Processor Binding Corporate Rules

Abstract

This Group Directive is a set of Processor Binding Corporate Rules (hereafter referred to as the "**P-BCRs**"), that governs all international transfers of Personal Data between Ericsson Companies that are BCR Members when providing services to Customers, where the BCR Member and the Customer in the Service Agreement have agreed that the P-BCRs will apply to transfers of Personal Data.

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 P-BCRs are designed to help the Ericsson Group and our Customers, (Controllers), 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 P-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 Processor (separately or jointly with another BCR Member) or as Sub-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 of our Customers, 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

We respect and promote human rights throughout our work, including by providing access to communication and information around the world.

We fundamentally believe that our hardware, software, services and solutions bring positive change to people. At the same time, we work to mitigate and minimize the risk of potential misuse of our technology.

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

We also advocate 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.

(Extract from Ericsson Code of Business Ethics)

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 P-BCRs help to clearly define the rules applicable to all BCR Members for processing Personal Data as Processors or Sub-Processors in order to ensure a consistent and high level of protection for Personal Data in connection with transfers between BCR Members.

Contents

Directive

Introduction

Data protection terms in the P-BCRs shall have the same meaning as they do in the GDPR. The terminology table in Section 7 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 to) Personal Data between different entities within the same corporate group. The P-BCRs help to ensure that the same level of protection for Personal Data is applied by all BCR Members when processing data from Controllers not belonging to Ericsson Group under a Service Agreement.

The Ericsson Group has implemented a groupwide data protection compliance program and has appointed a GDPO and a Chief Privacy Compliance Officer, who are involved in all matters related to the P-BCRs. The GDPO and the Chief Privacy Compliance Officer, report to the highest management level. In addition, there is a Head of Product Privacy working specifically with Privacy by Design and product privacy questions and Business Areas and Group Functions working specifically with questions related to Sales.

1. Binding nature

1.1 Duty to respect the P-BCRs

All BCR Members, including their Employees and External Workforce, have a duty to respect the P-BCRs. Ericsson Group's internal policies highlight the commitment from the Board of Directors and the Executive Management to ensure compliance with the P-BCRs.

Our People and workplace

We are committed to fostering an inclusive and supportive workplace where you can reach your full potential. We respect the dignity of every human being and work in accordance with all internationally recognized human rights including those outlined in the International Bill of Human Rights and the International Labor Organization's Declaration on Fundamental Principles and Rights at Work

(Extract from Ericsson Code of Business Ethics)

Each BCR Member, including its Employees and External Workforce, has a duty to follow the instructions on data processing given by the BCR Member acting as Processor. In addition, each BCR Member shall respect the instructions from the Controller regarding the data

processing and the security and confidentiality measures as provided in the Service Agreement (Article 28, 29 and 32 of the GDPR).

1.2 Means by which the P-BCRs are made binding within the Ericsson Group

1.2.1 Binding effect on BCR Members

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

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

1.2.2 Binding effect on Employees and External Workforce

The P-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 P-BCRs are one. Failure to do so may result in disciplinary action including termination of employment and/or civil and criminal liability.

Respect privacy and protect personal data

We process personal data responsibly and in accordance with privacy laws.

We protect personal data and support global efforts to safeguard it. We adhere to global privacy principles and applicable laws, including the EU General Data Protection Regulation (GDPR). We also have Binding Corporate Rules and contractual agreements which regulate how we process and share data.

(Extract from Ericsson Code of Business Ethics)

1.3 Third party beneficiary rights

1.3.1 Rights which are directly enforceable against a BCR Member

Data Subjects shall be able to enforce the P-BCRs as third party beneficiaries directly against a BCR Member where the requirements at stake are specifically directed to Processors in accordance with the GDPR. In this regards, Data Subjects are able to enforce the following elements of the P-BCRs directly against a BCR Member:

(a) The duty to respect the instructions from the Controller regarding the data processing including for data transfers to third countries (Article 28.3.a, 28.3.g, 29 of the GDPR and Section 1.1, 6.1.2 and 6.1.4 of the P-BCRs),

(b) The duty to implement appropriate technical and organizational security measures (Article 28.3.c and 32 of the GDPR and Section 6.1.4 of the P-BCRs) and duty to notify any Data Breach to the Controller (Article 33.2 of the GDPR and Section 6.1.4 of the P-BCRs),

