Light is OSRAM

OSRAM BCR

Binding Corporate Rules (the „BCR“) for OSRAM Group Companies and Adopting Companies for the protection of personal data

Terms

- **Adopting company** an OSRAM associated company in Germany or overseas in which the OSRAM group parent company or an affiliated company has a minority stake and which, with the approval of the OSRAM group parent company, has given a voluntary undertaking to comply with the regulations of the BCR by entering into the ICA;
- **BCR** the present Binding Corporate Rules and the regulations contained in them;
- **Consent** a freely given, specific informed and unambiguous expression of will whereby the data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her[1];
- **Controller** an entity (whether a natural or legal person, public authority, agency or other body), which alone or jointly with others determines the purposes and means of data processing;
- **CDPD** Corporate Data Privacy Department, the central department at OSRAM responsible for corporate data protection according to actual organizational chart;
- **Customers and suppliers** natural and legal persons with whom a business relationship exists or is planned;
- **Data subject** any identified or identifiable natural person whose data are processed. An identifiable person is one who can be identified, directly or indirectly, e.g. by reference to a specific identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of this natural person; Legal persons may be included within the scope of the BCR by an agreement to that effect between the company transferring the data and the data recipient (to that extent these are also considered data subjects);
- **DPC** Data Protection Coordinator, i.e. the person appointed by a participating company who is responsible for local implementation of and compliance with the BCR as well as support of the CDPD;
- **DPE** Data Protection Executive of an OSRAM group company; this role is performed by the CEO of the OSRAM group company in question;
- **DPO** Data Protection Officer, i.e. the person appointed by a participating company who oversees and consults management in questions of local implementation and compliance with the General Data Protection Regulation and other applicable data protection provisions and whose appointment is mandatory under certain conditions laid down therein;
- **EEA country / EEA countries** the member states of the European Union (EU) and the other signatories to the Treaty on the European Economic Area (EEA);

[1] Certain national legislations may set down special requirements for consent, which may affect the validity of the consent.

- **General Data Protection Regulation** the Regulation (EU) 2016/679 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;

- **Group company or OSRAM group company** the OSRAM group parent company and any company, in Germany or overseas, in which the OSRAM group parent company, directly or indirectly, has a majority holding or owns or controls the majority of the voting rights;

- **ICA** Inter-Company Agreement by acceding to which an OSRAM group company undertakes to comply with regulations of the BCR;

- **OSRAM group parent company** OSRAM GmbH;

- **Participating company** an OSRAM group company or an adopting company which accedes to the ICA and thereby gives an undertaking to comply with regulations of these BCR;

- **Personal data** all information relating to a data subject;

- **Personal data breach** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

- **Processing of personal data** or **data processing** any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination as well as erasure, destruction or restriction of the processing;

- **Processor** natural or legal person, public authority, agency or other body which processes personal data on behalf of a controller;

- **Special categories of personal data** information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data and biometric data used for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

- **Standard contractual clauses** EU Standard Contractual Clauses for Data Processors adopted by the decision of the European Commission 2010/87/EU or EU Standard Contractual Clauses between Data Controllers adopted by the decision 2011/497/EC or 2004/915/EC or any other contractual safeguards adopted by decisions of European Commission under Article 46 para 2 (c) of the General Data Protection Regulation;

- **Third party** any natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

Summary of the OSRAM BCR

The primary aim of these Binding Corporate Rules (BCR) is to ensure, in all OSRAM group companies and adopting companies, adequate protection of personal data transferred in the course of business from a participating company to other participating companies.

The following personal data fall under the BCR scope:

- All personal data originating from the EU / EEA which are subject to the General Data Protection Regulation;

- Personal data irrespective of their country of origin, to the extent that they are transferred from a (collecting) participating company to a (receiving) participating company.

For this purpose, it is essential to establish harmonized data privacy protection and data security standards for the processing of such personal data within the meaning of the General Data Protection Regulation and, thus, to assure – with respect to the personal data in scope of these BCR – that an adequate level of data protection and appropriate guarantees are provided within the meaning of the General Data Protection Regulation regarding the protection of the right to privacy and the exercise of related rights.

These BCR provide the general and generally valid regulatory framework for the processing of personal data in scope of these BCR relating to employees, customers, suppliers, shareholders, business partners or future business partners and other data subjects by OSRAM group companies or adopting companies. The present BCR reflect the situation prevailing at the time of the latest review of the BCR and the current international data protection requirements, specifically the requirements of the General Data Protection Regulation, the relevant guidelines, working documents of the EU Article 29 Data Protection Group and the European Data Protection Board, and the principles of the International Conference of Data Protection and Privacy Commissioners on International Standards on the Protection of Privacy (referred to below as the "Madrid Resolution") of November 5, 2009.

1. Content of Guideline

1.1 Scope of application of the BCR

All OSRAM group companies and all adopting companies worldwide come within the scope of the BCR. The BCR apply for the processing of

- all personal data originating from the EU / EEA which are subject to the General Data Protection Regulation;
- personal data irrespective of their country of origin, to the extent that they are transferred from a (collecting) participating company to a (receiving) participating company

relating to employees, customers, suppliers, shareholders, business partners or potential business partners and other data subjects by OSRAM group companies or adopting companies. Not only personal data from participating companies within an EEA country is covered by these BCR, but **ALL** data originating from a participating company as soon as such data are transferred to another participating company (including personal data from participating companies residing outside of EEA when such data are transferred to another participating company).

