Your Data, Your Rights: Ericsson’s Processor Binding Corporate Rules on data protection

Introduction

Integrity, transparency, and responsibility characterise the way Ericsson conducts business. As a processor of large volumes of our Customers’ personal data (see our Terminology list at the end of this document for more information), we recognise our responsibility to respect privacy rights and to put in place appropriate standards of data protection.

We operate in a highly networked, interconnected, and global business reality that demands a coordinated response to data protection. Our Processor Binding Corporate Rules (“BCR”) set down effective and uniform standards for the processing of personal data right across Ericsson’s global operations. Our BCR help us to comply with data protection standards within the European Union (“EU”) and the European Economic Area (“EEA”).

The following document is part of our transparency efforts to share information about our approach to data protection. It contains full information on the aspects of our BCR that confer rights on individuals whose personal data we process on behalf of our Customers – these individuals are known as “Data Subjects” (see our Terminology list at the end of this document for more information). This document is designed to help Data Subjects in the European Economic Area understand what standards they can expect from our company, and what rights they may have if something goes wrong. Insofar as there is a divergence between the wording of this document and the BCR, the language of the BCR shall take precedence.

FAQs

What are Binding Corporate Rules (BCR)?

Binding Corporate Rules, or BCR, are a binding code of practice that governs how a multinational company transfers personal data between different entities within its corporate group. A multinational company has different parts of its business based across the world, and therefore subject to different local laws. While some national laws might afford a high level of protection for personal data, others may fall below the standard set down by the EU/EEA Data Protection Directive (and the General Data Protection Regulation that succeeds the said Directive as from May 25, 2018). Therefore, most personal data governed by the laws of EU/EEA Member States cannot be transferred to countries that do not afford adequate protection, unless there are proper additional safeguards in place. An approved set of BCR is one such type of safeguard.

When we provide services, we act as Data Processors for our Customers, who act as Data Controllers. Our Customers determine why and how data is to be processed, and we process it on their behalf. To ensure that we act as a responsible partner for our Customers, we have adopted our own set of BCR, which have been approved by the relevant EU/EEA Data Protection Authorities. The Swedish Data Protection Authority (Datainspektionen) acted as the lead authority during the approval process.

When do Ericsson’s BCR apply?

Our BCR apply to all personal data processed by Ericsson on behalf of our Customers being transferred from the EU/EEA to a third country (i.e. a country outside the EU/EEA), or data accessed from a third country. For more information on the scope of our BCR, see section “F” (Description of transfers and material scope) below.
How do Ericsson’s BCR affect my rights?

If there is a breach of the BCR, then you may be able to obtain compensation from Ericsson if you are not able to bring a claim against the entity for whom we process your personal data (i.e. our Customer), either because it has disappeared or ceased to exist in law, or become insolvent. Further information can be found in section “B” (Third-party beneficiary rights for Data Subjects) below.

How do I find out more?

If you would like to know more about how we process your personal data on behalf of our Customers, or if you feel that you may have been the victim of a personal data breach, please do not hesitate to contact us using the contact details provided at the end of this document.¹

Information on Beneficiary Rights under our BCR

A. The duty to respect the BCR

All members of the Ericsson Group, employees, and contingent workforce must respect the BCR and the Service Agreement. We are under a clear duty to respect the Customer’s instructions regarding data processing as stated in the Service Agreement. The Ericsson Group Privacy Core Team shall support and advise on privacy compliance matters.

B. Third-party beneficiary rights for Data Subjects

In case the Data Subject is not able to bring a claim against the applicable Customer because the Customer has factually disappeared or ceased to exist in law or has become insolvent, and unless any successor entity of the Customer has assumed the entire legal obligations of the Customer by contract or by operation of law, then the following applies:

i. The Data Subjects are entitled to enforce these BCR against any Ericsson Group Entities which have breached these BCR

ii. The EEA contracting party² with the Customer is responsible for, and shall agree to take necessary actions to remedy the acts of Ericsson Group Entities established outside of EEA or remedy breaches caused by external sub-processors established outside of EEA and to pay compensation to Data Subjects for any damages resulting from the violation of these BCR.

iii. Ericsson AB can assume responsibility, however it may be more convenient for the Data Subject to turn to the processor entity in their own country which is the EEA contracting party with the Customer, if they so choose.