(c) The duty to respect the conditions when engaging a Sub-Processor either within or outside the Ericsson Group (Article 28.2, 28.3.d.28.4, 45, 46, 47 of the GDPR, and Section 6.1.4 and 6.1.7 of the P-BCRs),

(d) The duty to cooperate with and assist the Controller in complying and demonstrating compliance with the law such as for answering requests from Data Subjects in relation to their rights (Article 28.3.e, 28.3.f, 28.3.h of the GDPR and Sections 3.2, 6.1.1, 6.1.3, 6.1.4, 6.1.5 and 6.2 of the P-BCRs),

(e) Easy access to the P-BCRs (Article 47.2.g of the GDPR and Section 1.7 of the P-BCRs),

(f) The right to complain through internal complaint mechanisms (Article 47.2.i of the GDPR and Section 2.2 of the P-BCRs),

(g) The duty to cooperate with the supervisory authority (Article 31, 47.2.l of the GDPR and Section 3.1 of the P-BCRs),

(h) Liability, compensation and jurisdiction provisions (Article 47.2.e, 79, 82 of the GDPR and Sections 1.3, 1.5 and 1.6 of the P-BCRs), and

(i) National legislation preventing respect of BCRs (Article 47.2.m of the GDPR and Section 6.4 of the P-BCRs).

1.3.2 Rights which are enforceable against a BCR Member in case the Data Subject is not able to bring a claim against the Controller

A Data Subject whose Personal Data is covered by the P-BCRs pursuant to a Service Agreement shall have the right to enforce the P-BCRs as a third-party beneficiary against each BCR Member involved in the processing of the Data Subject's Personal Data in case the Data Subject is not able to bring a claim against the Controller; because the Controller has factually disappeared or ceased to exist in law or has become insolvent, unless any successor entity has assumed the entire legal obligations of the Controller by contract of by operation of law, in which case the Data Subject can enforce its rights against such entity.

In such a case, Data Subjects shall at least be able to enforce against the respective BCR Member the following Sections of the P-BCRs: 1.1, 1.3, 1.5, 1.6, 1.7, 2.2, 3.1, 3.2, 6.1, 6.3, and 6.4.

1.3.3 Judicial remedies and the right to lodge a complaint

The Data Subjects' rights as set out in Section 1.3.1 and 1.3.2 cover the judicial remedies for any breach of the third party beneficiary rights guaranteed and the right to obtain redress and where appropriate receive compensation for any damage (material harm but also any distress).

Data Subjects shall in particular be entitled to lodge a complaint before the Lead Supervisory Authority (choice between the supervisory authority of the EU Member State of his/her habitual residence, place of work or place of alleged infringement). Data Subjects in the EU shall also be entitled to lodge a complaint before the competent court of the EU Member State, with a choice for the Data Subject to act before the courts where the Controller or BCR Member has an establishment or where the Data Subject has his or her habitual residence pursuant to Article 79 of the GDPR.

Where the BCR Member and the Controller involved in the same processing are found responsible for any damage caused by such processing, the Data Subject shall be entitled to receive compensation for the entire damage directly from the BCR Member (Article 82.4 of the GDPR)

1.4 Responsibility towards the Controller

The P-BCRs are made binding towards the Controller through a specific reference to them in the Service Agreement which shall comply with Article 28 of the GDPR.

If and to the extent provided in the Service Agreement, the Controller shall have the right to enforce the P-BCRs (a) against any BCR Member for breaches such member has caused, and, (b) against Ericsson AB in case of a breach of the P-BCRs or of the Service Agreement by BCR Members established outside of the EU, or a breach of the written agreement referred to in Section 6.1.7 of the P-BCRs by any external Sub-Processor established outside of the EU. The Controller's rights shall cover the judicial remedies and the right to receive compensation, as further specified in the applicable Service Agreement.

1.5 The Ericsson Group accepts liability for paying compensation and to remedy breaches of the P-BCRs

Ericsson AB accepts responsibility for and agrees to take the necessary action to remedy the acts of other BCR Members established outside of the EU or breaches caused by external Sub-Processors established outside of the EU and to pay compensation for any damages resulting from a violation of the P-BCRs.