1.2 Principles of the processing of personal data and elements of data privacy framework

The following principles and elements of the data privacy framework derive specifically from the General Data Protection Regulation and the Madrid Resolution of November 5, 2009 should be taken into account when the processing of personal data is carried out by participating companies within the scope of these BCR:

1.2.1 Lawfulness and fairness of data processing

The processing of personal data shall be carried out lawfully in compliance with the relevant statutory provisions and with due regard for the principles laid down in these BCR.

Processing is only permissible, if at least one of the following prerequisites is fulfilled:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes; or
- Data processing is required for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- Processing is necessary for compliance with a legal obligation to which the controller is subject; or
- Processing is necessary to protect the vital interests of the data subject or of another natural person; or
- Processing is required for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or

- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data;

- Processing is stipulated or permitted by national law and regulations that apply for the participating company that originally transferred the data.

The controller must provide simple, fast and efficient procedures that allow the data subject to withdraw his/her consent at any time.

All participating companies shall process personal data fairly. Data processing is to be carried out in such a way that it is reasonably expected by the data subjects concerned and does not have unjustified adverse effects on them.

1.2.2 Purpose limitation

Personal data shall be processed exclusively for specified, explicit and legitimate purposes. Under no circumstances, shall personal data be processed in a way incompatible with the legitimate purposes for which the personal data was collected. Participating companies are obligated to adhere to the purpose of data transfer when storing and further processing or using data transferred to them by another participating company; the purpose of data processing may only be changed with the consent of the data subject or to the extent permitted by the national law of the country to which the participating company originally transferring the data is subject.

1.2.3 Transparency

All participating companies shall process personal data in a transparent manner. Under Articles 13 and 14 of the General Data Privacy Regulation, data subjects whose personal data is processed by a participating company shall be provided with the following information by the participating company (in consultation with the transferring company, if applicable):

- Identity and contact details of the controller and of the transferring company;
- Where applicable, contact details of the data protection officer of the respective participating company;
- Categories of personal data concerned;
- Recipients or categories of recipients of personal data;
- Purpose of processing as well as the legal basis for the processing;
- Where applicable, legitimate interests pursued by the controller or by a third party;
- Where applicable, reference to the appropriate safeguards undertaken to protect personal data transferred to recipients established in third countries or international organizations as well as the means by which a copy of these safeguards is obtainable or where they have been made available;
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- Where the processing is based on a consent of a data subject, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- The right to lodge a complaint with the supervisory authority;
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- The existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- The source from which personal data originates, including publicly accessible sources (unless this is personal data collected directly from the data subject).

These BCR are made available to all data subjects benefitting from the third party beneficiary rights as laid down in the subsection 1.2.18.1.3 hereof along with information as listed in this subsection.

To the extent that the personal data was not collected directly from the data subject, as an exception such information need not be provided, if the data subject already has information, or if this would involve disproportionate effort.

1.2.4 Data quality, data minimization and storage limitation

Personal data must be factually correct and – if necessary – kept up to date. Appropriate measures are to be taken to ensure that inaccurate or incomplete data is rectified or erased.

Data processing shall be guided by the principle of data economy. The aim shall be to collect, process and use only the personal data required, i.e. as little personal data as possible. In particular, data shall be anonymized, provided that the cost and effort involved is commensurate with the desired purpose. Statistical evaluations or studies based on anonymized data are not relevant for data privacy protection purposes, provided that such data cannot be used to identify the data subject.

Personal data which are no longer required for the business purposes for which they were originally collected and stored, are to be erased. Should statutory retention periods apply, the processing of the respective data shall be restricted.

1.2.5 Onward transfer of data

The transfer of personal data from a participating company to a non-participating company is only permissible under the following conditions:

- If the receiving entity is a processor, the conditions set out in Article 28 of the General Data Protection Regulation are satisfied;

- If the receiving entity is a controller that along with a participating company jointly determines the purposes and means of processing, the requirements established in Article 26 of the General Data Protection Regulation are fulfilled.

Further transfers of personal data which a participating company located in a non-EEA country (= data importer) received from another participating company located in an EEA country (= data exporter), by the data importer to an external controller outside the OSRAM group established in a non-EEA country without adequate level of data protection are only permissible, provided that (i) the receiving entity is endowed with an adequate level of protection for personal data within the meaning of Articles 45-48 of the General Data Protection Regulation, e.g. by concluding standard contractual clauses or (ii) by applying derogations for specific situations according to Article 49 of the General Data Protection Regulation.

1.2.6 Special categories of personal data and data related to criminal convictions and offences

Special categories of personal data must not be processed as a general principle. Should the processing of special categories of personal data be necessary, the explicit consent of the data subject must be obtained, unless:

- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by applicable local law or a collective agreement under applicable local law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
- the data subject is physically or legally incapable of giving his/her consent (e.g. in case of a medical emergency) and processing is necessary to protect the vital interests of the data subject or of another natural person; or
- the data subject has already manifestly made public the data in question; or
- data processing is necessary for the establishment, exercise or defence of legal claims;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of applicable local law or pursuant to contract with a health professional and subject to obligation of professional secrecy.

