OSRAM BCR
Bindende Unternehmensrichtlinie (Binding Corporate Rules - „BCR“) für OSRAM-Konzerngesellschaften und beitretende Gesellschaften zum Schutz personenbezogener Daten

Definitionen

- **Auftragsdatenverarbeiter** die natürliche oder juristische Person, die personenbezogene Daten im Auftrag für eine verantwortliche Stelle verarbeitet;
- **BCR** die vorliegenden Binding Corporate Rules und die darin enthaltenen Regelungen;
- **Beitretende Gesellschaft** eine in- oder ausländische OSRAM-Beteiligungsgesellschaft, an der die OSRAM Konzernobergesellschaft oder ein verbundenes Unternehmen eine Minderheitsbeteiligung hält und die sich mit Zustimmung der OSRAM Konzernobergesellschaft auf freiwilliger Basis durch den Abschluss eines Beitrittsvertrages auf die Regelungen der BCR verpflichtet hat;
- **Betroffener** jede bestimmte oder bestimmbare natürliche Person, deren Daten verarbeitet werden. Bestimmbar ist eine Person dann, wenn sie direkt oder indirekt identifiziert werden kann, z. B. durch Zuordnung zu einer Kennziffer; juristische Personen können durch entsprechende Vereinbarung zwischen der datenübermittelnden Gesellschaft und dem Datenempfänger in den Geltungsbereich der BCR einbezogen werden und gelten insoweit als Betroffene;
- **CDPO** den OSRAM Chief Data Protection Officer (Konzerndatenschutzbeauftragter);
- **DPC** den Data Protection Coordinator, d.h. die Person, die von der teilnehmenden Gesellschaft als für die Umsetzung und Einhaltung der BCR zuständige Person benannt wurde;
- **DPE** den Data Protection Executive einer Konzerngesellschaft; diese Position wird vom jeweiligen CEO der Konzerngesellschaft wahrgenommen;
- **DS Abteilung** die gemäß OSRAM Organisationsplan für den konzernweiten Datenschutz zuständige zentrale Abteilung des OSRAM Konzerns;
- **Dritter** jede natürliche oder juristische Person oder andere Stelle, die nicht Betroffener, Auftragsdatenverarbeiter oder der verantwortlichen Stelle zuzurechnen ist;
- **Einwilligung** eine ohne Zwang und in Kenntnis der Sachlage erfolgte Willensäußerung, mit der der Betroffene akzeptiert, dass seine personenbezogenen Daten verarbeitet werden[*)];
- **EU-Datenschutzrichtlinie** die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr;
- **EWR-Land / EWR-Länder** die Mitgliedsstaaten der Europäischen Union (EU) sowie die anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (EWR);
- **Konzerngesellschaft bzw. OSRAM-Konzerngesellschaft** die OSRAM Konzernobergesellschaft und jede in- oder ausländische Gesellschaft, an denen die OSRAM Konzernobergesellschaft direkt oder indirekt mit Mehrheit beteiligt ist bzw. die Mehrheit der Stimmrechte oder die Managementkontrolle besitzt;
- **Kunden und Lieferanten** die natürlichen und juristischen Personen, mit denen eine Geschäftsbeziehung besteht oder geplant ist;

[*)] *Besondere Anforderungen an eine Einwilligung können sich aus dem jeweiligen nationalen Recht ergeben und für die Wirksamkeit der Einwilligung bedeutsam sein.*