Ericsson AB will accept liability as if the violation had taken place by it in the Member State in which it is based instead of the BCR Member outside the EU, or the external Sub-Processor established outside of the EU. This BCR Member may not rely on a breach by a Sub-Processor (internal or external of the Ericsson Group) of its obligations in order to avoid its own liabilities.

1.6 The burden of proof lies with the Ericsson Group and not the Data Subject

Ericsson AB has the burden of proof to demonstrate that the BCR Member outside of the EU or the external Sub-Processor is not liable for any violation of the P-BCRs which has resulted in the Data Subject claiming damages.

Where the Controller can demonstrate that it has suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of P-BCRs, it will be for Ericsson AB to prove that the BCR Member outside of the EU or the external Sub-Processor was not responsible for the breach of the P-BCRs giving rise to those damages or that no such breach took place.

If Ericsson AB can prove that the BCR Member outside the EU or the external Sub-Processor is not responsible for the act, it may discharge itself from any responsibility/liability.

1.7 Easy access to the P-BCRs and easy access to information about third party beneficiary rights

1.7.1 Access for the Controller

If a Customer agrees in a Service Agreement that the P-BCRs are part of the contract with one or more BCR Members, then the P-BCRs shall be incorporated into the Service Agreement. The P-BCRs will be annexed to the Service Agreement or a reference to it will be made with a possibility of electronic access.

In addition, in order to ensure transparency and easy access to the P-BCRs for Customers, the P-BCRs will be available on the Ericsson Group's website:
https://www.ericsson.com/en/legal/privacy

All Customers may also request a copy of the P-BCRs by emailing ericsson.group.privacy@ericsson.com.

1.7.2 Access for the Data Subjects

All Data Subjects benefitting from the third party beneficiary rights shall be provided with the information on their third party beneficiary rights with regard to the processing of their Personal Data and on the means to exercise those rights. To ensure transparency every Data Subject shall have easy access to the P-BCRs.

The P-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.

In addition, in order to ensure transparency and easy access to the P-BCRs for Data Subjects outside the Ericsson Group (i.e. not having access to the intranet), the P-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 P-BCRs by emailing ericsson.group.privacy@ericsson.com

2. Effectiveness

2.1 Training program

According to Ericsson Privacy Policy appropriate privacy training 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 on behalf of Customers. This includes training specific to the P-BCRs.

The GDPO, DPOs, Chief Privacy Compliance Officer, Compliance (Privacy) Officers, Data Protection Advisors, Privacy Advisors and Security Directors (network of Ericsson Privacy Professionals) have the responsibility to establish, maintain, and deploy appropriate training on privacy including on the P-BCRs.

2.2 Complaint handling process

The Ericsson Group has delegated the GDPO as the specific contact point for Data Subjects. Data Subjects who wish to report a privacy incident, question or present a complaint pertaining his/her Personal Data can contact Group Data Protection Officer by postal mail at Ericsson AB, Group Function Legal Affairs, 164 80 Stockholm, Sweden or send an e-mail to ericsson.group.privacy@ericsson.com.

In countries where local contacts for privacy related matters exist, Data Subjects can also report an incident by way of sending an e-mail to such local contact or contacts as per the following link https://www.ericsson.com/4abd8a/assets/local/legal/data-protection-officer-list.pdf.

All BCR Members have a duty to communicate a claim or request without undue delay to the Controller without obligation to handle it (except if it has been agreed otherwise with the Controller). A BCR Member shall handle complaints from Data Subjects where the Controller has disappeared factually or has ceased to exist in law or became insolvent.

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

(a) When complaints are received, they will be handled by an Ericsson Privacy Professional, including the GDPO and/or the relevant DPO, without undue delay and always within one month. An extension of up to two 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 the complaint is rejected, and the consequences if 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. In the event that the Ericsson Group no longer maintains the Personal Data, the Data Subject will be informed accordingly.

2.3 Audit program

The Ericsson Group's Corporate Audit and Management Framework shall ensure that all aspects of the P-BCRs are adhered to, and shall include methods for ensuring that corrective actions take place for BCR Members on a regular basis, at a minimum annually, or on request by the Group Compliance Committee accountable for the Privacy Strategy, the GDPO or the relevant DPO, to ensure verification of compliance with these P-BCRs.