The competent DPO or DPC of the participating company or the CDPD shall be consulted prior to the processing of special categories of personal data.

Processing of personal data related to criminal convictions and offences shall not be carried out as a rule. Should processing of these data be necessary, it may only be permissible after the prior consultation with the CDPD under the control of the competent supervisory authority or subject to appropriate safeguards as established by the General Data Protection Regulation and other applicable data protection provisions.

1.2.7 Automated individual decisions-making

If personal data is processed for the purpose of making automated individual decisions, the legitimate interests of the data subject must be ensured through appropriate measures. Decisions which have negative legal consequences for the data subject or substantially prejudice the data subject, may not be reached exclusively on the basis of an automated individual procedure designed to evaluate an individual's personal characteristics, i.e. decisions may not be exclusively based on the use of information technology. Automated procedures may generally only be used as a tool for the decision-making process.

An exception to this "tool-only" principle applies in cases

- Where the decision is taken in the context of entering into or performing a contract and the legitimate interests of the data subject are adequately safeguarded i.e. by providing him/her with information about the logic of how such a decision is reached and by giving him/her the opportunity to review and comment. In case the data subject submits comments, the controller must review its decision; or

- Where it is authorized by applicable local law; or

- Where decision is based on the data subject's explicit consent

1.2.8. Records of processing activities

All participating companies shall document and maintain records of processing activities carried out in the respective company. Each DPC or DPO shall be responsible to ensure that records of processing activities are documented and reviewed on a regular basis. The CDPD provides the participating companies with access to an electronic record keeping system, where records should be laid down. The CDPD also provides participating companies with templates and instructions on the maintenance of the records and monitors the compliance with this obligation.

1.2.9. Data protection impact assessments

Where a processing activity, considering the nature, scope, context and purposes of the processing, is likely to result in a high risk for the rights and freedom of data subjects, participating companies are required to conduct data protection impact assessments in accordance with Article 35 of the General Data Protection Regulation and guidance hereto issued by the supervisory authorities. The CDPD provides DPCs and DPOs with guidance and methods for conducting such data protection impact assessments.

The legal requirements to the content of such assessments are to be observed.

If a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller must not commence or continue the processing and shall consult the competent supervisory authority according to Article 36 of the General Data Protection Regulation.

1.2.10 Data security

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, participating companies are to take appropriate technical and organizational measures to ensure the requisite data security, which protects personal data against accidental or unlawful erasure, unauthorized use, alteration, against loss, destruction as well as against unauthorized disclosure or unauthorized access. Special categories of personal data are to be given special protection.
The security measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the protected data while at the same time striving to reflect the state of the art in data security.

The security measures to be provided relate in particular to computers (servers and workplace computers), networks, communication links and applications. To ensure an adequate level of technical and organizational measures for data protection, the Corporate Guideline on Information Security was introduced with binding effect for the entire OSRAM group (OSRAM guideline IT3000). The current version of the guideline is available on the Intranet.

Specific measures used to ensure adequate protection of personal data include pseudonymisation and encryption of personal data, admission controls, system access controls, data access controls, transmission controls, input controls, transportation controls, storage controls, job controls, availability and recovery controls as well as segregation controls to ensure:

- the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- the existence of a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

All workplace computers – including mobile devices (e.g. laptops) – are password-protected. The OSRAM intranet has a firewall system to protect internal company content from unauthorized external access. Transmission of personal data within the company's own network is generally encrypted – to the extent that the nature and intended purpose of the personal data requires this.

1.2.11 Confidentiality of data processing

Only personnel of the participating companies that are authorized and have been specifically instructed in compliance with data privacy protection requirements, may collect, process or use personal data. Access authorization of the individual employee will be restricted according to the nature and scope of his/her particular field of activity. The employee is prohibited from using personal data for private purposes, transferring or otherwise making available personal data to unauthorized persons. Unauthorized persons in this context include, for example, other employees, to the extent that they do not require the personal data to complete specialist tasks assigned to them. The confidentiality obligation continues beyond the end of the employment relationship of the employee in question.

1.2.12 Data breach notification

All participating companies undertake to inform the CDPD without undue delay of any (suspected) data breach affecting personal data within the scope of these BCR.

The CDPD shall assess the nature of the data breach and categories of the affected data/data subjects as well as its consequences for rights and freedoms of the affected data subjects and determine, if the data breach in question is likely to result in a (high) risk to the rights and freedoms of natural persons.

If required, the CDPD together with the respective DPC/DPO coordinates the notification of the data breach to the supervisory authority or/and the affected individuals as well as ensures appropriate documentation of all data breaches and provides such documentation to the respective authority upon request.

1.2.13 Privacy by design and by default

Considering the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing each participating company shall take appropriate technical and organisational measures to meet the principles of data protection by design and by default.

For this purpose, participating companies shall adopt internal policies and implement measures aiming at, inter alia, minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency about the functions and processing of personal data, enabling the data subject to monitor the data processing and enabling the controller to create and improve security features.
Processes and procedures shall be designed, developed and implemented in a way that, by default, only personal data which are necessary for each specific purpose of the processing are processed. This obligation applies to (i) the amount of personal data collected, (ii) the extent of their processing, (iii) the period of their storage and (iv) their accessibility.

