existence of, and the significance and the envisaged consequences of any automated decision-making; and the appropriate safeguards where Personal Data are transferred to a third country or international organisation. The communication shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language;

(c) The right to have inaccurate Personal Data ***rectified*** and, taking into account the purposes of the processing, have incomplete Personal Data ***completed***, including by means of providing a supplementary statement. The communication shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language;

(d) The right to have their Personal Data ***erased*** when they are no longer necessary for the purposes for which they were collected or otherwise processed; in case of a withdrawal of consent on which the processing was based, where there is no other legal ground for the processing; in case of an objection to the processing, where, when applicable, there are no overriding legitimate grounds for the processing; when the Personal Data have been unlawfully processed or have to be erased for compliance with a legal obligation in EU or member state law to which the Controller is subject; or when the Personal Data have been collected in relation to the offer of information society services. The right to erasure does not apply to the extent the processing is necessary for exercising the right of freedom of expression and information; for compliance with a legal obligation under EU or member state law to which the Controller is subject and which requires processing, or for the performance of a task carried out in the public interest; for reasons of public interest in the area of public health; for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or for the establishment, exercise or defence of legal claims. The communication shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language;

(e) The right to obtain ***restriction*** of processing of their Personal Data to limited purposes, when the accuracy of the Personal Data is contested (for a period enabling the Controller to verify the accuracy); when the processing is unlawful and their erasure is opposed in favor of the restriction of their use; when the Controller no longer needs the Personal Data, but the Personal Data are required by the Data Subject for the establishment, exercise or defence of legal claims; or

when the Data Subject has objected to processing, pending the verification whether the legitimate grounds of the Controller override those of the Data Subject. The communication shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language;

(f) The right to be ***notified*** of any rectification or erasure of Personal Data or restriction of processing. The communication shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language;

(g) The right to receive the Personal Data provided by them in a structured, commonly used and machine-readable format and to transmit this Personal Data to another Controller (***data portability***), including, where technically feasible, directly from one Controller to another, where the processing is based on the Data Subject's consent or on the basis that it is necessary for the performance of a contract. The communication shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language;

(h) The right to ***object*** to the processing of their Personal Data, including profiling and direct marketing, where the processing is based on it being necessary for the performance of a task carried out in the public interest or for the purposes of the legitimate interests pursued by the Controller or by a third party. In such a case, the Controller shall cease to process the Personal Data unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims. In the case of an objection to the processing of Personal Data for direct marketing purposes, the Controller always shall cease to process the Personal Data. The communication shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language;

(i) The right to not be evaluated or subject to decisions based solely on ***automated decision-making***, including profiling, which produces legal effects or similarly significantly affects the Data Subject, unless the processing is based on the data subject's explicit, alternatively that the processing is necessary for entering into, or for the performance of, a contract between the Data Subject and a Controller or is authorised by EU or member state law to which the Controller is subject, in which cases the Controller shall have implemented suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests. The communication shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language; and

(j) The right to lodge a complaint with a Supervisory Authority, as set out in Section 4.3, without prejudice to any other administrative or judicial remedy.

BCR Members shall respond to any queries or requests made by Data Subjects in relation to the above, and shall adhere to the Internal Complaint Mechanisms set out in Section 7.

4. Enforcing the BCRs - Third party beneficiary rights

4.1 Access to information about third party beneficiary rights

All Data Subjects will be provided with information on their third-party beneficiary rights, with regard to the processing of their Personal Data and on the means to exercise those rights. All Data Subjects will also be provided with up-to-date information, in a clear, intelligible and transparent way, on the scope of the C-BCRs, Ericsson Group's liability, the data protection principles, lawfulness of the processing, security and Data Breach notifications, restrictions on onward transfers and the rights of Data Subjects. The C-BCRs are part of Ericsson's Privacy Policy and as such published on the intranet for easy and unrestricted access for each and everyone within the Ericsson Group.

To ensure transparency and easy access Ericsson AB shall ensure that a copy of the C-BCRs is provided to all Employees and External Workforce via the intranet and also provide to such Data Subjects upon request. In addition, in order to ensure transparency and easy access to the C-BCRs for Data Subjects outside the Ericsson Group (i.e. not having access to the intranet) the C-BCRs shall be available on the Ericsson Group's website https://www.ericsson.com/en/legal/privacy.