The Ericsson Group Entity having assumed responsibility according to ii. or iii. above will accept liability as if such violation had been caused by the former instead of the Ericsson Group Entity outside the EEA or instead of the external sub-processor established outside of the EEA.

Further, if the Ericsson Group Company having assumed responsibility according to ii or iii above can prove that the member of the group outside the EEA is not responsible for the act, it may discharge itself from any responsibility.

C. Responsibility towards the Customer

¹ The Customer has an obligation to provide Data Subjects with a full copy of our BCR and our Service Agreement with them (excluding any sensitive or confidential commercial information) upon request.

² The Ericsson Group Entity situated in the EEA that has entered into the Services Agreement with the Customer.
The Customer has the right to enforce these BCR and the Service Agreement against any of the Ericsson Group Entities for breaches that they have caused; including the right to enforce against the EEA contracting party with the Customer should the breach have been caused by an external sub-processor established outside of EEA.

The EEA contracting party with the Customer, and Ericsson AB if needed, is responsible for, and shall agree to take necessary actions to remedy the acts of Ericsson Group Entities established outside of EEA or remedy breaches caused by external sub-processor established outside of EEA and to pay compensation for any damages resulting from the violation of these BCR as agreed in the Service Agreement.

The EEA contracting party with the Customer will accept liability as if such violation had been caused by the EEA contracting party with the Customer itself instead of the Ericsson Group Entity outside the EEA or instead of the external sub-processor established outside of EEA.

Further, if the EEA contracting party with the Customer can prove that the member of the group outside the EEA is not responsible for the act, it may discharge itself from any liability.

D. Complaint handling process

Data Subjects who wish to file a complaint or a request shall be instructed to send an e-mail to ericsson.group.privacy@ericsson.com, preferably according to the instruction: [How do I communicate securely by email with Ericsson users](mailto:ericsson.group.privacy@ericsson.com). Such complaints or requests shall be reported into the SIMS tool and communicated to the relevant Customer and handled according to the instructions in the Service Agreement by the Customer.

When a Customer has disappeared factually or has ceased to exist in law or become insolvent and no successor entity of the Customer has assumed the entire legal obligations of the Customer by contract of by operation of law, then Ericsson Group will handle complaints by Data Subjects according to the following procedure:

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 replies, such as right to lodge a claim before the relevant courts and/or data protection authorities. Complaints shall be dealt with by Group Function Legal Affairs.

The relevant Data Protection Authority will be the Data Protection Authority in Sweden (where Ericsson’s global headquarters are situated); or in the country where the EEA contracting party with the Customer is situated; or any other country where the Data Subject has the legal right to take action before the Data Protection Authority. The relevant court will be a court in Sweden (where Ericsson’s global headquarters are situated); or in the country where the EEA contracting party with the Customer is situated; or in any other country in which the Data Subject in accordance with mandatory law has the right to take action before a court.

E. Duty to cooperate with the Customer and Data Protection Authorities

Ericsson Group Entities have a clear duty to co-operate with and to accept to be audited by applicable Data Protection Authority or Customers. In the event that a Data Protection Authority has issued a

---

3 Security Incident Management System (SIMS) is where Privacy issues are recorded and dispatched to relevant security managers for actions.

4 Including measures to be executed, response time and consequences should a complaint or request not be dealt with accordingly.
binding decision then this decision must be followed within the Ericsson Group when Ericsson has not exercised its right to appeal of the decision. In addition, Ericsson Group Entities must take into consideration any advice on issues related to privacy regulations. Data Protection Authorities may advise on any issue related to data protection in which case an affected Ericsson Group Entity is responsible for informing the Group Privacy Core Team and, if necessary, seeking advice in the matter.

**F. Material scope and description of transfers**

These BCR are to ensure a proper level of protection of personal data when transferring data from the European Economic Area to a third country which do not have an adequate level of protection.