1.2.14 Commissioned data processing

If participating companies commission another company to process personal data under the terms of these BCR, the following requirements must be observed:

- The processor is to be carefully selected by the controller; only a processor shall be selected that provides necessary guarantees to implement appropriate technical and organizational measures required to perform data processing in compliance with data privacy protection regulations and ensure the protection of the rights of the data subjects;

- The controller shall ensure and regularly verify that the processor remains fully compliant with the agreed technical and organizational security measures;

- The performance of commissioned data processing must be regulated in a written or otherwise documented contract, in which the rights and obligations of the processor are unambiguously defined;

- The processor must be bound by contract to process the data received from the controller only within the contractual framework and in accordance with the documented instructions issued by the controller. The processing of data for the processor's own purposes or for the purposes of a third party must be prohibited by contract, unless processing is required by applicable local law, in which case, the processor shall inform the controller of that legal requirement before processing to the extent permitted by applicable local law;

- The processor shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

  The processor must not engage another processor (subprocessor) without prior specific or general written authorization of the controller. In the former case, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller opportunity to object to such changes. The initial processor remains fully liable to the controller for the performance of the obligations by the subprocessor and its compliance with the provisions of the General Data Protection Regulation and other applicable data protection laws;

- Considering the nature of the processing, the processor shall assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to data subject requests;

- Taking into account the nature of processing and the information available to the processor, the latter shall assist the controller in implementing appropriate technical and organizational measures, immediately inform controller of any data breach and provide information required for the notification of data breaches to supervisory authorities or/and data subjects as well as in other ways support the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the General Data Protection Regulation;

- The processor shall at the choice of the controller, delete or return all the personal data to the controller after the end of the provision of services relating to processing, and delete existing copies unless applicable local laws require storage of the personal data;

- The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations laid down in a written contract concluded between them and established by the applicable data protection provisions and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller;

- The controller retains responsibility for the legitimacy of processing and continues to be the point of contact for data subjects and the supervisory authority.

1.2.15 Rights of data subjects

Data subjects have the inalienable rights listed below in respect of their personal data processed by a participating company within the scope of these BCR.

- The data subject can **demand information** about personal data stored in relation to him/her and the purposes of its processing. The data subject also has the right to information about the identity of the controller, categories of personal data concerned, the recipients or categories of recipients to whom the data have been or may be disclosed and the sources from which the data originate, in case if they were not collected from the data subject. The right to information also covers the envisaged period for which the personal data will be stored and the logical structure of profiling and automated processing operations, to the extent that automated decisions are affected. Furthermore, the data subject shall be provided with information about the existence of the data subject rights according to this section, including the right to lodge a complaint with a supervisory authority.

  The above information needs to be provided in an intelligible form; i.e. the data subject is entitled to obtain a copy of the personal data processed about him/her or at least information about such data in a concise, transparent, intelligible and easily accessible form and in clear and plain language. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form. If requests from the data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either (i) charge a reasonable fee considering the costs of gathering and providing the information or (ii) refuse to act on the request.

- The data subject can demand **rectification,** if his/her personal data are found to be incorrect or incomplete.

- The data subject has the right to demand that his/her personal data be **erased**, (i) if the data processing was unlawful or has become unlawful in the interim, (ii) or as soon as the data is no longer required for the purpose of the processing, (iii) if the data subject withdraws consent on which the processing is based provided that there is no other legal ground for the processing, (iv) in case when the data subjects objects to the processing and there are no overriding legitimate grounds for the processing, or (v) where the erasure obligation is established by local law to which the controller is subject.

  Justified claims by the data subject for erasure are to be acted on, unless the processing is required for (i) compliance with a legal obligation established by local law to which the controller is subject or for (ii) the establishment, exercise or defence of legal claims. In case when the statutory retention periods apply, or the data cannot be erased, the restriction of processing of the data in question may be used upon the request from the data subject.

- The data subject has the right to have processing of personal data **restricted**, where (i) the accuracy of the personal data is contested, for a period enabling the controller to verify the accuracy of the personal data; (ii) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (iii) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims or (iv) in case when the data subject objected to the processing and the verification whether the legitimate grounds of the controller override those of the data subject is pending.

- The data subject has the right to **receive** the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and has the right to transmit those data to another controller, provided that (i) processing of the data is based on consent from the data subject or alternatively on the contract with the data subject and (ii) the processing is carried out by automated means.

- The data subject has the right not to be subject to a decision based solely **on automatic processing,** including profiling, which produces legal effects concerning him or her unless the decision is (i) necessary for entering into or performance of a contract, (ii) is based on the data subject's explicit consent or (iii) authorized by applicable local law.

- The data subject has the right to **object**, on grounds relating to his or her situation, at any time to the processing of his or her personal data which is based on the legitimate interest of the controller or is required for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. The controller must no longer process the personal data in question unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

  The data subject has the right to object at any time to processing of personal data concerning him or her for direct marketing purposes, including profiling to the extent that it is related to such direct marketing. If the data subject objects to processing for direct marketing purposes, the personal data can no longer be processed for such purposes.

- The data subject has the right to lodge a complaint with a supervisory authority.