All Data Subjects may also request a copy of the C-BCRs by emailing privacy.bcr@ericsson.com.

4.2 Enforceable elements of the C-BCRs

Data Subjects shall have the right to enforce the following elements of the C-BCRs as third-party beneficiaries:

(a) Data protection principles, lawfulness of processing, and security and Data Breach notifications (Section 2.1-2.10);

(b) Transparency and easy access to the C-BCRs (Section 2.2 and 4.1);

(c) Rights of information, access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction, objection to processing, right not to be subject to decisions based solely on automated processing, including profiling (Section 3);

(d) Local laws and practices affecting compliance of the C-BCRs and in case of government access requests (Section 6.5 and 6.6);

(e) Right to complain through the internal compliant mechanism of the Ericsson Group (Section 7);

(f) Cooperation duties with Competent Supervisory Authorities (Section 6.3);

(g) Liability and jurisdiction provisions (Section 5);

(h) Lawfulness and fairness (Section 2.1);

(i) Security, integrity and confidentiality (Section 2.7);

(j) Restrictions on transfers and onward transfers to external Processors and Controllers (not members of the Ericsson Group) (Section 2.10);

(k) Duty to inform Data Subjects about any update of the C-BCRs and of the list of BCR Members (Section 9);

(l) Right to judicial remedies, redress and compensation (Section 4.4); and

(m) The third-party beneficiary rights (Section 4.1 and 4.2).

Data Subjects' third-party beneficiary rights are comprised to the sections listed above and do not extend to any other sections of the C-BCRs. Moreover, third party-beneficiary rights are related to Personal Data transferred from the EU/EEA to a third country.

4.3 Right to lodge a complaint

The Data Subject shall have a right to lodge a complaint with a Supervisory Authority. The Data Subject may choose to lodge such a complaint with the Supervisory Authority in the member state of his habitual residence, place of work or place of the alleged infringement.

The Data Subject shall also have the right to lodge a complaint before the competent court of the EU member state; either where the BCR Member has an establishment or where the Data Subject has his or her habitual residence.

4.4 Right to judicial remedies

The Data Subject shall have a right to judicial remedies and the right to obtain redress and, where appropriate, compensation in case of any breach of one of the enforceable elements of the C-BCR's as set out in Section 4.2. The BCR Members accept that Data Subjects may be represented by a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of an EU member state, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their Personal Data where provided for by member state law.

5. Liability

5.1 Liability for breaches of the C-BCRs by BCR Members located in the EU/EEA

Each BCR Member in the EU/EEA accepts responsibility for and agrees to take necessary action to remedy the acts of non-compliance with the enforceable elements of the C-BCRs set

out in Section 4.2 that it commits and to pay compensation for any material or non-material damages resulting from the violation of the C-BCRs by such BCR Member.

The BCR Member has the burden of proof to demonstrate that it is not liable for the alleged breach of the C-BCRs. It may discharge itself from liability if it can prove that the Data Subject did not incur any harm that the BCR Member would be liable to compensate under the GDPR.

5.2 Liability for breaches of the C-BCRs by BCR Members located outside the EU/EEA

Ericsson AB accepts responsibility for and agrees to take necessary action to remedy acts of non-compliance with these C-BCRs by BCR Members located outside of the EU/EEA and to pay compensation for any material or non-material damages resulting from the violation of the C-BCRs by such BCR Members. Ericsson AB's liability in this regard only extends to Personal Data that have been transferred under these C-BCRs from the EU/EEA to a third country.

Any claim by a Data Subject will be subject to the jurisdiction of the national courts and Supervisory Authorities in the EU/EEA and the Data Subject will have the rights and remedies against Ericsson AB as if the violation had been caused by Ericsson AB itself in Sweden.

If Data Subjects can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of the C-BCRs, it will be for Ericsson AB to prove that the BCR Member outside of the EU/EEA was not responsible for the breach of the C-BCRs giving rise to those damages, or that no such breach took place.

6. Ericsson Group Requirements

6.1 Accountability, record of processing activities and compliance efforts

Every BCR Member acting as a Controller is responsible for and must be able to demonstrate compliance with the C-BCRs (*accountability*), including through the implementation of appropriate technical and organisational measures to ensure data protection "by design and by default" (Section 2.7 and 6.2 of these C-BCRs).