These BCR are applicable throughout the Ericsson Group when Ericsson is the Data Processor\(^5\) and a Customer is the Data Controller.

The rules are applicable to processing of personal data by electronic means and in systematically accessible paper based filing systems. Examples of operations in scope include but are not limited to:

(a) Managed Services  
(b) Customer Support  
(c) Remote Software delivery  
(d) Data Mining and Big Data analysis  
(e) Business and R&D Analytics  
(f) Cloud Services  
(g) M-Commerce  
(h) Account Management  
(i) Marketing, Sales, and Promotions  
(j) Government and Regulatory Affairs

Ericsson Group Entities in scope for these 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.

The Customer shall also ensure that these BCR are applied to all transfer and processing of its personal data performed by Ericsson.

**G. Privacy principles**

**Transparency and Fairness**

Customers shall be informed about in which countries Ericsson Group Entities or external sub-processors will process personal data. Any changes regarding such countries shall be communicated to relevant Customers.

\(^5\) Mainly relating to international transfer and processing of Customers’ subscriber data.
Information about applicable processing activities shall be made available to Customers and relevant Data Protection Authorities on the “need-to-share” basis. Significant changes related to processing shall be communicated to relevant Customers.

Relevant Customers and relevant Data Protection Authorities shall be promptly notified if existing or anticipated future legislation prevents the expected compliance with these BCR or the applicable Service Agreement. If so, the Customer shall be entitled to suspend transfer of data.

If not against criminal investigation law, relevant Customers shall be promptly informed if Ericsson is required by a law enforcement authority to disclose Customers’ personal data.

**Purpose Limitation**

All personal data processed on behalf of the Customer shall only be collected and processed for fulfilment of legal or contractual obligations. Ericsson shall respect that the Customer exclusively determines the definition of, and the purposes for processing of the personal data being processed on its behalf.

Personal data in Ericsson’s custody and processed on behalf of the Customer shall be returned at the end of the contract unless Ericsson is instructed to destroy the data.

**Data Quality**

(k) All Ericsson Group Entities must assist the Customer to comply with applicable data protection laws in particular to have data updated, corrected, deleted or anonymised.

(l) Necessary measures shall be taken to rectify any inaccuracy and to delete personal data when reasonably requested by the Customer. It shall be ensured that such measures are taken by all Ericsson Group Entities and external sub-processors holding the personal data in question. If not otherwise agreed, Customers’ personal data shall be deleted or anonymised when the data is no longer needed for the fulfilment of legal or contractual obligations.

**Security**

Security measures meeting requirements of EEA member state law of the exporting Customer and meeting Customers’ instructions set out in the Service Agreement shall be adhered to in addition to Ericsson Group standard security as set forth in applicable group steering documents. Such measures will protect personal data from misuse or accidental destruction, loss, alteration disclosure or access. Access rights to personal data are authorised individually on the need-to-have principle if not otherwise agreed with the Customer. Staff who access personal data shall meet confidentiality obligations as specified by applicable non-disclosure agreements. Any security breach affecting the privacy of personal data being processed on behalf of the Customer shall promptly be communicated to the relevant Customer.

The Security Incident Management Process outlines the mandatory instructions to ensure that security and privacy incidents are properly reported and managed in order to avoid unnecessary damage and cost and to comply with legislation, rules, and contractual obligations.

**Data Subject Rights:**

Please see sections B (Third-party beneficiary rights for Data Subjects) and D (Complaints handling process) of this document.

**Sub-processing and Onward Transfer**
The Service Agreement between the Customer and an Ericsson Group Entity established at the beginning of a service shall preferably stipulate permission to sub-process data by any member of the Ericsson Group. This agreement will include information on the main elements, such as parties, countries, security measures, etc.).