Results from audits, along with progress on resolving audit findings, shall be communicated by Corporate Audit Function to the Group Compliance Committee, the Board of Directors of Ericsson AB, its Executive Management and to the GDPO. Audits can be also conducted by external auditors.

Supervisory Authorities competent for the Controller can have access to P-BCRs compliance audit reports upon request, and Supervisory Authorities will have the authority/power to carry out a data protection audit of any BCR Member if required.

Supervisory Authorities may audit any BCR Member and any advice originating from such audits shall be adhered to. This commitment does not prevent the BCR Members from challenging such advice in court or other applicable instances when deemed appropriate and necessary.

Any Processor or Sub-Processor processing the Personal Data on behalf of a particular Controller will accept, at the request of that Controller, to submit their data processing facilities for audit of the processing activities relating to that Controller which shall be carried out by the Controller or an inspection body composed of independent members and in possession of the required professional qualifications, bound by a duty of confidentiality, selected by the Controller, where applicable, in agreement with the Supervisory Authority.

2.4 Network of Ericsson´s Privacy Professionals for monitoring compliance with the P-BCRs

The Ericsson Group has designated DPOs where required under applicable 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 P-BCRs. All these professionals enjoy the highest management support for carrying out these tasks. In alignment with the existing model, decisions, communications, compliance and other governing activities shall be the responsibility of the Group Compliance Committee.

Considering the relevance of the Personal Data processed pertaining to human resources matters, the Ericsson Group has appointed a Head of People Privacy working specifically with these matters. The Group Compliance Committee, work to ensure compliance on human resources data protection matters.

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

(a) GDPO, Chief Privacy Compliance Officer, Chief Compliance Officer, Designated DPOs, Privacy Advisors and the entire Network of Privacy Professionals shall monitor compliance on the P-BCRS and advise on the implementation of the P-BCRs.

(b) The GDPO shall ensure that the P-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) Corporate Audit Function and Management Frameworks are responsible for the audit program, which requires auditing of the P-BCRs on a regular basis, at a minimum annually. They are responsible for communicating progress and audit findings to Ericsson AB's board of directors, its executive management and to the GDPO.

(d) The GDPO has the responsibility to coordinate and arrange for access to data processing facilities should the competent Supervisory Authority request a P-BCRs compliance audit. The Group Compliance Committee shall receive the audit results for evaluation.

(e) Sales is responsible for ensuring that Personal Data as part of sales processes and tools is handled in accordance with the P-BCRs.

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

(g) 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 P-BCRs.

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

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

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

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

3. Cooperate duty

3.1 Duty to cooperate with Supervisory Authorities

All BCR Members shall have a duty to cooperate with and to accept to be audited by the Supervisory Authorities competent for the relevant Controller and to comply with the advice of these Supervisory Authorities on any issue related to these rules.

3.2 Duty to cooperate with the Controller

Any Processor or Sub-Processor shall have a duty to cooperate and assist the Controller to comply with data protection law, such as its duty to respect the Date Subject rights or to handle their complaints, or to be in a position to reply to investigation or inquiry from Supervisory Authorities. This shall be done in a reasonable time and to the extent reasonably possible.

4. Description of processing and data flows

4.1 Transfers and material scope of the P-BCRs

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

Under the P-BCRs the Ericsson Group processes Personal Data on behalf of a Customer. The processing primarily relates to Customer´s customers, employees, business contracts, and other business related third parties. Processing takes place across the Ericsson Group by the different Ericsson Companies; including but not limited to Business Units, Customer Units, Geographical Organizations, and the following areas:

a) Managed Services

b) Networks

c) Technologies

d) Digital Services

e) Customer Support

f) Research and Development

g) Legal and Compliance

h) Government and Regulatory

i) General Account Management

j) Corporate Audit

k) Security

l) Sales

m) Marketing

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

4.2 Geographical scope of the P-BCRs

It is up to the Controller to apply the P-BCRs to:

(a) All Personal Data processed for Processor activities and that are submitted to EU law (for instance, data has been transferred from the EU), or

(b) All processing of data processed for Processor activities within the Ericsson Group whatever the origin of the data.