Every BCR Member must maintain a written record, including in electronic form, of all categories of processing activities carried out on Personal Data transferred under these C-BCRs. This record should be made available to the Competent Supervisory Authority/Authorities upon request.

For a BCR Member acting as a Controller, the record should include the name and contact details of the BCR Member and, where applicable, its representative and a data protection officer; information on the purposes of the processing; a description of the categories of Data Subjects and of the Personal Data; information on the categories of recipients to whom the Personal Data have been or will be disclosed; and, where applicable, information on transfers of Personal Data to a third country or an international organisation, including the

identification of that third country or international organisation and, where required, the documentation of suitable safeguards. The record shall also, where possible, include information on the envisaged time limits for erasure of the different categories of Personal Data and a general description of technical and organisational security measures implemented.

For a BCR Member acting as a Processor, the record should include the name and contact details of the BCR Member acting as a Processor and of the Controller on behalf of which the BCR Member is acting, and, where applicable, its representative and a data protection officer; information on the categories of processing carried out on behalf of the Controller; where applicable, information on transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, where required, the documentation of suitable safeguards; and, where possible, a general description of the technical and organisational security measures implemented.

Where a BCR Member's processing activities on Personal Data transferred under these C-BCRs are likely to result in a high risk to the rights and freedoms of natural persons, the BCR Member shall ensure that a Data Protection Impact Assessment is carried out. Where such Data Protection Impact Assessment indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk, the BCR Member acting as a Controller should, prior to processing, consult the Competent Supervisory Authority/Authorities.

6.2 Data protection by design and default

BCR Members shall implement appropriate technical and organisational measures, such as pseudonymization, which are designed to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the data protection requirements of the GDPR and protect the rights of Data Subjects (*data protection by design*). Such measures shall be implemented considering the state of the art, the cost of implementation, and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing (as further described in section 2.7).

BCR Members shall also implement appropriate technical and organisational measures for ensuring by default that only Personal Data which is necessary for each specific purpose is processed (*data protection by default*). This requirement applies e.g. to the amount of Personal Data collected, the extent of their processing, the period of their storage and their accessibility.

6.3 Mutual assistance and cooperation with Competent Supervisory Authorities

BCR Members shall cooperate and assist each other to handle a request or complaint from a Data Subject or an investigation or inquiry by Competent Supervisory Authorities in the EU/EEA.

BCR Members shall cooperate with, accept to be audited and to be inspected, including where necessary on-site, by the Competent Supervisory Authorities, and take into account the advice of, as well as abide by the decisions of, these Competent Supervisory Authorities on any issues related to the C-BCRs. This commitment does not limit BCR Members from challenging such advice or decision in court or other applicable instances when deemed appropriate and necessary.

BCR Members shall upon request provide the Competent Supervisory Authorities with any information about the processing operations covered by the C-BCRs.

Any dispute related to the Competent Supervisory Authorities exercise of supervision of compliance with the C-BCRs will be resolved by the courts of the member state of that Supervisory Authority, in accordance with that member state's procedural law. The BCR Members agree to submit themselves to the jurisdiction of these courts.

6.4 Relationship between national laws and the C-BCRs

Where the local legislation, for instance EU legislation, requires a higher level of protection for Personal Data it will take precedence over the C-BCRs. In any event, Personal Data shall be processed in accordance with applicable data protection laws, including local laws and regulations, in particular Articles 5 and 6 of the GDPR.

Nothing in the C-BCRs shall prevent a BCR Member from processing Personal Data or performing any other act that would otherwise be legally permissible under the GDPR.

6.5 Actions in case of national legislation affecting compliance of the C-BCRs

A BCR Member, acting as Data Importer, must promptly notify the Data Exporter and Ericsson AB if, when using these C-BCRs as a tool for transfers, and for the duration of the BCR membership, it has reasons to believe that it is or has become subject to laws or practices that would prevent it from fulfilling its obligations under the C-BCRs, including following a change in the laws in the third country or a measure (such as a disclosure request).

Upon verification of such notification, the BCR Member acting as Data Exporter, along with Ericsson AB and the contact for these C-BCRs, should commit to promptly identify supplementary measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the BCR Member acting as Data Exporter and/or Data Importer, in order to enable them to fulfil their obligations under the C-BCRs. The same applies if a BCR Member acting as Data Exporter has reasons to believe that a BCR Member acting as its Data Importer can no longer fulfil its obligations under this C-BCRs.

