BINDING CORPORATE RULES FOR DATA CONTROLLER

Abstract
This Binding Corporate Rule (BCR) for Data Controller, Group Directive, herein after referred to as C-BCR, is a set of binding rules that govern the Processing (including access and transfer) of Personal Information1 within the Ericsson Group, where an Ericsson Group entity is the Data Controller of such Personal Information.

Application
This Directive applies to all individuals and Ericsson units who are involved in the Processing of Personal Information or in the development of tools or services used to process Personal Information where an Ericsson Group entity is the Data Controller.

Purpose
The purpose of this C-BCR is to clearly define the rules applicable to all Ericsson Group Entities for Processing Personal Information in order to ensure a consistent and adequate protection of Personal Information throughout the entire Ericsson Group. This is to ensure that, when accessing or transferring Personal Information from the European Economic Area (hereinafter called “EEA”, which includes the European Union, Norway, Iceland, and Lichtenstein) to third countries (which under the laws of the EEA member states are not deemed to have an adequate level of data privacy protection), the Ericsson Group entity in the third country will have an adequate level of data privacy protections in place.

Contents
1 Directive ..............................................................................Error! Bookmark not defined.
   1.1 Introduction........................................................................Error! Bookmark not defined.
   1.2 Scope ...............................................................................Error! Bookmark not defined.
   1.3 Definitions .........................................................................Error! Bookmark not defined.

2 Processing of Personal Information ........................................Error! Bookmark not defined.
   2.1 Legal basis for processing Personal Information Error! Bookmark not defined.
   2.2 Processing of Sensitive Personal Information Error! Bookmark not defined.
   2.3 Transparency and information right.................Error! Bookmark not defined.
   2.4 Purpose limitation ......................................................Error! Bookmark not defined.
   2.5 Data quality and proportionality.........................Error! Bookmark not defined.
   2.6 Security and confidentiality ....................................Error! Bookmark not defined.

3 Data Subject Rights...............................................................Error! Bookmark not defined.
   3.1 Data Subject Rights ......................................................Error! Bookmark not defined.
   3.2 Automated individual decisions .........................Error! Bookmark not defined.
   3.3 Third party beneficiary rights..........................Error! Bookmark not defined.

1 This is Ericsson privacy terminology, which also includes Personal Data as defined in the EU Data Protection Directive 95/46/EC or, if adopted, the replacing General Data Protection Regulation.
1 Directive

1.1 Introduction
Ericsson strives for standardized global and regional ways of working, where possible. As a result, global and regional service centers have been established for centralized administration and support including the Processing of Personal Information. In a globalized environment with a presence in more than 180 countries, cross-country managers, a mobile workforce, remote access and international transfers of Personal Information is essential.

Binding Corporate Rules is a mechanism that can be used to legally access and transfer Personal Information within a corporation from the EEA to members of the corporation located outside of the EEA.

The rules as part of this C-BCR are to ensure that the same level of data privacy protections exists in all Ericsson Group entities to support Personal Information access and data transfers cross border.

Ericsson's Code of Business Ethics [1] and the Group Policy on Privacy [2], approved by the Chief Executive Officer (CEO), is a commitment from Ericsson’s Board of Directors that they will ensure compliance with the prescribed rules in this C-BCR.
“Our responsibility for compliance

Everyone working for Ericsson is required to review the Code, to support and work in line with the company’s commitments stated herein, and to follow the rules in the Code addressed to us as well as all applicable laws. In addition, we must follow Ericsson’s Group policies, directives and instructions as well as local directives and instructions; failure to do so may result in disciplinary action including termination of employment and/or civil and criminal liability.

We place additional responsibilities on our leaders. Through their actions, they shall demonstrate the importance of compliance. Leading by example is critical, as is being available for those who have questions or wish to report possible violations of this Code.

Leaders must ensure that this Code is respected and is enforced in their organizations. Leaders may not turn a blind eye toward unethical conduct.”

Code of Business Ethics

1.2 Scope

This C-BCR applies to worldwide intra-group Processing (collection, use, retention, access, transfer and disposal) of Personal Information. The scope of the C-BCR includes areas where Ericsson is the Data Controller of Personal Information (e.g. employee, external workforce, visitor, shareholders, customer representatives or other third party) where such information is processed as part of automated or partially automated tools and processes. Such areas include, but are not limited to, Business Units, Regional or Local Organizations, and the following Group Functions:

1 Human Resources (HR)
2 Finance
3 Legal
4 Corporate Audit
5 Security
6 Sourcing
7 Sales

Ericsson Group Entities in scope for this BCR are Telefonaktiebolaget LM Ericsson (LME) and any company or legal entity of which LME, directly or indirectly, owns more than 50% of the issued share capital, has more than 50%
of the voting rights at general meetings of shareholders or has the power to
appoint a majority of the directors of such company or legal entity. A list of the
Ericsson Group Entities in scope for this BCR can be found here. In addition
Ericsson India Global Services Private Limited is also an Ericsson Group Entity
in scope for this BCR even if not on the said list. The rules herein are also
applicable in the case external sub-processing is agreed.

