OSRAM BCR

Binding Corporate Rules („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 an Adoption Agreement;
- **BCR** the present Binding Corporate Rules and the regulations contained in them;
- **CDPO** the OSRAM Chief Data Protection Officer;
- **Consent** a freely given and informed expression of will whereby the data subject agrees to the processing of his/her personal data [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;
- **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 is processed. An identifiable person is one who can be identified, directly or indirectly, e.g. by reference to an identification number; 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 with responsibility for implementation of and compliance with the BCR, appointed by the participating company;
- **DPE** Data Protection Executive of an OSRAM group company; this role is performed by the CEO of the OSRAM group company in question;
- **DP Department** the central department at OSRAM responsible for corporate data protection according to actual organizational chart;
- **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);
- **EU Data Protection Directive** the Directive 95/46/EC of the European Parliament and of the Council of October 24 1995 on the protection of individuals with regard to the processing of personal data and on the free flow of 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;
- **OSRAM group parent company** OSRAM GmbH;
- **Participating company** an OSRAM group company for which implementation of these BCR is mandatory, or an adopting company which voluntarily enters into an Adoption Agreement;
- **Personal data** all information relating to a data subject;
- **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, storage, retention, adaptation, alteration, reading, retrieval, use, disclosure by transmission as well as blocking, erasure or destruction;

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

- **Processor** natural or legal person which processes personal data on behalf of a controller;
- **Third party** any natural or legal person or other entity other than the data subject, processor or controller.

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 EU Data Protection Directive;
- 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 EU Data Protection Directive and thus to assure – with respect to the personal data in scope of these BCR - that an adequate level of data protection and sufficient guarantees are provided within the meaning of the EU Data Protection Directive 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 entry into force of the BCR and the current international data protection requirements, specifically the requirements of the EU Data Protection Directive, the relevant working documents of the EU Article 29 Data Protection Group 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 EU Data Protection Directive;
- 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 future business partners and other data subjects by OSRAM group companies or adopting companies.

Not only personal data from a 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 Substantive principles for the processing of personal data

The following principles which derive specifically from the EU Data Protection Directive and the Madrid Resolution of November 5, 2009 apply to the processing of personal data by participating companies within the scope of these BCR:

1.2.1 Legitimacy & legality of data processing

The processing of personal data shall be done 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 freely given his/her unambiguous, effective consent; or
- Data processing is required for the purpose of creating, executing or terminating a contractual relationship or similar relationship of trust with the data subject; or
- Processing is necessary to safeguard justified interests of the controller and there is no reason for assuming that the data subject has an overriding legitimate interest in precluding data processing; or
- Processing is stipulated or permitted by national law and regulations that apply for the participating company that originally transferred the data; or
- Processing is necessary for compliance with legal obligations to which the controller is subject; or
- Processing is required, exceptionally, to protect the life, health or safety of the data subject.

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

1.2.2 Purpose

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 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. 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 of the controller and of the transferring company
- Categories of recipient or identity of the receiving entity
- Purpose of processing
- Origin of the data (unless this is personal data collected directly from the data subject)
- Right of objection to the processing of personal data of the data subject for advertising purposes
- Other information to the extent required for reasons of equity, e.g. rights of information, rectification and erasure.

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 has already been informed, or if this would involve disproportionate effort.

1.2.4 Data quality and data minimization

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 corrected 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 is no longer required for the business purposes for which it was originally collected and stored, is to be erased. In the event that statutory retention periods apply, the data shall be blocked rather than erased.

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:

- The receiving entity is endowed with an adequate level of protection for personal data within the meaning of Article 25, 26 of the EU Data Protection Directive, e.g. by concluding an EU standard con-

tract (EU Standard Contractual Clauses for Data Processors 2010/87/EU or EU Standard Contractual Clauses between Data Controllers 2011/497/EC or 2004/915/EC) or by concluding other appropriate contractual agreements between the transferring and the receiving entity;
- If the receiving entity is a processor, the conditions set out in Article 16 and 17 of the EU Data Protection Directive must be additionally satisfied.

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 under the following conditions:

- Prior to such onward transfer, the data subject must have been informed in an intelligible form about the intended onward transfer of his personal data (purpose, data exporter, recipient, recipient country, lacking adequate protection level at the recipient); and
- The data subject must have been given the opportunity to object against such onward transfer of his personal data; or
- Where special categories of personal data are concerned, the data subject must have given his prior and unambiguous consent to the onward transfer of such data.