Where the BCR Member, acting as Data Exporter, along with Ericsson AB and the contact for these BCRs as included in section 12, assesses that the C-BCRs – even if accompanied by supplementary measures – cannot be complied with for a transfer or set of transfers, or if instructed by the Competent Supervisory Authority, it commits to suspend the transfer or set

of transfers at stake, as well as all transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the transfer is ended.

Following such a suspension, the BCR Member acting as Data Exporter has to end the transfer or set of transfers if the C-BCRs cannot be complied with and compliance with the BCR is not restored within one month of suspension. In this case, Personal Data that have been transferred prior to the suspension, and any copies thereof, should, at the choice of the BCR Member acting as Data Exporter, be returned to it or destroyed in their entirety.

Ericsson AB and the contact for these BCRs, as stated in section 12 will inform all other BCR Members of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of transfers is carried out by any other BCR Member or, where effective supplementary measures could not be put in place, the transfers at stake are suspended or ended.

BCR Members acting as Data Exporters undertake to monitor, on an ongoing basis, and where appropriate in collaboration with BCR Members acting as Data Importers, developments in the third countries to which the Data Exporters have transferred Personal Data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

6.6 Obligations of the Data Importer in case of government access requests

Without prejudice to the obligation of the BCR Member acting as Data Importer to inform the Data Exporter of its inability to comply with the commitments contained in the C-BCRs (see Section 2.11 and 6.5 above), the BCR Member acting as Data Importer will:

(a) promptly notify the Data Exporter and, where possible, the Data Subject (if necessary, with the help of the Data Exporter) if it:

(i) receives a legally binding request by a public authority under the laws of the country of destination, or of another third country, for disclosure of Personal Data transferred pursuant to the C-BCRs; such notification will include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided;

(ii) becomes aware of any direct access by public authorities to Personal Data transferred pursuant to the C-BCRs in accordance with the laws of the country of destination; such notification will include all information available to the Data Importer.

(b) if prohibited from notifying the Data Exporter and/or the Data Subject, use its best efforts to obtain a waiver of such prohibition, with a view to communicate as much information as possible and as soon as possible, and will document its best efforts in order to be able to demonstrate them upon request of the Data Exporter.

(c) provide the BCR Member acting as Data Exporter, at regular intervals, with as much relevant information as possible on the requests received (in particular,

number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If the Data Importer is or becomes partially or completely prohibited from providing the Data Exporter with the aforementioned information, it will, without undue delay, inform the Data Exporter accordingly.

(d) preserve the abovementioned information for as long as the Personal Data are subject to the safeguards provided by the C-BCRs, and shall make it available to the Competent Supervisory Authority upon request.

(e) review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and will challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law, and principles of international comity. The Data Importer will, under the same conditions, pursue possibilities of appeal.

(f) when challenging a request, seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It will not disclose the Personal Data requested until required to do so under the applicable procedural rules.

(g) document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Data Exporter. It will also make it available to the Competent Supervisory Authorities upon request.

(h) provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

Any transfer of Personal Data by a BCR Member to any public authority cannot in any case be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

7. Internal complaint mechanisms

7.1 Complaints

Any Data Subject is able to exercise their rights under the C-BCRs and to file a complaint about a BCR Member by using the complaints mechanism described in this Section 7.

A Data Subject who wishes to file a complaint or a request to a BCR Member is encouraged to do so by sending an email in written form to privacy.bcr@ericsson.com, or by mailing the Chief Privacy Officer at Ericsson, Torshamnsgatan 21164 80 Stockholm, Sweden, and, additionally, in countries where local contacts for privacy related matters exist, to such local contact or

contacts as per the following link https://www.ericsson.com/4abd8a/assets/local/legal/data-protection-officer-list.pdf.

Such complaints or requests shall be processed in accordance with Ericsson Group's tools and processes and, for BCR Members acting as Processors, communicated to the relevant BCR Member acting as Controller without undue delay.