The nature of the data transferred is

- Employee and external workforce data (human resources data), as well as
  employee emergency contact data and for international assignments also
  family member data;
- Employee and external workforce data of customers, suppliers and other
  third parties;
- Job applicant data;
- Visitors to Ericsson Group’s premises and webpages; and
- Personal data of shareholders.

The purposes of the transfer and the processing after transfer are to ensure
competent and efficient administration by central competence centers of the
following:

- Data necessary to administrate employment and external workforce (to fulfill
  obligations under labor law and other legal obligations as well as to
  administrate employee benefits and access rights);
- Shareholder’s data necessary for shareholdings records and shareholder’s
  meetings;
- Visitor data, for example to allow access rights and handle cookie consents
  for webpages;
- Customer and third-party workforce data such as business contact details
  and data relating to certification of performed training by such workforce
  processed for administrating contracts and other business relations; and
- Job applicant data for recruitment activities.

Data exporter can be any Ericsson legal entity in EEA, but the major part of
personal data is exported by Ericsson AB in Sweden. The major part of
personal data is transferred to Ericsson’s internal support centers in the
Philippines and India. Transfer is mainly in the form of remote access to servers
located in EEA. However, transfers can be made to other countries as well. For
example, managers in third countries can access personal information of their
subordinates in EEA for fulfilling the employment contract.

1.3 Definitions
Definitions pertaining to this C-BCR can be found in the Privacy Terminology [9]
reference.
2 Processing of Personal Information

2.1 Legal basis for processing Personal Information

Personal Information is processed on the following grounds:

1. The Data Subject has unambiguously given his/her consent; or
2. 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; or
3. The Processing is necessary for compliance with a legal obligation to which the Data Controller is subject; or
4. The Processing is necessary in order to protect the vital interests of the Data Subject; or
5. The Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the Data Subject.

Ericsson Group Entities who are Processing Personal Information, including Sensitive or Special categories of Personal Information herein referred to as ‘Sensitive Data’, shall abide by Group Instruction, Baseline Privacy Requirements [5]. In addition, the following requirements shall be adhered to.

2.2 Processing of Sensitive Personal Information

Processing of Sensitive Data is prohibited except where:

6. The Data Subject has given his/her explicit consent to the Processing of Sensitive Data, except where the applicable laws prohibit it; or
7. The Processing is necessary for the purposes of carrying out the obligations and specific rights of the Data Controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
8. 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 his consent; or
9. The Processing relates to Sensitive Data made public by the Data Subject; or
10. The Processing of Sensitive Data is necessary for the establishment, exercise or defense of legal claims; or
11. The Processing of the Sensitive Data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where the Sensitive 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.
2.3 **Transparency and information right**
This C-BCR is part of Ericsson’s Management System and as such published on the intranet for easy and unrestricted access for each and everyone within the Ericsson Group. A sub-set of this BCR shall also be accessible on http://www.ericsson.com/about-us/privacy covering the main data protection obligations undertaken the Ericsson Group companies, updated information as regard the Group Members bound by the BCR and the means available to data subjects in order to ascertain compliance with the rules.

A Privacy Notice specifying the purpose for Personal Information collection, use, and recipients of Personal Information including the identity of the Data Controller(s) as well as right of access to and the right to rectify his/her Personal Information shall be made available to the Data Subject.

Information for how Data Subjects can obtain access to Personal Information shall be available on the internet (ericsson.com) and on the intranet. Employees and external workforce shall also be advised to contact Ericsson HR Direct with any privacy related questions.

2.4 **Purpose limitation**
As required in Group Instruction, Baseline Privacy Requirements [5], Personal Information shall only be collected and processed to fulfil legitimate business purposes including legal and contractual obligations. Personal Information shall not be further processed in a way incompatible with those purposes. Additional safeguards, such as stipulated in the EU Directive 95/46/EC, will be provided for Sensitive Data.