- The data subject has the right to an effective judicial remedy where he or she considers that his or her rights under the General Data Protection Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with the General Data Protection Regulation.

- If the data processing is based on the consent from the data subject, he or she has the right to withdraw his or her consent at any time.

The data subject can assert the above rights in writing vis-à-vis the participating company, the competent DPC/DPO of the participating company or the CDPD. The justified request of the data subject shall receive a response from the contacted entity within a reasonable period, and the response shall be in written form (e-mail is sufficient).

The participating company must facilitate the exercise of data subject rights listed above. For this purpose, participating company provides the response to the request from the data subject without undue delay and in any event not later than one month following the receipt of the request.

1.2.16 Accountability

All participating companies are required to take measures to demonstrate the compliance with requirements of the General Data Protection Regulation and other applicable data protection provisions, in particular with help of the respective documentation. For this purpose, they shall (i) adhere and implement data privacy and information security policies and regulations, (ii) maintain records of the categories of processing activities, (iii) observe the requirements of data privacy by design and default and, where necessary, (iv) conclude written contracts with data processors or other controllers, (v) designate a data protection officer as well as (vi) carry out data protection impact assessments.

Accountability obligations are ongoing, and the measures taken are to be reviewed and updated regularly.

1.2.17 Description of the data transfer

OSRAM has a complex group structure with a large number of participating companies, between which personal data is exchanged for many purposes. Data exchange takes place between participating companies established in an EEA country, but also with participating companies established outside of the EEA. The need to exchange data throughout the OSRAM group affects personal data of employees, existing and potential customers, suppliers, service providers, shareholders, other business and contracting parties as well as applicants and complainants. These could include – depending on the intended purpose – employee and contract master data, employment data and employment history, data on training or education activities, employee assessments, bank account and credit card information, communication information, some special categories of personal data (e.g. information on marital, religious affiliation, physical and psychical health), etc.
This data is processed and transferred within the OSRAM consolidated group exclusively within the scope of normal business purposes and for purposes of internal administration. Data transfer is thus done for purposes of recruitment, HR administration and staff development, for compliance purposes, for the execution and implementation of assignments and projects for external and internal customers, for the processing of purchase orders and work orders with suppliers and service providers, for the fulfillment of reporting duties, for the fulfillment of accounts payable or collection of accounts receivable, for accounting, for purposes of internal communication, for purposes of consolidation and pooling of IT processes in certain regions in order to reduce costs, and also in connection with the cooperation and coordination of group companies at regional or at a global level in the course of global business transactions and projects.

1.2.18 Procedural issues

1.2.18.1 Binding nature of the BCR

The BCR are comprehensively binding.

1.2.18.1.1 Binding nature for group companies and participating companies

The BCR have been adopted by the responsible governance owners of the OSRAM group and put into effect by publication of guideline CO 3000(BCR for the protection of personal data).

Responsibility for implementation of the BCR in the participating company rests with its executive management, execution in individual cases rests with the entity within that company which processes personal data as part of its specialist role. In OSRAM group companies, responsibility rests with the CEO of the OSRAM group company in his/her capacity as Data Protection Executive (DPE).

The BCR are to be observed and complied with by all OSRAM group companies and by all adopting companies, with binding effect.

In order to document accession to and implementation of the BCR, in the case of group companies, the executive management of the group company in question shall join the ICA. The signing of the ICA and subsequent acceptance of the respective application by OSRAM group parent company makes the BCR regulations individually binding for the group company in question. The ICA is to be signed by the executive management of the group company and returned to the CDPA at the OSRAM group parent company. The ICA is attached as an Annex to the BCR.

In principle, all OSRAM group companies are required to sign and implement the BCR, unless an OSRAM group company has been granted an exemption from implementing the BCR for a valid reason, (e.g. no business activity, no employees, no processing of personal data, imminent liquidation or divestment). An application for an exemption must be submitted by e-mail to the CDPD by the OSRAM group company, citing the reason. The CDPD will decide the merits of the application and will notify the group company of its decision. In this case data transfers between this OSRAM group company and other OSRAM group companies are only possible, if other appropriate safeguards ensuring an adequate level of protection of personal data according to Articles 45-48 of the General Data Protection are taken.

Adopting companies, i.e. companies other than OSRAM group companies, in which the OSRAM group parent company maintains a direct or indirect holding, may voluntarily undertake to comply with the BCR regulations, provided that the CDPD accepts such application. Whether companies other than OSRAM group companies are granted the opportunity to participate voluntarily in the BCR process, is at the complete discretion of the CDPD.

In order to document acceptance and implementation of the BCR by the adopting company, an ICA is concluded between the OSRAM group parent company and the adopting company; the BCR are attached as an Annex to the ICA. Upon conclusion of the ICA, the BCR regulations are individually binding for the adopting company. The text of the ICA is attached as an Annex to the BCR.

The CDPD maintains on the OSRAM intranet an electronic register of participating companies which have given an undertaking to comply with the provisions of the BCR by joining the ICA as well as their contact data. The latest version of the electronic register (status overview) can be viewed at any time on the Intranet at https://privacy.osram.com/DPstatus.