Ericsson Group will handle complaints by Data Subjects according to the following procedure:

(a) When complaints are received, they will be handled by Ericsson Privacy Advisor, including the GDPO and/or the relevant DPO, and the Data Subject will be provided with information on actions taken to the complaint without undue delay and always within one (1) month. An extension of up to two (2) further months may be granted due to the volume or complexity of a given request/requests. In such cases the Data Subject shall be informed of the delay within one (1) month of the receipt. Upon submission of a complaint, the Data Subject will receive an acknowledgement, and will be provided with an expected timeframe for handling of the complaint.

(b) The Data Subject will be informed about the consequences in the event of delays for the reply to the complaint, in case of rejection of the complaint and in case the complaint is considered justified. The Data Subject will also be informed of the recourse available in the event he/she is not satisfied by the response, such as the right to lodge a claim before the relevant court(s) and/or Supervisory Authorities. However, this right is not dependent on the Data Subject having used the complaint handling process beforehand.

7.2 Report incidents

All Employees are required to report any suspected or observed security and privacy incidents by submitting them to the Security Management Incidents System (SIMS). This ensures that the incident handling process is properly initiated. Once a new incident is logged in SIMS, it is automatically assigned to case handlers based on the reporter's country location.

The assigned case handler is responsible for assessing whether the incident falls within their area of responsibility. If it does not, the case should be redirected to the appropriate organisation. The case handler is tasked with managing and handling security incidents, as well as escalating them when necessary.

The Global Data Protection Officer (GDPO), Chief Privacy Officer, Data Protection Officer (DPO) (https://www.ericsson.com/4abd8a/assets/local/legal/data-protection-officer-list.pdf), or Privacy Advisor will assist the BCR Member in evaluating the severity of the incident and recommending the next steps. The BCR Member must adhere to the requirements outlined in Section 2.9.

7.3 Taking action

Data Subjects are entitled to file a cause of action before a court or lodge a complaint before a Supervisory Authority as set out in Section 7.1. In these situations, Data Subjects that are Employees of Ericsson Group receiving information of the action from or on behalf of the Data Subject or the Supervisory Authority shall send an e-mail about the cause of action or complaint to privacy.bcr@ericsson.com

8. Compliance and supervision of compliance

8.1 Audit program

The Ericsson Group has implemented a program that provides for regular audits and if there are indications of non-compliance to ensure verification of compliance with the C-BCRs. The audit program covers all aspects of the C-BCRs (for instance, applications, IT systems, databases that process Personal Data, or onward transfers, decisions taken as regards mandatory requirements under national laws that conflict with the C-BCRs, review of the contractual terms used for the transfers out of the Ericsson Group to Controllers or Processors, corrective actions, etc.), including methods and action plans ensuring that corrective actions have been implemented. Not all aspects of the C-BCRs will be monitored each time a BCR Member is audited, but all aspects of the C-BCRs are monitored at appropriate regular intervals for that BCR Member.

The GDPO decides on the annual audit plan for C-BCRs. On the basis of the risks posed by the processing activities covered by the C-BCRs to the rights and freedoms of data subjects, it has been determined that regular audits shall be performed at least annually. BCR Members may also be subject to specific, ad hoc, audits if there are indications of non-compliance with the C-BCRs or if otherwise requested by a Privacy Officer or function, any unit in the scope of their privacy tasks, or any other competent function in the organisation.

Audits will be conducted by, or under the leadership of, the GDPO. Measures designed to guarantee and safeguard the autonomy and independence of the GDPO as to the performance of the duties related to these audits have been implemented to ensure that no conflict of interest arises. External auditors may be engaged for conducting audits where appropriate to meet resource demands and/or to ensure independence. In addition, Group Function Corporate Audit may at all times audit any aspect of compliance with the internal governance framework, including the C-BCRs.

Results of audits along with progress on resolving audit findings shall be communicated to the following: (i) the executives and board of the BCR Member subject to the audit, (ii) the Privacy Officer or function, and (iii) the board of the Ericsson Group Liable Member.

Competent Supervisory Authorities can have access to the results of any audit reports by BCR Members upon request. BCR Members will immediately inform the GDPO and cooperate fully and transparently with the Competent Supervisory Authority without undue delay in the fulfilment of any such request.