2.5 **Data quality and proportionality**
As required in Group Instruction, Baseline Privacy Requirements [5], Personal Information shall be accurate and where necessary, kept up to date. Personal Information shall be adequate, relevant and not excessive in relation to the purposes for which it is transferred and further processed.

Personal Information shall not be processed for longer than necessary or for purposes other for which it was originally obtained.

2.6 **Security and confidentiality**
As required in Group Instruction, Baseline Privacy Requirements [5], Personal Information shall be handled as Ericsson Confidential and protected according to Group Instruction, Information Security Requirements [6]. For Personal Information processed in an IT system or application, the Baseline Requirements for Ericsson IT [7] shall be applied.

Security measures shall protect Personal Information from misuse or accidental destruction, loss, alteration disclosure or access. Access to Personal Information shall be authorized individually based on the ‘need to know’ principle.
3 Data Subject Rights

3.1 Data Subject Rights
Every Data Subject has the following rights:

12 To obtain, without constraint, at reasonable intervals and without excessive delay or expense a copy of all Personal Information relating to him/her that is processed; or

13 To obtain the rectification, erasure or blocking of Personal Information due to it being incomplete or inaccurate; or

14 To object, at any time, on compelling legitimate grounds relating to his particular situation, to the processing of his Personal Information, unless that processing is required by law. Where the objection is justified, the processing must cease. The processing may continue if justified and permitted by law; or

15 To object, on request and free of charge, to the processing of Personal Information relating to him/her for the purposes of direct marketing.

3.2 Automated individual decisions
No evaluation of, or decision about, a Data Subject, which significantly affects him/her, will be based solely on automated processing of his/her Personal Information unless that decision:

16 Is taken in the course of the entering into the performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the Data Subject, has been satisfied or that there are suitable measures to safeguard his/her legitimate interests, such as arrangements allowing him/her to put his/her point of view; or

17 Is authorized by a law, which also lays down measures to safeguard the Data Subject’s legitimate interests.

3.3 Third party beneficiary rights
For Personal Information exported from the EEA:

18 The Data Subject shall have a right to judicial remedy for any breach of the rights guaranteed him by this C-BCR and the national law applicable to the processing in question.

19 Any Data Subject who has suffered damage as a result of an unlawful data processing operation or of any act incompatible with the national provisions for the protection of Personal Information or a breach of this C-BCR is entitled to receive compensation for the damage suffered.

20 The Data Subject can choose to lodge claims before the Data Protection Authority or a court in the jurisdiction of the data exporter located in the EEA or in Sweden.
4 Ericsson Group Requirements

4.1 Relationships with processors that are Members of the Ericsson Group
All members of the Ericsson Group, employees and external workforce must comply with Ericsson’s Group policies, directives and instructions as well as local directives and instructions. Failure to do so may result in disciplinary action including termination of employment and/or civil and criminal liability.

4.2 Restrictions on transfers and onward transfers to external processors and controllers (not Members of the Ericsson Group)
External processors located inside the EEA or in a country recognized by the EU Commission as ensuring an adequate level of data privacy protection shall be bound by a written agreement stipulating that the processor shall act only on instructions from Ericsson and shall be responsible for the implementation of adequate security and confidentiality measures.

All transfers of Personal Information to external controllers located outside the EEA must respect the European rules on trans-border data flows (Articles 25-26 of Directive 95/46/EC: for instance making use of the EU Standard Contractual Clauses approved by the EU Commission 2001/497/EC or 2004/915/EC or by other adequate contractual means according to Articles 25 and 26 of the EU Directive).

All transfers of Personal Information to external processors located outside the EEA must respect the rules relating to the processors (Articles 16-17 Directive 95/45/EC) in addition to the rules on trans-border data flows (Articles 25-26 of Directive 95/46/EC).

4.3 Liability
For Data Subjects in the EEA, Telefonaktiebolaget LM Ericsson accepts responsibility for and agrees to take the necessary action to remedy the acts of other members of the Ericsson Group outside of the EEA and to pay compensation for any damages resulting from the violation of the C-BCRs by members of the Ericsson Group.

Telefonaktiebolaget LM Ericsson also accepts that if a member of the Ericsson Group outside of EEA violates this C-BCR relating to personal data transferred from EEA the courts or other competent authorities in EEA will have jurisdiction and the Data Subject will have the rights and remedies against Telefonaktiebolaget LM Ericsson. Nevertheless, the primary liability towards authorities, courts and Data Subjects in the EEA lies with the data exporting member of the Ericsson Group, to remedy the acts and pay penalties and compensation for any damages resulting from the violation of the C-BCR.