5. Mechanisms for reporting and recording changes

5.1 Process for updating the P-BCRs

The P-BCRs can be modified (for instance to take into account modifications of the regulatory environment or the Ericsson Group structure). Any changes to the P-BCRs shall be reported to

all BCR Members, and to the relevant Supervisory Authorities, via the Lead Supervisory Authority, and to the Controllers whose Service Agreements include the P-BCRs.

Where a change affects the processing conditions, the information should be given to the Controller in such timely fashion that the Controller has the possibility to object to the change or to terminate the Service Agreement according to its terms before the modification is made (for instance, on any intended changes concerning the addition or replacement of Sub-Processors, before the data are communicated to the new Sub-Processor).

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

(a) Group Function Legal Affaires and Compliance keeps a fully updated list of the BCR Members and of the Sub-Processors involved in the data processing activities for the Controller which shall be made accessible to the Controller, data subjects and Supervisory Authorities.

(b) Group Function Legal Affaires and Compliance keeps track of and record any updates to the rules and provide the necessary information to systematically to the Controller and upon request to Supervisory Authorities upon request;

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

(d) Any changes to the P-BCRs or to the list of BCR Members in Annex 1 shall be reported once a year to the relevant Supervisory Authorities via the Lead Supervisory Authority with a brief explanation of the reasons justifying the update; and

(e) Where a modification would affect the level of the protection offered by the P-BCRs or significantly affect the P-BCRs (i.e. changes to the binding character), it must be promptly communicated to the relevant Supervisory Authorities, via the Lead Supervisory Authority.

6. Data protection safeguards

6.1 Privacy principles and rules on transfers or onward transfers outside of the EU

6.1.1 Transparency, fairness, and lawfulness

Processors and Sub-Processors will have a general duty to help and assist the Controller to comply with the law (for instance, to be transparent about Sub-Processor activities in order to allow the Controller to correctly inform the data subject).

6.1.2 Purpose limitation

Processors and Sub-Processors will have a duty to process the Personal Data only on behalf of the Controller and in compliance with the Service Agreement and its documented instructions including with regard to transfers of Personal Data to a third country, unless required to do so by Union or Member State law to which the Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing takes place, unless that law prohibits such information on important grounds of public interest (Article 28.3 a of the GDPR). In other cases, if the Processor cannot provide such compliance for whatever reasons, it agrees to inform promptly the Controller of its inability to comply, in which case the Controller is entitled to suspend the transfer of data and/or terminate the contract.

On the termination of the provision of services related to the data processing, the Processors and Sub-Processors shall, at the choice of the Controller and in accordance with the terms of the applicable Service Agreement, delete or return all the Personal Data transferred to the Controller and delete the copies thereof and certify to the Controller that it has done so, unless legislation imposed upon them requires storage of the Personal Data transferred. In that case, the Processors and the Sub-Processors will inform the Controller and warrant that it will guarantee the confidentiality of the Personal Data transferred and will not actively process the Personal Data transferred anymore.

6.1.3 Data quality

Processors and Sub-Processors will have a general duty to help and assist the Controller to comply with the law, in particular:

(a) Processors and Sub-Processors will execute any necessary measures when requested by the Controller in the Service Agreement, in order to have the data updated, corrected or deleted. Processors and Sub-Processors will inform each BCR Member to whom the data have been disclosed of any rectification, or deletion of data.

(b) Processors and Sub-Processors will execute any necessary measures, when asked by the Controller, in order to have the data deleted or anonymised from the moment the identification form is not necessary anymore. Processor and Sub-Processors will communicate to each entity to whom the data have been disclosed of any deletion or anonymisation of data.

6.1.4 Security

Processors and Sub-Processors will have a duty to implement all appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented by the processing as provided by Article 32 of the GDPR.

Processors and Sub-Processors will also have a duty to assist the Controller in ensuring compliance with the obligations as set out in Articles 32 to 36 of the GDPR taking into account the nature of processing and information available to the Processor (Art.28.3 f of the GDPR).

Processors and Sub-Processors must implement technical and organisational measures which at least meet the requirements of the data controller's applicable law and any existing particular measures specified in the Service Agreement.