- **OSRAM Konzern** die OSRAM Konzernobergesellschaft sowie alle OSRAM-Konzerngesellschaften;
- **OSRAM Konzernobergesellschaft** die OSRAM GmbH;
- **Personenbezogene Daten** alle Informationen über einen Betroffenen;
- **Teilnehmende Gesellschaft** eine OSRAM-Konzerngesellschaft, für die die Umsetzung dieser BCR verpflichtend ist, oder eine Gesellschaft, die sich auf freiwilliger Basis durch den Abschluss eines Beitrittsvertrages auf die Regelungen der BCR verpflichtet hat („beitretende Gesellschaft“);
- **Übermittlung personenbezogener Daten** oder **Datenübermittlung** die Weitergabe personenbezogener Daten, ihre Verbreitung oder jede Form der Bereitstellung zur Ansicht oder zum Abruf an Dritte;
- **Verantwortliche Stelle** die Stelle (natürliche oder juristische Person, Behörde oder sonstige rechtlich selbständige Stelle), die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Datenverarbeitung entscheidet;
- **Verarbeitung personenbezogener Daten** oder **Datenverarbeitung** jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten - wie etwa das Erheben, Speichern, die Aufbewahrung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Nutzung, die Weitergabe durch Übermittlung sowie das Sperren, Löschen oder Vernichten.

Zusammenfassung der OSRAM BCR

Primäres Ziel dieser Binding Corporate Rules („BCR“) ist es, ein weltweit angemessenes und einheitliches Datenschutzniveau innerhalb des gesamten OSRAM Konzerns bzw. bei allen teilnehmenden Gesellschaften herzustellen und damit den adäquaten Schutz von personenbezogenen Daten, die im Geschäftsablauf von einer teilnehmenden Gesellschaft an andere teilnehmende Gesellschaften übermittelt werden, weltweit sicherzustellen. Unter den Anwendungsbereich dieser BCR fallen dabei folgende personenbezogene Daten:

- Personenbezogene Daten aus der EU / dem EWR, auf die die EU-Datenschutzrichtlinie Anwendung findet;
- Personenbezogene Daten ungeachtet ihres Herkunftslandes, sofern sie von einer (datenerhebenden) teilnehmenden Gesellschaft an eine andere (empfangende) teilnehmende Gesellschaft übermittelt wurden.

Hierfür ist es erforderlich, für die Verarbeitung personenbezogener Daten einheitliche Datenschutz- und Datensicherheitsstandards im Sinne der EU-Datenschutzrichtlinie festzulegen und so sicherzustellen, dass im Hinblick auf die unter den Schutzbereich dieser BCR fallenden personenbezogenen Daten weltweit ein angemessenes Datenschutzniveau und ausreichende Garantien im Sinne der EU-Datenschutzrichtlinie hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte gewährleistet werden.

Diese BCR stellen das generelle und allgemeingültige Rahmenregelwerk für die Verarbeitung der unter den Anwendungsbereich der BCR fallenden personenbezogenen Daten von Mitarbeitern, Kunden, Lieferanten, Geschäftspartnern oder künftigen Geschäftspartnern sowie sonstiger Betroffener durch OSRAM-Konzerngesellschaften oder beitretende Gesellschaften dar.

Die vorliegenden BCR berücksichtigen den derzeitigen Stand und die aktuellen Vorgaben im internationalen Datenschutz, insbesondere die Anforderungen der EU-Datenschutzrichtlinie, die einschlägigen Arbeitsdokumente der Art. 29 Datenschutzgruppe der EU sowie die Grundsätze der Internationalen Konferenz der Datenschutzbeauftragten über Internationale Standards zum Schutz der Privatsphäre (im folgenden: "Madrid -Resolution") vom 5. November 2009.

1. Inhalt der Richtlinie

1.1 Anwendungsbereich der BCR

Alle OSRAM-Konzerngesellschaften und beitretende Gesellschaften weltweit fallen in den Anwendungsbereich dieser bindenden Unternehmensrichtlinie.

Die BCR gelten für die Verarbeitung

- aller personenbezogenen Daten aus der EU / dem EWR, auf die die EU-Datenschutzrichtlinie Anwendung findet;

- personenbezogener Daten ungeachtet ihres Herkunftslandes, sofern sie von einer (datenerhebenden) teilnehmenden Gesellschaft an eine andere (empfangende) teilnehmende Gesellschaft übermittelt wurden.

Erfasst werden personenbezogene Daten von Mitarbeitern, Kunden, Lieferanten, Aktionären sowie von allen sonstigen – gegenwärtigen oder künftigen - Vertrags- und Geschäftspartnern der teilnehmenden Gesellschaften und sonstiger Betroffener.