Telefonaktiebolaget LM Ericsson and the data exporting member of the Ericsson Group in EEA accept liability as if the violation had taken place by them in the member state in which they are based instead of the member of the Group outside of EEA.

The burden of proof towards Data Subjects stays with either Telefonaktiebolaget LM Ericsson or the data exporting member of the Ericsson
4. Group to demonstrate that the member of the Ericsson Group outside the EEA is not liable for the violation resulting in the damages claimed by the Data Subject.

If Telefonaktiebolaget LM Ericsson or the data exporting member of the Ericsson Group can prove that the member of the Ericsson Group outside the EEA is not liable for the violation, it may discharge itself and the Ericsson Group from any responsibility.

4.4 Mutual assistance and cooperation with Data Protection Authorities

Members of the Ericsson Group shall cooperate and assist each other to handle a request or complaint from an individual or an investigation or inquiry by Data Protection Authorities in the EEA.

Entities will abide by the advice of the Data Protection Authorities in the EEA on any issues regarding the interpretation of the BCRs. This commitment does not limit Ericsson entities from challenging such advice in court or other applicable instances when deemed appropriate and necessary.

4.5 Updates of the rules

The Head of Financial reporting and Control is responsible for updating the list of the members of the Ericsson Group. The Chief Privacy Officer has access to the updates of the list and keeps track of and record any updates to the rules and provides necessary information to the data subjects or the Data Protection Authorities on request. The Chief Privacy Officer reports any substantial changes to the BCR or to the list of members once a year to the Data Protection Authorities granting the authorization with a brief explanation of the reasons justifying the update. No transfer of personal data can be made under this BCR from EEA to a new member of the Ericsson Group until the exporter has made sure that the new member is effectively bound by the rules and can deliver compliance.

4.6 Relationship between national laws and the C-BCRs

Where the local legislation, for instance EU legislation, requires a higher level of data protection, it will take precedence over the C-BCR. In any event, Personal Information shall be processed in accordance to the applicable law as provided by the Article 4 of the Directive 95/46/EC and the relevant local legislation.

4.7 Actions in case of national legislation preventing respect of C-BCRs

Where a member of the Ericsson Group has reason to believe that the legislation applicable to it prevents the member of the Ericsson Group from fulfilling its obligations under the C-BCRs and has substantial effect on the guarantees provided by the rules, it will promptly inform the Ericsson Chief Privacy Officer (CPO), except where prohibited by a law enforcement authority, such as prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. Where there is conflict between national law and the commitments in the C-BCR, the Ericsson CPO will take a responsible decision
on what action to take and will consult the competent Data Protection Authorities in case of doubt.

5 Internal Complaint Mechanisms

5.1 Complaints
Data Subjects with access to HR Direct who wish to file a complaint or a request pertaining to their Personal Information shall be instructed to contact HR Direct. Data Subjects who do not have access to HR Direct who wish to file a complaint or a request pertaining to their Personal Information shall be instructed to send an e-mail to ericsson.group.privacy@ericsson.com.

Any Data Subject can make a complaint that any member if the Ericsson Group is not complying with this C-BCR.

When complaints are received, they will be acknowledged, and the complainant will be provided with an initial timeframe for the handling of the complaint. In addition, the complainant will be informed about the consequences in case of rejection of the complaint, consequences in case the complaint is considered as justified and consequences if the complainant is not satisfied by the reply, such as right to lodge a claim before the relevant courts and/or data protection authorities. Complaints shall be dealt with by the Data Protection Officer at Group Function HR.

5.2 Report incidents
Individuals who wish to report a security or privacy incident shall be instructed to use the Security Incident Management System (SIMS) and such incidents shall be handled according to the Security Incident Management [8]. In cases where incidents are e-mailed to ericsson.group.privacy@ericsson.com or directly reported to a Privacy Advisor (found at Ericsson Privacy Forum) those incidents shall be reported into SIMS to invoke the incident handling process. When a new incident is received in SIMS, it is automatically distributed to case handlers based on the reporter's home location. The case handler shall assess whether the incident received is within the scope of his area of responsibility. If needed, the case should be re-routed to the responsible organization. The case handler is responsible for handling and managing security incidents and for escalation.