Processors shall inform the Controller without undue delay after becoming aware of any Data Breach. In addition, Sub-Processors shall have the duty to inform the Processor and the Controller without undue delay after becoming aware of any Data Breach.

6.1.5 Data Subject rights

Processors and Sub-Processors will execute any appropriate technical and organizational measures, insofar as this is possible, when asked by the Controller, for the fulfilment of the Controller's obligations to respond to requests for exercising the data subjects rights as set out in Chapter III of the GDPR (Article 28.3 e of the GDPR) including by communicating any useful information in order to help the Controller to comply with the duty to respect the rights of the data subjects.

Processor and Sub-Processors will transmit to the Controller any data subject request without answering it unless he is authorised to do so.

6.1.6 Sub-processing within the Group

Data may be sub-processed by other BCR Members bound by the P-BCRs only with the prior informed specific or general written authorization of the Controller. The Service Agreement will specify if a general prior authorization given at the beginning of the service would be sufficient or if a specific authorization will be required for each new Sub-Processor. If a general authorization is given, the Controller should be informed by the Processor of any intended changes concerning the addition or replacement of a Sub-Processor in such a timely fashion that the Controller has the possibility to object to the change or to terminate the contract before the data are communicated to the new Sub-Processor.

6.1.7 Onward transfers to external Sub-Processors

Data may be sub-processed by non-members of the P-BCRs only with the prior informed specific or general written authorization of the Controller. If a general authorization is given in the relevant Service Agreement, the Controller should be informed by the Processor of any intended changes concerning the addition or replacement of Sub-Processors in such a timely fashion that the Controller has the possibility to object to the change or to terminate the contract before the data are communicated to the new Sub-Processor.

Where a BCR Member subcontracts its obligations under the Service Agreement, with the authorization of the Controller, it shall do so only by way of a contract or other legal act under Union or Member State law with the Sub-Processor which provides that adequate protection is provided as set out in Articles 28, 29, 32, 45, 46, 47 of the GDPR and which ensures that the same data protection obligations as set out in the Service Agreement between the Controller and the Processor and Sections 1.3, 1.4, 3 and 6 of the P-BCRs are imposed on the Sub-Processor, in particular providing sufficient guarantees to implement appropriate technical and organization measures in such a manner that the processing will meet the requirements of the GDPR (Article 28.4 of the GDPR).

6.1.8 Transfer impact assessment

A BCR Member transferring Personal Data to a country outside the EU– whether to a BCR Member or to Controllers or Processors located in Countries outside the EU – must carry out a transfer impact assessment with the help of the data importer and/or the Customer if needed.

A transfer impact assessment must confirm the following:

(a) the level of protection required by EU Law is respected in the country outside the EU concerned:

(b) the guarantees provided by these P-BCRs can be complied with in practice; and

(c) the legislation in the country outside the EU does not create possible interference with the fundamental rights of Data Subjects and complies with the Charter of Fundamental Rights of the EU.

Where a transfer impact assessment cannot confirm the items set out above, the BCR Member exporting Personal Data should assess whether the parties to the transfer can provide supplementary contractual, technical or organisational measures to ensure an essentially equivalent level of protection as provided by the GDPR.

The specific circumstances of the transfer (especially categories of data, means of transfer, further transfer to a third party) as well as the laws and practices applicable to the company in the third country, including those requiring the disclosure of data to public authorities or authorizing access by such authorities, must be taken into account.

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

The BCR Member must document the assessment 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.

6.2 Accountability, record of processing activities and other tools

All Processors have a duty to make available to the Controller all information necessary to demonstrate compliance with their obligations as provided by Article 28.3 h of the GDPR and allow for and contribute to audits, including inspections conducted by the Controller or another auditor mandated by the Controller. In addition, a Processor shall immediately inform the Controller if in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

In order to demonstrate compliance with the P-BCRs each BCR Member need to maintain a record of all categories of processing activities carried out on behalf of each Controller in line with the requirements as set out in Article 30.2 of the GDPR. This record should be maintained in writing, including in electronic form and should be made available to the competent Supervisory Authority/Authorities upon request (Article 30.3 and 30.4 of the GDPR).