Unter den Schutzbereich der BCR fallen dementsprechend nicht nur personenbezogene Daten aus teilnehmenden Gesellschaften mit Sitz in einem EWR-Land, sondern darüber hinaus weltweit **alle** von einer teilnehmenden Gesellschaft stammenden personenbezogenen Daten, sobald diese Daten an eine andere teilnehmende Gesellschaft übermittelt wurden (und damit auch personenbezogene Daten, die von einer teilnehmenden Gesellschaft mit Sitz außerhalb des EWR herrühren und dann an eine andere teilnehmende Gesellschaft übermittelt werden).

1.2 Materielle Grundsätze für die Verarbeitung personenbezogener Daten

Bei der Verarbeitung personenbezogener Daten durch teilnehmende Gesellschaften im Rahmen dieser BCR gelten die folgenden Grundsätze, die sich insbesondere aus der EU-Datenschutzrichtlinie und der Madrid-Resolution vom 5. November 2009 ableiten:

1.2.1 Zulässigkeit & Gesetzmäßigkeit der Datenverarbeitung

Die Verarbeitung der personenbezogenen Daten hat gesetzeskonform unter Einhaltung der jeweils geltenden gesetzlichen Bestimmungen sowie unter Beachtung der in diesen BCR niedergelegten Prinzipien zu erfolgen.

Sie ist nur zulässig, wenn mindestens eine der folgenden Voraussetzungen erfüllt ist:

- Der Betroffene hat freiwillig und eindeutig eine wirksame Einwilligung erteilt; oder
- Die Datenverarbeitung ist zur Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich; oder
- Die Verarbeitung ist zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich und es besteht kein Grund zu der Annahme, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung überwiegt; oder
- Die Verarbeitung wird durch für die übermittelnde teilnehmende Gesellschaft geltende nationale Rechtsvorschriften angeordnet oder erlaubt; oder
- Die Verarbeitung ist erforderlich für die Einhaltung rechtlicher Verpflichtungen, denen die Verantwortliche Stelle unterliegt; oder
- Die Verarbeitung ist ausnahmsweise nötig, um das Leben, die Gesundheit oder die Sicherheit des Betroffenen zu schützen.

Die Verantwortliche Stelle muss es dem Betroffenen ermöglichen, auf einfache, schnelle und effiziente Weise jederzeit seine Einwilligung widerrufen zu können.

1.2.2 Zweckbestimmung

Personenbezogene Daten dürfen ausschließlich für spezifische, eindeutig festgelegte und rechtmäßige Zwecke verarbeitet werden. In keinem Fall dürfen personenbezogene Daten auf eine Weise verarbeitet werden, die mit den legitimen Zwecken, für die die personenbezogenen Daten erhoben wurden, nicht vereinbar wären. Teilnehmende Gesellschaften sind verpflichtet, die Zweckbestimmung der von einer anderen teilnehmenden Gesellschaft an sie übermittelten Daten bei der Speicherung und weiteren Verarbeitung und Nutzung dieser Daten zu beachten; Zweckänderungen sind nur mit Einwilligung des Betroffenen zulässig oder soweit das jeweilige nationale Recht der übermittelnden teilnehmenden Gesellschaft dies zulässt.

1.2.3 Transparenz

Jede teilnehmende Gesellschaft hat personenbezogene Daten auf transparente Art und Weise zu verarbeiten. Betroffene, deren personenbezogene Daten von einer teilnehmenden Gesellschaft verarbeitet werden, müssen von der teilnehmenden Gesellschaft (ggf. in Absprache mit der übermittelnden Gesellschaft) über folgendes informiert

werden:

- Identität der Verantwortlichen Stelle und der übermittelnden Gesellschaft
- Kategorien von Empfängern oder Identität der empfangenden Stelle
- Zweck der Verarbeitung
- Herkunft der Daten (sofern keine Direkterhebung der personenbezogenen Daten beim Betroffenen erfolgt ist)
- Widerspruchsrecht gegen die Verarbeitung personenbezogener Daten des Betroffenen für Zwecke der Werbung
- andere Informationen, sofern dies aus Billigkeitsgründen erforderlich ist, z.B. Auskunfts-, Berichtigungs- und Löschungsrechte.