8.2 Training program

According to Ericsson Privacy Policy appropriate and up-to date privacy trainings will be provided and required, on an ongoing basis, to Employees and External Workforce who have permanent or regular access to Personal Data or are involved in the collection of Personal Data or in the development of tools or services used to process Personal Data. This includes training specific to the C-BCRs. The training program includes mandatory privacy training for all new Employees and External Workforce members, which is subsequently conducted every three years. Additionally, targeted training is provided for specific units such as Human Resources and Sourcing. The training covers, among other things, procedures of managing requests for access to Personal Data by public authorities.

The Chief Privacy Officer, the GDPO, DPOs, and any other employee with privacy duties in the BCR member, have the responsibility to establish, maintain, and deploy appropriate training on privacy including on the C-BCRs.

8.3 Governance and responsibilities

Governance of the C-BCRs shall be part of the Ericsson Privacy Policy.

The Ericsson Group has appointed a Chief Privacy Officer, a GDPO and DPOs where required under relevant regulations, and BCR Members have additionally appointed specific persons such as Data Protection Advisors, Privacy Managers and Advisors, and Privacy Officers with responsibility to monitor compliance with the C-BCRs. These roles enjoy the highest management support for carrying out their tasks. The Chief Privacy Officer, GDPO and designated DPOs, as well as other privacy professionals, may be directly contacted. The Ericsson Group is committed to publish their contact details.

Considering the relevance of the Personal Data processed pertaining to human resources matters, the Ericsson Group has appointed dedicated privacy resources working specifically with these matters.

Additional responsibilities specific to the C-BCRs include the following:

(a) GDPO, Chief Privacy Compliance Officer, designated DPOs and the Network of Privacy Advisors shall monitor compliance on these C-BCRs and advise on the implementation of the C-BCRs.

(b) The GDPO shall ensure that the C-BCRs' compliance audits are carried out on a regular basis. Moreover, the GDPO shall ensure that audit findings are addressed in a proper and timely manner.

(c) The GDPO has the responsibility to coordinate and arrange for access to data processing facilities should the Competent Supervisory Authority request a C-BCRs compliance audit.

(d) Human Resources (People) Function is responsible for ensuring that Personal Data as part of human resources processes and tools is handled in accordance with the C-BCRs.

(e) Legal and Compliance is responsible for ensuring that Personal Data as part of legal and compliance processes and tools are handled in accordance with the C-BCRs.

(f) Security is responsible for ensuring that Personal Data as part of security processes and tools is handled in accordance with the C-BCRs.

(g) Finance is responsible for ensuring that Personal Data as part of finance processes and tools is handled in accordance with the C-BCRs.

(h) IT is responsible for ensuring that privacy controls are designed into internal IT applications and systems up front.

(i) Sourcing is responsible for ensuring that privacy controls and data transfer agreements are part of contractual agreements with third party suppliers.

9. Updating the C-BCRs

The C-BCRs have to be kept up-to-date in order to reflect the current situation (for instance to take into account modifications of the regulatory environment, relevant EDPB recommendations or the Ericsson Group structure).

The Ericsson Group shall report any changes to the C-BCRs (including changes to the list of BCR Members) to all BCR Members without undue delay using the Ericsson Group's internal communications process, including the intranet.

The Ericsson Group shall also, without undue delay and in advance, notify Supervisory Authorities, via the Lead Supervisory Authority, of any significant modifications to the C-BCRs that would possibly be detrimental to the level of the protection offered by the C-BCRs or significantly affect them (e.g. changes to the way in which they are binding). The notification shall include a brief explanation of the reasons for the update after which the Supervisory Authority will assess whether the changes made require a new approval.

Updates to the C-BCRs or to the list of BCR Members in Annex 1 are possible without having to reapply for an approval provided that:

(a) Ericsson Group keeps a fully updated list of the BCR Members and keeps track of and record any updates to the rules and provide the necessary information to the Data Subjects or Competent Supervisory Authorities upon request;

(b) No transfer of Personal Data is made to a new BCR Member until the new BCR Member is effectively bound by the C-BCRs and can deliver compliance;

(c) Where a modification would possibly affect the level of the protection offered by the C-BCRs or significantly affect the C-BCRs (i.e. changes to the binding character), it is promptly communicated to the relevant Supervisory Authorities, via the Lead Authority; and

(d) Any changes to the C-BCRs or to the list of BCR Members in Annex 1 are reported once a year to the relevant Supervisory Authorities via the Lead Supervisory Authority with a brief explanation of the reasons justifying the update. Such annual update shall contain a confirmation that Ericsson AB has sufficient assets, or has made appropriate arrangements to enable itself to pay compensation for damages resulting from a breach of the C-BCRs.