5.3 Taking action
Data Subjects are entitled to take action before a Data Protection Authority or court as set out in 3.3 above. In these situations, the employee or officer of Ericsson receiving information of the action from or on behalf of the Data Subject or the Data Protection Authority shall send an e-mail about the action to ericsson.group.privacy@ericsson.com.
6 Compliance and Supervision of Compliance

6.1 Audit Program
The Ericsson internal audit program shall ensure that this C-BCR is adhered to, including all aspects of the BCRs, such as creating a process for ensuring that corrective actions take place for all Ericsson entities on a regular basis, at a minimum bi-annually. Results from audits, along with progress on resolving audit findings, shall be communicated by Corporate Audit to the Board of Directors of Telefonaktiebolaget LM Ericsson (publ) and the Ericsson CPO. Applicable Data Protection Authorities may have access to such C-BCR compliance audit reports on a need-to-have basis. However, prior to submitting the results, the Group Privacy Core Team shall be informed.

EU Data Protection Authorities may audit any member of the Ericsson Group and any advice originating from such audits shall be adhered to, where appropriate. This commitment does not limit the members of the Ericsson Group from challenging such advice in court or other applicable instances when deemed appropriate and necessary.

6.2 Privacy Program
The existing Global Privacy Framework [10] shall ensure the implementation of these C-BCR rules where applicable. This includes, but is not limited to, Privacy Impact Assessments, Privacy by Design, and the implementation of the Baseline Privacy Requirements as further described in Group Directive, Data Privacy Management [4].

6.3 Training Program
As required in Group Instruction, Baseline Privacy Requirements [5], appropriate privacy training will be provided to personnel on an ongoing basis who have permanent or regular access to Personal Information or are involved in the collection of Personal Information or in the development of tools or services used to process Personal Information. This include training specific to C-BCRs.

As per Ericsson’s Privacy Policy [4] the Chief Financial Officer (CFO) is ultimately responsible for ensuring that the organization meets its data privacy compliance obligations. The Chief Privacy Officer (CPO) has the responsibility to coordinate, communicate and consult with the regional Security Directors on data protection issues. CPO and the Regional Security Directors have the responsibility to establish, maintain and deploy appropriate training on privacy including on this BCR.

6.4 Governance
Governance of this C-BCR shall be part of the existing Global Privacy Framework Governance model, as described in Group Directive, Data Privacy Management [4]. In alignment with the existing model, decisions, communications, compliance and other governing activities shall be the responsibility of the Group Privacy Core Team; escalations shall be handled at the Group Information Security Board (GISB).
6.5 Responsibilities
Responsibilities of this C-BCR shall be part of the existing privacy responsibilities as part of the Global Privacy Framework, as described in Group Directive, Data Privacy Management [4].

Additional responsibilities specific to C-BCR include the following:

The Expert, Data Protection & HR at Group Function Legal Affairs, has the responsibility to coordinate and arrange for access to data processing facilities should the Data Protection Authority request a C-BCR compliance audit. The Group Privacy Core Team shall receive the audit results for evaluation.

The Chief Privacy Officer (CPO) shall ensure that C-BCR compliance audits are carried out on regular basis. Moreover, the CPO shall ensure that audit findings are addressed in a proper and timely manner.

The Network of Privacy Advisors shall advise on the implementation of this C-BCR.

Group Security is responsible for the Global Privacy Framework in order to ensure implementation and compliance to applicable privacy requirements, including this C-BCR.

HR (Global, Regional, BU, and Local) is responsible for ensuring that Personal Information as part of HR processes and tools is handled in accordance to this C-BCR and Baseline Privacy Requirements.

Legal (Global, Regional, BU, and Local) is responsible for ensuring that Personal Information as part of Legal processes and tools is handled in accordance to this C-BCR and Baseline Privacy Requirements.

Security (Global, Regional, BU, and Local) is responsible for ensuring that Personal Information as part of Security processes and tools is handled in accordance to this C-BCR and Baseline Privacy Requirements.

Finance (Global, Regional, BU, and Local) is responsible for ensuring that Personal Information as part of Finance processes and tools is handled in accordance to this C-BCR and Baseline Privacy Requirements.

IT (Global, Regional, BU, and Local) is responsible for ensuring that privacy controls are designed into IT application and systems up front in accordance with the Baseline Privacy Requirements.

Sourcing (Global, Regional, BU, and Local) is responsible for ensuring that privacy controls and data transfer agreements are part of contractual agreements with third parties.

7 Contact for this Directive
Head of Group Security, GFFIE

8 References
[3] Group Policy, [011 03-2815 Uen], Privacy
[7] Group Instruction, [1/00021-3142 Uen], Baseline Requirements for Ericsson IT
[8] Instruction, [GFFI-15:011504], Security Incident Management
[9] Information, [LME-14:003111 Uen], Privacy Terminology
[10] Instruction, [GFFI-16:003067 Uen], Global Privacy Framework