1.2.6 Special categories of personal data

Special categories of personal data, for instance information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or sex life, may 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,

- the data subject is not in a position to give his/her consent (e.g. medical emergency) and processing is necessary to protect the vital interests of the data subject or of another person; or
- processing is required in connection with medical diagnosis, preventive medicine, the provision of care or treatment and the management of healthcare services where data processing is carried out by medical staff who are subject to the obligation of professional secrecy or by other staff subject to an equivalent obligation of secrecy, or
- the data subject has already made public the data in question; or
- processing is necessary for the establishment, exercise or defense of legal claims, provided that there are no grounds for assuming that the data subject has an overriding legitimate interest in ensuring that such data is not processed; or
- processing is expressly permitted by law under the applicable national legislation for the participating company which originally transferred the data (e.g. for the purpose of registering/protecting minorities), and additional guarantees within the meaning of the EU Data Protection Directive are provided for the processing of the data, including specifically adequate security measures for this data.

The competent data privacy protection officer or DPC of the participating company shall be consulted prior to the processing of special categories of personal data.

1.2.7 Automated individual decisions

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 a law.

1.2.8 Data security

Controllers 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 Process IM3000). The current version of the guideline is available on the Intranet.

Specific measures used to ensure adequate protection of personal data include admission controls, system access controls, data access controls, transmission controls, input controls, job controls, availability controls and segregation controls.

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.

1.2.9 Confidentiality of data processing

Only personnel, who 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.

1.2.10 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; a processor shall be selected who is able to ensure the necessary technical and organizational security measures required to perform data processing in compliance with data privacy protection regulations;
- 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 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;

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

1.2.11 Substantive rights of the data subject

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, its origin and the purpose of the processing. The data subject also has the right to information about the identity of the controller and, in the event of the transfer of personal data, the data subject also has the right to information about the recipients or categories of recipient. The right to information also covers the logical structure of automated processing operations, to the extent that automated decisions are affected. 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 an intelligible form. If the local applicable law of the company which originally transferred the data provides such exemption, the data subject does not have a right to information if it would involve considerable impairment of business purposes, including specifically the disclosure of business secrets and the interest in safeguarding the business secrets outweighs the data subject's interest in disclosure. Local legal regulations may restrict the data subject's right to information if this right is exercised repeatedly within a short period of time, unless the data subject can show a legitimate reason for the repeated assertion of claims for information. The participating company may charge the data subject a reasonable fee for providing the information, to the extent that the applicable national law of the participating company which originally transferred the data permits this.
- The data subject can demand **rectification** if his/her personal data is found to be incorrect or incomplete.
- The data subject has the right to demand that his/her personal data be **blocked off** if it is not possible to establish whether the data is correct or incorrect.
- The data subject has the right to demand that his/her personal data be **erased** if the data processing was unlawful or has become unlawful in the interim or as soon as the data is no longer required for the purpose of the processing. Justified claims by the data subject for erasure are to be acted on within a reasonable period, to the extent that statutory retention periods or contractual obligations do not prevent erasure. In the event of statutory retention periods, the data subject may demand that his/her data be blocked rather than erased. The same applies if it would be impossible to erase the data.
- The data subject has the right to **object** – free of charge - to the processing of his/her personal data for advertising purposes or for purposes of market research and/or opinion polling purposes. The data subject shall be informed of his/her right to object.
- The data subject also has a **general right of objection** to the processing of his/her personal data, if because of the data subject's special personal situation, the protectable interest of the data subject outweighs the legitimate interest the controller has in processing the personal data.

The data subject can assert the above rights in writing vis-à-vis the participating company, the competent DPC of the participating company or the DP Department of the OSRAM group parent company. 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).

1.2.12 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 and also with participating companies established outside the EEA.

The need to exchange data throughout the OSRAM group affects personal data of employees, customers, suppliers, shareholders and other business partners and contracting parties. This includes – depending on the intended purpose – for example, name, Global Identifier, date of birth, nationality, marital status, gender, contact details, address details, account details, bank details, religious affiliation, information about education, knowledge and skills, career, entry date, position level, 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.

1.2.13 Procedural issues

1.2.13.1 Binding nature of the BCR

The BCR are comprehensively binding.

1.2.13.1.1 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 IM4000 (BCR for the protection of personal data).

Responsibility for implementation of the BCR in the participating company rests with executive management of the participating company, 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 acceptance and implementation of the BCR, in the case of group companies, the executive management of the group company in question shall issue an explicit written Declaration of Commitment to the regulations of the BCR. The issuing of this written Declaration of Commitment makes the BCR regulations individually binding for the group company. The Declaration of Commitment is to be signed by the executive management of the group company and returned to the DP Department of the OSRAM group parent company. The Declaration of Commitment 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 DP Department by the OSRAM group company, citing the reason. The DP Department will decide the merits of the application and will notify the group company of its decision.

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 make a legally binding commitment to comply with BCR regulations, if the company so wishes and if the DP Department agrees to such participation. 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 DP Department.