The Lead Supervisory Authority should be notified once a year also where no changes to the C-BCRs have been made. Such annual notification shall also contain a confirmation that Ericsson AB has sufficient assets or has made appropriate arrangements to enable itself to pay compensation for damages resulting from a breach of the C-BCRs.

It is the responsibility of the Chief Privacy Officer to keep a fully updated list of the BCR Members, a record of any updates to the C-BCRs, and provide the necessary information to Data Subjects, and, upon request, to Competent Supervisory Authorities.

10. Non-Compliance and termination of the C-BCRs

To ensure compliance with the C-BCRs, all BCR Members must observe the following:

(a) Ensure no transfer is made to a BCR Member unless the BCR Member is effectively bound by the C-BCRs and can deliver compliance;

(b) The Data Importer must promptly inform the Data Exporter if it is unable to comply with the C-BCRs, for whatever reason, including the situations further described under Section 6.5 above;

(c) Where the Data Importer is in breach of the C-BCRs or unable to comply with them, the Data Exporter should suspend the transfer;

(d) The Data Importer should, at the choice of the Data Exporter, immediately return or delete the Personal Data (including any copies thereof) that has been transferred under the C-BCRs in its entirety, where:

(i) the Data Exporter has suspended the transfer, and compliance with this C-BCRs is not restored within a reasonable time, and in any event within one month of suspension; or

(ii) the Data Importer is in substantial or persistent breach of the C-BCRs; or

(iii) the Data Importer fails to comply with a binding decision of a competent court or Supervisory Authority regarding its obligations under the C-BCRs.

The Data Importer should certify the deletion of the data to the Data Exporter. Until the data is deleted or returned, the Data Importer should continue to ensure compliance with the C-BCRs;

In case of local laws applicable to the Data Importer that prohibit the return or deletion of the transferred Personal Data, the Data Importer should warrant that it will continue to ensure compliance with the C-BCRs and will only process the data to the extent and for as long as required under that local law. For situations where applicable local laws and/or practices affect compliance with the C-BCRs, see Section 2.11 and 6.5 above.

A BCR Member acting as Data Importer, which ceases to be bound by the C-BCRs may keep, return, or delete the Personal Data received under the C-BCRs, as agreed with BCR Member acting as Data Exporter. If the BCR Members agree that the Personal Data may be kept by the Data Importer, protection must be maintained in accordance with Chapter V GDPR.

11. Terminology

Term	Definition
BCR Members	Refers to all Ericsson Companies once they have become party to the Intra-Group Agreement and are thereby bound by the C-BCRs as stated in Section 1.2.2. A list of BCR Members and their contact details are set out in Annex 1.
C-BCRs	Refers to these Controller Binding Corporate Rules.
Controller	Refers to a natural or legal person, public authority, agency, or any other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
Competent Supervisory Authority	Refers to the EU/EEA data protection Supervisory Authority competent for the Data Exporter.
Data Breach	Refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
Data Exporter	Refers to a Controller (or, where permitted, a Processor) established in the EU/EEA that transfers Personal Data to a Data Importer.
Data Importer	Refers to a Controller or Processor located in a third country that receives Personal Data from the Data Exporter.

Data Protection Impact Assessment	Refers to an assessment of the impact of envisaged processing operations on the protection of Personal Data, as set out in Article 35 of the GDPR.
Data Subject	Refers to an identified or identifiable natural person to whom specific Personal Data relates. It is someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
EDPB	Refers to the European Data Protection Board.
EEA	Refers to the European Economic Area. The EEA is made up of the member states of the EU as well as Iceland, Lichtenstein, and Norway.
Employees	Refers to any individual employed by a BCR Member.
Ericsson Companies	Refers to a Legal Entity (including any of its branches) controlled directly or indirectly by LM Ericsson, and whose financial statements are included in the consolidated financial statements of the Ericsson Group.
Ericsson Group	Refers to the group of Ericsson Companies.
Ericsson Group Liable Member	Refers to Ericsson AB.
Ericsson Privacy Policy	Set of Ericsson Privacy Group Directives or Instructions applicable for all Employees and External Workforce involving privacy matters [https://www.ericsson.com/en/legal/privacy/privacy-policy] and ruling Ericsson Privacy Principles [https://www.ericsson.com/en/legal/privacy].
EU	Refers to the European Union, namely its member states.
External Workforce	Refers to contingent workforce (such as consultants, independent contractors, freelancers, etc.), i.e. individuals not actually employed by any BCR Member.
GDPO	Refers to Group Data Protection Officer. The GDPO is part of Group Function Legal Affairs and Compliance.