Otherwise and prior to the processing, consent from the Customer shall be obtained on a case-by-case basis. Prior to onward transfer of personal data to external sub-processors the Customer’s written consent thereto shall be obtained. Written instructions to provide that adequate protection is implemented by external sub-processors must be agreed before processing of personal data may take place. Such instruction shall include the following provisions to be included in agreements with external sub-processors:

- Personal data shall be processed only according to Ericsson’s instructions and for the purpose authorized by Ericsson.
- Personal data shall be kept confidential.
- Further sub-processing down the line shall not be allowed without prior written consent of Ericsson, who first must obtain the Customer’s consent.
- Ericsson shall promptly be informed of any occurred or suspected Privacy Breach.
- Security measures that will be in place to mitigate risks towards the personal data.

For onward transfers of personal data from EEA Ericsson uses the Standard Contractual Clauses pursuant to European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under the EU/EEA Data Protection Directive (and the General Data Protection Regulation that succeeds the said Directive as from May 25, 2018) or other legal mechanism for transfer such as Binding Corporate Rules.

H. List of entities bound by the BCR

A list of main Ericsson Group Entities can be found here. In addition the BCR also applies to Ericsson India Global Services Private Limited in India. The rules herein are also applicable in the case external sub-processing is agreed.

I. Terminology list

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymised</td>
<td>Personal data elements have been removed so that the individual is not identified, also referred to as “de-identified”.</td>
</tr>
<tr>
<td>Binding Corporate Rules</td>
<td>Codes of practice drawn up and followed voluntarily by multinational organisations. These rules aim to ensure adequate safeguards for processing and transfers of personal data between entities, which are part of the same corporate group, and that are bound by these corporate rules. The rules are based on European data protection standards.</td>
</tr>
<tr>
<td>Customer</td>
<td>A natural or legal person, public authority, agency, or any other body with whom Ericsson has a Service Agreement to process personal data on that entity’s behalf. See “Data Controller” below.</td>
</tr>
</tbody>
</table>

Note: A Customer may wish to prohibit or restrict data transfer.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Controller</td>
<td>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. In this context, the Data Controller is an external entity with whom Ericsson has a Service Agreement, such as a customer, partner, etc. It is the Data Controller that is primarily liable towards Data Protection Authorities and Data Subjects for ensuring that personal data transferred outside the EEA are protected.</td>
</tr>
<tr>
<td>Data Processor</td>
<td>The Data Processor is the natural or legal person, public authority, agency, or any other body which processes personal data on behalf of the Data Controller. In this context the Data Processor is an Ericsson Group Entity.</td>
</tr>
<tr>
<td>Data Subject</td>
<td>An identified or identifiable person to whom specific personal data relates. It is someone who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more specific factors (physical, physiological, mental, economic, cultural, social).</td>
</tr>
<tr>
<td>EEA contracting party</td>
<td>The Ericsson entity situated in an EEA7 country that is party to the Service Agreement with the Customer.</td>
</tr>
<tr>
<td>Personal data</td>
<td>Personal data shall mean any information relating to a Data Subject.</td>
</tr>
<tr>
<td>Privacy Breach</td>
<td>The unauthorised access, use or disclosure of Personal Information in a manner not permitted by law, regulation, or contract, which compromises the security and privacy of personal data and which creates a substantial risk of identity theft, fraud, or harm against an individual. This includes any accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of personal data.</td>
</tr>
<tr>
<td>Processing</td>
<td>Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means (for example: collection, recording, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, deleting or destruction, etc.).</td>
</tr>
<tr>
<td>Third country</td>
<td>A “third country” is a country outside of the EEA. The EU Commission maintains a list of third countries which ensure an adequate level of data protection.</td>
</tr>
<tr>
<td>Third-party beneficiary</td>
<td>A third-party beneficiary is a person who is not a party to a contract, but has legal rights to enforce the contract or share in proceeds because the contract was made for the third party's benefit.</td>
</tr>
</tbody>
</table>

**Contact Details**

Should you have any further enquiries regarding Ericsson’s BCR or our approach to personal data protection generally, please do not hesitate to contact us using the following details:

---

7 European Economic Area (EEA). The European Economic Area is made up of the EU Member States as well as Norway, Iceland, and Liechtenstein.
ericsson.group.privacy@ericsson.com

or by postal mail to:

Group Data Protection Officer, Ericsson AB, Group Function Legal Affairs, 164 80 Stockholm, Sweden.