The status overview also includes and identifies accordingly those group companies that have exceptionally been granted exemption from the obligation to sign and implement the BCR for a valid reason. The status overview also records and identifies the group companies that have not (yet) fulfilled their obligation to accept and implement the BCR. The status overview is attached as Annex to the BCR.

If a group company has not (yet) acceded the ICA to the BCR, the legitimacy of data transfer is to be assured through appropriate safeguards, such as by signing and implementing the Standard Contractual Clauses.

The commitment to comply with the BCR can be ended by withdrawal, cancellation or termination on the part of OSRAM group parent company or on the part of the participating company. The loss of group company status does not automatically mean an end to the obligations arising from the BCR. In this case, termination of the BCR by the OSRAM group parent company or the (former) group company is necessary. Also, in the event of withdrawal/cancellation of the ICA or in the event of termination of the BCR, the obligations arising from the BCR with respect to the personal data processed up until withdrawal, cancellation or termination shall remain, until this data has been erased by the company in question, in compliance with the statutory regulations.

1.2.18.1.2 Binding nature vis-à-vis employees of participating companies

Employees of the participating companies are also bound by the regulations of the BCR. The CEO of the particular participating company is obliged to ensure by appropriate means that the BCR have a binding legal effect for the employees.

The BCR regulations and all other regulations relating to data privacy protection are available at all times to the employees of the participating companies.

The participating companies inform their employees that failure to comply with the BCR regulations may result in disciplinary measures or measures under employment law (e.g. formal warning, dismissal) being taken against the employees.

1.2.18.1.3 Binding nature vis-à-vis data subjects

Certain regulations in the BCR are also binding vis-à-vis data subjects, by virtue of third party beneficiary rights. The regulations in the following sections confer benefits on third parties: Sections 1.2.1. – 1.2.7, 1.2.10 – 1.2.15, 1.2.18.1.3, 1.2.18.2, 1.2.18.6, 1.2.18.9, 1.2.18.10 and 1.2.19.

Data subjects are entitled to enforce compliance with one of the above-mentioned third party beneficiary rights by a participating company, by lodging a complaint before the competent supervisory authority or by seeking other legal remedies in the competent courts. Data subjects may claim compensation for damages within this procedure.

Data subjects can choose to lodge their claims

- before the supervisory authority or before the courts in the EEA-country where the participating company that transferred the data is established; or
- before the competent supervisory authority or the courts of the Member States where the data subject has his or her habitual residence or place of work, if the data subject resides in the EEA-country; or
- before the supervisory authority or before the courts in the EEA-country where the headquarters of the OSRAM group parent company are located; or
- before the competent supervisory authority.

This means that in the event of a breach of the BCR regulations by a participating company established outside the EEA, courts and authorities within the EEA are also competent. In these cases, the data subject holds the same rights vis-à-vis the OSRAM group parent company, as if the breach had been committed by the OSRAM group parent company and not by a participating company established outside the EEA.

In order to ensure that data subjects enjoy third party beneficiary rights also in those countries where the granting of third party beneficiary rights in the BCR document is possibly not sufficient, OSRAM will – to the extent necessary – draw up additional contractual agreements with the relevant participating companies. A third party beneficiary clause granting the necessary rights to data subjects is included in the ICA which group companies or adopting companies sign to signify their acceptance and implementation of the BCR.

1.2.18.2 Publicity of BCR

The BCR and the third party beneficiary clause are easily accessible for data subjects. The data subject can contact the competent DPC or DPO of the participating company or alternatively can contact the OSRAM group parent company directly. Along with information listed under subsection 1.2.3 hereof ("Transparency") OSRAM will make the BCR available to the data subjects in an appropriate manner, specifically by publishing the current version of the BCR on the OSRAM internet pages. Additional relevant BCR documents – i.e. the Annexes referenced in the BCR – are provided to the data subject upon request to the CDPD.

1.2.18.3 Implementation of BCR in the participating companies

The executive management of a participating company – or the CEO of a participating group company in his/her capacity as DPE – is responsible for the proper implementation of and compliance with the BCR. The executive management of the participating company may delegate this task – but may not delegate responsibility – to the DPC or the DPO.

OSRAM has established a worldwide network of DPCs and DPOs. On acceding the ICA to the BCR each participating company appoints a DPC or, if required, a DPO and sends the DPC's or DPO's contact details to the CDPD. The participating company shall notify the CDPD without delay of any changes in the identity of the DPC or the DPO.

The DPC or the DPO shall (i) serve as the local contact point for data subjects, i.e. within the framework of the complaint procedure, (ii) oversee the implementation and compliance with the BCR, (iii) consult employees in questions regarding data privacy, (iv) facilitate the cooperation between the CDPD, audit department or supervisory authorities and a participating company in questions and (v) maintain and update necessary records of processing activities and data protection impact assessments for the purposes of the principles of accountability.

The DPO/DPC reports once a year to the executive management of the relevant participating company and DPC reports regularly – but at least once a year – to the CDPD. The DPC/DPO reports on matters including specifically the degree of implementation of the BCR in the individual participating company.

The Head of the CDPD heads the CDPD and coordinates and guides all DPCs and DPOs of participating companies. The Head of the CDPD reports to the CIO of the OSRAM group parent company, the CIO reports to the CFO. The Head of the CDPD coordinates and drives the group-wide BCR implementation in the participating companies, in particular the collection of the ICAs, advice and guidance for the DPC in terms of BCR implementation and collection and evaluation of regular DPC/DPO reports regarding privacy and regarding BCR implementation status.