GDPR	Refers to the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing the Directive 95/46/EC (General Data Protection Regulation), and any amendments and reenactments thereto.
Intra-Group Agreement	Refers to the intra-group agreement (internal reference GFLA-23:000524 Uen "Internal Group Agreement relating to Ericsson Binding Corporate Rules for Controllers"), which includes a specific commitment confirming the binding effect of the C-BCRs.
Lead Supervisory Authority	Refers to the Swedish Authority for Privacy Protection (IMY) (Sw. *Integritetsskyddsmyndigheten)*.
Legal Entity	Refers to an association, corporation, partnership or similar that has legal standing under law and has legal capacity to enter into agreements or contracts, assume obligations, sue and be sued in its own name, and to be held responsible for its actions.
Personal Data	Refers to any information relating to an identified or identifiable natural person (i.e. a Data Subject, as defined above).
Processing	Refers to any operation or set of operations which is performed upon Personal Data or on sets of Personal Data, whether or not by automated means (for example: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction etc.).
Processor	Refers to the natural or legal person, public authority, agency, or other body that processes Personal Data on behalf of the Controller. In the context of this document, the Processor is typically a BCR Member processing data on behalf of a BCR Members acting as a Controller.
Security Incident Management Process (SIMS)	Refers to Ericsson Group's process for planning and be prepared for security incidents, detect, report and assess security incidents and vulnerabilities, respond to security incidents, and learn and make improvements if a security incident has occurred.
Special Categories of Personal Data	Refers to Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Supervisory Authority/Authorities	Refers to the independent public authority/authorities in each EU/EEA member state charged with the responsibility for monitoring the application of the GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of Personal Data within the EU. Some member states may have multiple authorities charged with such responsibilities.

12. Contact for these C-BCRs

Chief Privacy Officer

Privacy.bcr@ericsson.com

Ericsson

Torshamnsgatan 21

164 80 Stockholm, Sweden

13. Annexes and references

13.1 Annexes

Annex 1 BCR Members

Annex 2 Nature of Personal Data transferred

13.2 References

- Group Policy, Code of Business Ethics Our Compass - Code of business ethics guide - Internal (ericsson.com)
- List of local Data Protection Officers data-protection-officers.xlsx (ericsson.com)
- Information document Privacy Notice for Ericsson Employees and External Workforce Privacy notice about personal data processed by Ericsson - Internal

Annex 1

According to list published at Privacy - Ericsson.

Annex 2

1. Nature and categories of the Personal Data transferred

The Ericsson Group processes the following main categories of Personal Data:

1. Employees: name, academic and professional data, contact details, personal identification number, employment information, compensation, bank account information, emergency contacts, etc.

2. External Workforce: name, academic and professional data, contact details, personal identification number, compensation, bank account information, etc.

3. Visitors to BCR Members' premises: contact details, video surveillance information, etc.

4. Shareholders: name, contact details, shareholding, etc.

5. Customer representatives: name, work title, contact details, etc.

6. Providers: name, contact details, etc.

7. Job applicants/candidates: name, contact details, personal identification number, academic and professional data and other information related to the recruitment process.

8. Other third parties: name, contact details, etc.

2. Purposes of processing

The BCR Members mainly processes the Personal Data for the purposes set out below:

1. Access control/Facilities

2. Personnel management (HHRR)

3. Candidates (recruitment)

4. Customers (including marketing & communications purposes)

5. Security incidents

6. Legal proceedings and contracts

7. Video surveillance

8. Whistleblowing (including investigations activities)
9. Contacts
10. Providers

3. Types of processing

The types of processing activities carried out include, though are not limited to: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4. Transfers to third countries

The business of the Ericsson Group is global and personal data may be transferred by and between any BCR Members (see Annex 1).