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

The DP Department 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 signing a Declaration of Commitment or Adoption Agreement. The latest version of the electronic register (status overview) can be viewed at any time on the Intranet. 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.

If a group company has not (yet) issued a Declaration of Commitment to the BCR, the legitimacy of data transfer to that group company is to be reviewed in each individual case and is to be assured through appropriate special measures, such as by the signature of the EC 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 Declaration of Commitment or of the declaration to conclude the Adoption Agreement 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.

1.2.13.1.2 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 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.

1.2.13.1.3 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. – 1.2.10, 1.2.11, 1.2.13.1.3, 1.2.13.6, 1.2.13.9, 1.2.13.10 and 1.2.14.

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 data protection 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 jurisdiction of the participating company located in an EEA country that transferred the data; or
- before the jurisdiction of the headquarters of the OSRAM group parent company; or
- before the competent data protection 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.

The competence of courts and authorities in the EEA as described above does not apply, however, if the data recipient is established in a country outside the EAA but that country does have an adequate level of data protection as acknowledged by a decision of the EU Commission.

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 Declaration of Commitment which group companies sign to signify their acceptance and implementation of the BCR. The same applies for the Adoption Agreement which the adopting companies conclude with the OSRAM group parent company.

1.2.13.2 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 of the participating company or alternatively can contact the OSRAM group parent company directly. 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 - will be provided to the data subject upon request to the DP Department.

1.2.13.3 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.

OSRAM has established a worldwide network of DPCs. On issuing the Declaration of Commitment to the BCR or concluding the Adoption Agreement on the BCR, each participating company appoints a DPC and sends the DPC's contact details to the DP Department. The participating company shall notify the DP Department without delay of any changes in the identity of the DPC.

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

The CDPO heads the DP Department and coordinates and guides all DPC of participating companies. The CDPO reports to the CIO of the OSRAM group parent company, the CIO reports to the CFO. The CDPO coordinates and drives the group-wide BCR implementation in the participating companies, in particular the collection of BCR commitment forms and BCR Adoption Agreements, advice and guidance for the DPC in terms of BCR implementation and collection and evaluation of regular DPC reports regarding privacy and regarding BCR implementation status. Furthermore, the CDPO is in charge of producing and making available adequate BCR trainings for the participating companies. In addition, the CDPO is in charge of updating the BCR and of communicating such updates to the relevant data protection authorities. The DP Department supports the CDPO in the fulfillment of his tasks.

The CDPO 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.

1.2.13.4 Monitoring of compliance with BCR

Compliance with the BCR by the participating companies is subject to regular review primarily by the DPC 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 serious data privacy breaches and on problems of fundamental importance, the DPC consults the CDPO and takes account of his/her advice and decisions when remedying such data privacy 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 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.

1.2.13.5 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.

1.2.13.6 Internal complaint process

Data subjects can contact the competent internal complaint handling department (DP Department; for contact details, see Section 1.2.15 Contact 0) or the participating company's competent local point of contact for data protection (generally the DPC), 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 – at the latest within three (3) months of receipt of the complaint. In the confirmation of receipt the data subject will be informed which entity – i.e. the DP Department or the DPC – 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 CDPO are obligated to cooperate with the data protection 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.

1.2.13.7 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 CDPO 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 CDPO 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 CDPO, 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 data protection authority upon request. OSRAM may redact parts of the audit data to the extent necessary to protect confidential company information.

The competent data protection 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.

1.2.13.8 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 data protection authorities.

Major changes to the BCR will require, under certain circumstances, the granting of a new approval by the competent data protection authorities. All other changes to the BCR are possible without such new approval.

The DP Department 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 1.2.13.1.1).

After official BCR approval by the data protection authority the CDPO will notify these approving authorities of changes to the BCR and also 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.

1.2.13.9 Mutual assistance and cooperation with the data protection 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 data protection authorities in the context of implementation of the BCR. They will answer BCR-related requests from the data protection 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.

1.2.13.10 Relationship between 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 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 CDPO without delay. He/she will record the reported conflict in the status overview (cf. Section 1.2.13.1.1).

The DP Department 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 DP Department will also inform the competent data protection authority of the regulatory conflict and, together with the data pro-

tection authority and the participating company, will seek a practical solution that comes as close as possible to the principles in the EU Data Protection Directive.

1.2.14 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.

1.2.15 Contact

Data subjects can raise any concerns with the DPC of the relevant participating company or with the OSRAM CDPO (Chief Data Protection Officer):

OSRAM GmbH
Department for Data Protection
Marcel-Breuer-Str. 6
D- 80807 Munich
Phone:+49 (0) 89 6213-4978
Fax:+49 (0) 89 6213-2036
Email: privacy@osram.com
Internet: http://www.osram.com