Furthermore, the Head of the CDPD is in charge of producing and making available adequate BCR trainings for the participating companies. In addition, the Head of the CDPD oversees updating the BCR and of communicating such updates to the competent supervisory authorities. The CDPD supports the Head of the CDPD in the fulfillment of his/her tasks.

The Head of the CDPD reports once a year to the management of the OSRAM group parent company. This report includes specifically the degree of implementation of the BCR in all participating companies.

1.2.18.4 Monitoring of compliance with BCR

Compliance with the BCR by the participating companies is subject to regular review primarily by the DPC or the DPO appointed by executive management of the participating company. Executive management of the participating company supports the DPC in the exercise of his/her duties and involves him/her in the event of complaints being lodged by data subjects for non-compliance with the BCR.

In the event of data privacy breaches and in case of problems of fundamental importance, the DPC/DPO consults the Head of the CDPD and takes account of his/her advice and decisions when remedying personal data breaches and problems.

The OSRAM group parent company is entitled to carry out random checks on the work of the DPC in connection with the implementation of and compliance with the BCR in the participating company, either by requesting a written self-assessment by the DPC/DPO or as part of audit interviews. The content of such audit interviews shall be documented by the auditor.

Any participating company that transfers data has the right to review the data processing at the recipient participating company in individual cases. In so doing, the transferring company will exercise any rights which data subjects are ascertained to have, and will support data subjects, who have suffered damage through violations of the obligations imposed by these BCR, in the assertion of their rights against the company responsible.

1.2.18.5 Training

A key aspect of proper implementation of the BCR is appropriate provision of information and instruction to employees. This includes informing employees that breaches of the BCR may give rise to consequences for them under criminal, liability or employment law.

OSRAM offers specific information and special training measures on the BCR designed to provide adequate information and training to the employees of a participating company on the proper handling and protection of personal data in connection with implementation of the BCR. The training measures are targeted specifically at employees who permanently or regularly handle personal data. For these employees, attendance at training courses is mandatory. Training courses on the BCR are to be repeated at appropriate regular intervals.

Information and training measures can include, for instance, the delivery of web-based training (WBT), the provision of appropriate presentations and training material for self-study, classroom-based training programs and the organization of workshops tailored specifically to employees.

Successful participation by employees in training programs is to be documented.

Further details are set out in a detailed Training Concept.

1.2.18.6 Internal complaint process

Data subjects can contact the competent internal complaint handling department (CDPD); for contact details, see Section 1.2.20 Contact) or the participating company's competent local point of contact for data protection (generally the DPC/DPO), at any time, with complaints about a breach of the BCR by a participating company or with any questions. The data subject shall be given prompt confirmation of receipt of the complaint at the entity contacted and the complaint shall be answered within a reasonable period – in any event within one (1) month of receipt of the complaint. In the confirmation of receipt, the data subject will be informed which entity – i.e. the CDPD or the DPC/DPO – will handle the complaint.

The employees involved with complaint processing in the competent complaint handling department benefit from an appropriate level of independence in the exercise of this function.

In any inquiry, the participating company and CDPD are obligated to cooperate with the supervisory authorities of the country and to respect their judgment.

Further details – form of complaint, processing timescales, procedure following acceptance and/or rejection of complaint, further legal remedies – are set out in a separate Complaint Management Concept.

1.2.18.7 BCR audit

OSRAM has enhanced the existing internal audit and control system with a BCR audit program in order to ensure that compliance with an adequate level of data protection as required in the BCR regulations is subject to regular review in the participating companies.

Primary responsibility for the performance of paper-based audits, regular onsite BCR audits and ad-hoc BCR audits lies with the OSRAM audit department. Alternatively, and where needed, a BCR audit can also be conducted by an accredited external auditor.

The intervals of regular BCR audits are determined and scheduled by the OSRAM audit department in conjunction with their overall audit roadmap.

Once a year, a regular paper-based BCR audit in form of a self-assessment (filling of a questionnaire) takes place in the participating companies. The Head of the CDPD receives the results of such regular self-assessments. The OSRAM audit department is informed about the results.

Under specific circumstances (i.e. data protection incidents, complaints by data subjects, deficiencies detected in the context of the BCR self-assessments), the CDPD or the OSRAM Information Security department (IT DIS) can request additional ad-hoc BCR audits outside the regular audit roadmap for BCR audits.

The BCR audit covers all aspects of the BCR. If a BCR audit concludes that corrective actions need to be taken to remedy a breach of the BCR, the BCR audit shall also ensure that the necessary corrective actions are implemented.

The Head of the CDPD, the responsible member of the OSRAM group parent company management and the executive management of the audited participating company receive the full BCR audit report. The results of the BCR audit are made available to the competent supervisory authority upon request. OSRAM may redact parts of the audit data to the extent necessary to protect confidential company information.

The competent supervisory authority has the right to conduct its own BCR audit of a participating company. The authority may either conduct the BCR audit itself or have it conducted by an accredited independent auditor. An official BCR audit is limited exclusively to compliance with the BCR by the participating company. Due regard shall be given to restrictions arising from confidentiality agreements or from business and trade secrets.