The BCR Members shall also assist the Controller in implementing appropriate technical and organizational measures to comply with data protection principles and facilitate compliance with the requirements set up by the P-BCRs in practice such as data protection by design and by default (Article 25 and 47.2 d of the GDPR).

6.3 The list of entities bound by the P-BCRs

The BCR Members bound by the P-BCRs are listed in Annex 1.

6.4 Transparency in case of national legislation preventing respect of the P-BCRs

Where a BCR Member has reasons to believe that the existing or future legislation applicable to such BCR Member may prevent the BCR Member from fulfilling the instructions received from the Controller, or its obligations under the P-BCRs, or the Service Agreement, it will promptly notify this to (i) the GDPO who shall inform the Controller, which is entitled to suspend the transfer of data and/or terminate the contract (or affected portions of a contract), as applicable and subject to the terms of the Service Agreement, and to (ii) the Supervisory Authority competent for the BCR Member making the notification and the Supervisory Authority competent for the Controller.

Any legally binding request for disclosure of the Personal Data by a law enforcement authority or state security body shall be communicated to the Controller unless otherwise prohibited (such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation). In any case, the request for disclosure should be put on hold and the Supervisory Authority competent for the Controller and the competent Supervisory Authority for the Processor should be clearly informed about the request, including information about the data requested, the requesting body and the legal basis for disclosure (unless otherwise prohibited).

If in specific cases the suspension and/or notification are prohibited, the requested BCR Member will use its best efforts to obtain the right to waive this prohibition in order to

communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.

If, in the above cases, despite having used its best efforts, the requested BCR Member is not in a position to notify the competent Supervisory Authorities, it must annually provide general information on the requests it received to the competent Supervisory Authorities (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.).

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

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

6.5 The relationship between national laws and the P-BCRs

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

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

7. 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 P-BCRs as stated in Section 1.2. A list of BCR Members and their contact details are set out in Annex 1.
P-BCRs	Refers to these Processor Binding Corporate Rules.
Controller/Customer	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, and on behalf of which the BCR Member processes Personal Data under a Service Agreement.

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.
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, location data, an online identifier or to one or more specific factors (physical, physiological, genetic, mental, economic, cultural, social etc.).
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 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.
Ericsson Privacy Professionals	The Ericsson Privacy Professionals conform the network of Ericsson Privacy Professionals. Such professionals are the following but not limited to: Group Data Protection Officer, Chief Privacy Officer, Chief Information Security Officer, Product Privacy Officer, Head of People Privacy, Local Data Protection Officers, Privacy Advisors.
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-23:000525 Uen "Internal Group Agreement relating to Ericsson Binding Corporate Rules for Processors"), which includes a specific commitment confirming the binding effect of the P-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.
LM Ericsson	Refers to the Swedish limited liability company Telefonaktiebolaget LM Ericsson (publ), company registration number 556016-0680; the parent company of the Ericsson Group.
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, organization, 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/Customer.
Service Agreement	An agreement between a BCR Member (Processor) and a Customer (Controller) for providing services involving processing of Personal Data, and referencing the P-BCRs.
Sub-Processor	Means an entity appointed by a Processor to process Personal Data with the approval of the Controller. The entity may be any BCR Member, or a third party sub-processor
Supervisory Authority/Authorities	Refers to the public authority/authorities charged with the responsibility of overseeing compliance with the GDPR in each EU/EEA member state. Some member states may have multiple authorities charged with such responsibilities.

8. Contacts for these P-BCRs

Group Data Protection Officer

ericsson.group.privacy@ericsson.com

Ericsson

Torshamnsgatan 21

164 80 Stockholm, Sweden

9. Annexes and references

9.1 Annexes

Annex 1 BCR Members

Annex 2 Nature of Personal Data transferred

9.2 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. Customers´ end user: IMEI, SMISDN, IMSI, IP Addresses, Navigation data, location data, Calls Registry- CDRs, etc.
2. Customer´s Workforce: name, academic and professional data, contact details, personal identification number, compensation, bank account information, etc.
3. Customer representatives: name, work title, contact details, etc.
4. 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. Customers (including marketing and communications purposes)
2. End users' data
3. Contact Persons

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) according to the contract with Customer.