Details of the BCR audit are set out in a separate BCR Audit Concept.

1.2.18.8 BCR updating & change management

OSRAM reserves the right to change and/or update these BCR at any time. Such updating of the BCR may be necessary specifically as a result of changed legal requirements, significant changes to the structure of the OSRAM group or conditions imposed by the competent supervisory authorities.

Major changes to the BCR will require, under certain circumstances, the granting of a new approval by the competent supervisory authorities.

All other changes to the BCR are possible without such new approval providing that the CDPD keeps a fully updated list of the all participating companies and keeps track of and record any updates to the rules and provide the necessary information to the data subjects or supervisory authorities upon request. The list of all operating OSRAM group companies and their BCR acceptance status can be found in OSRAM Intranet at https://privacy.osram.com/DPstatus.

Changes to the BCR are possible without new approval in case no transfer is made to a new participating company until it is effectively bound by the BCR and can deliver compliance.

Any changes to the BCR or to the list of the participating companies should be reported once a year to the competent supervisory authority.

Where a modification would possibly affect the level of the protection offered by the BCR or significantly affect the BCR, it must be promptly communicated to the competent supervisory authority.

The CDPD maintains a list of all changes/updates to the BCR since the BCR came into force. It also maintains a regularly updated list of all participating companies which are effectively bound by the BCR (status overview, cf. Section 1.2.18.1.1). The respective information can be found on OSRAM Intranet at https://privacy.osram.com/DPstatus.

After official BCR approval by the supervisory authority the CDPD will notify these approving authorities of changes to the BCR and changes to the status overview, upon request, but at least once a year. These notifications contain a brief explanation of the reasons justifying the changes.

1.2.18.9 Mutual assistance and cooperation with the supervisory authorities

All participating companies will trustfully cooperate and support one another in the event of inquiries and complaints from data subjects with regard to non-compliance with the BCR.

The participating companies further undertake to trustfully cooperate with the competent supervisory authorities in the context of implementation of the BCR. They will answer BCR-related requests from the supervisory authority within an appropriate timeframe and in an appropriate fashion and will follow the advice and decisions of the competent data protection authority with regard to implementation of the BCR.

1.2.18.10 Relationship between the BCR and local statutory regulations

The legitimacy of processing of personal data is judged on the basis of the applicable local law to which the participating company that originally transferred the data is subject. To the extent that the applicable local law stipulates a higher level of protection of personal data than these BCR, data processing shall be in accordance with the applicable law. Each participating company shall check for itself (e.g. through its data privacy protection officer, DPC/DPO or by the legal department), whether such local statutory regulations (e.g. data privacy laws) exist and shall ensure compliance with these. If the applicable local law provides a lower level of protection for personal data than these BCR, the present BCR shall be applied.

In the event that obligations arising from the applicable local law are in conflict with the BCR, the participating company shall inform the CDPD without delay, unless otherwise prohibited, such as in case of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. The CDPD will record the conflict in the status overview (cf. Section 1.2.18.1.1).

The CDPD will inform all participating companies which previously transferred data to the participating company in question, of the reported conflict between the BCR and the local law. The CDPD will also inform the competent supervisory authority of the regulatory conflict and, together with the data protection authority and the participating company, will seek a practical solution that comes as close as possible to the principles in the General Data Protection Regulation.

The competent supervisory authority shall be in any case notified, where any legal requirement a participating company is subject to is likely to have a substantial adverse effect on the guarantees provided by the BCR, e.g. in case of any legally binding request for disclosure of the personal data by a law enforcement authority or state security body.

If the notification to the CDPD or to the competent supervisory authority is suspended or prohibited under criminal law to preserve the confidentiality of a law enforcement investigation, the participating company use its best efforts to obtain the right to waive this suspension/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 the notification to the competent supervisory authority is not possible, the participating company must annually provide general information on the requests it received to the competent supervisory authority (e.g. indicating number of applications for disclosure, type of data requested, requester if possible, etc.).

The participating company ensures that transfers of personal data to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

1.2.19 Liability

Each participating company is liable for any breach of the BCR committed by the participating company.

In addition, the OSRAM group parent company accepts liability for non-compliance with the BCR by participating companies established outside the EEA, including the undertaking to pay compensation for damages in the event of a proven breach of the BCR and a resulting violation of a data subject's rights caused by such non-compliance of a non-EEA participating company. It furthermore agrees to take the necessary action to remedy the BCR breaches of non-EEA participating companies.

The burden of proof lies with the OSRAM group parent company. It shall demonstrate that no breach of the BCR has taken place or that the participating company established outside the EEA is not liable for the breach of the BCR on which the data subject's claim for damages is based.

If the OSRAM group parent company can prove that the non-EEA participating company is not liable for the violation of the BCR, it may discharge itself from any responsibility.

1.2.20 Contact

Data subjects can raise any concerns with the DPC/DPO of the relevant participating company or with the CDPD:

OSRAM GmbH

Corporate Data Privacy Department
Marcel-Breuer-Str. 6
D-80807 Munich
Phone: +49 (89) 6213-3889
Email: privacy@osram.com
Internet: https://www.osram.com