Soweit die personenbezogenen Daten nicht direkt beim Betroffenen erhoben wurden, kann die Information ausnahmsweise unterbleiben, wenn der Betroffene bereits informiert ist oder damit ein unverhältnismäßiger Aufwand verbunden wäre.

1.2.4 Datenqualität und Datensparsamkeit

Personenbezogene Daten müssen sachlich richtig sein und – wenn nötig – auf den neuesten Stand gebracht werden. Es sind angemessene Maßnahmen dafür zu treffen, dass nicht zutreffende oder unvollständige Daten berichtigt oder gelöscht werden.

Die Datenverarbeitung hat sich am Ziel der Datensparsamkeit auszurichten. Es sollen nur die erforderlichen personenbezogenen Daten - d. h. so wenig personenbezogene Daten wie möglich - erhoben, verarbeitet oder genutzt werden. Insbesondere ist von den Möglichkeiten der Anonymisierung Gebrauch zu machen, soweit der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht. Statistische Auswertungen oder Untersuchungen, die auf der Basis anonymisierter Daten erfolgen, sind nicht datenschutzrelevant, soweit die Daten den Rückschluss auf den Betroffenen nicht mehr ermöglichen.

Personenbezogene Daten, die für die Geschäftszwecke, für die sie ursprünglich erhoben und gespeichert wurden, nicht mehr benötigt werden, sind zu löschen. Im Falle gesetzlicher Aufbewahrungsfristen sind die Daten anstelle der Löschung zu sperren.

1.2.5 Weiterübermittlung von Daten

Die Weiterübermittlung von personenbezogenen Daten von einer teilnehmenden Gesellschaft an eine nicht teilnehmende Gesellschaft ist nur unter den folgenden Voraussetzungen zulässig:

- Die empfangende Stelle gewährleistet ein angemessenes Datenschutzniveau im Sinne von Art. 25, 26 der EU-Datenschutzrichtlinie, z.B. durch den Abschluss von EU Standardvertragsklauseln (EU Standardvertragsklauseln 2010/87/EU für Auftragsdatenverarbeiter bzw. EU Standardvertragsklauseln 2001/497/EG oder 2004/915/EG zwischen für die Datenverarbeitung Verantwortlichen) oder durch den Abschluss sonstiger geeigneter vertraglicher Vereinbarungen zwischen der übermittelnden und der empfangenden Stelle;
- Sofern es sich bei der empfangenden Stelle um einen Auftragsdatenverarbeiter handelt, müssen die Voraussetzungen der Artikel 16 und 17 der EU-Datenschutzrichtlinie ergänzend erfüllt werden.

Die Weiterübermittlung personenbezogener Daten, die eine teilnehmende Gesellschaft mit Sitz in einem Nicht-EWR-Land (= Datenimporteur) von einer anderen teilnehmenden Gesellschaft mit Sitz in einem EWR-Land (= Datenexporteur) erhalten hat, durch den Datenimporteur an einen für die Verarbeitung verantwortlichen, externen Empfänger außerhalb der OSRAM Gruppe mit Sitz in einem Nicht-EWR-Land ohne angemessenes bzw. anerkanntes Datenschutzniveau ist nur unter folgenden Voraussetzungen zulässig:

- Der Betroffene muss vor der Weiterübermittlung seiner personenbezogenen Daten in verständlicher Weise über die beabsichtigte Weiterübermittlung informiert worden sein (Zweck, Datenexporteur, Empfänger, Empfängerländer, fehlendes angemessenes Datenschutzniveau beim Empfänger); und
- Dem Betroffenen muss die Möglichkeit gegeben worden sein, der Weiterübermittlung seiner personenbezogenen Daten zu widersprechen; bzw.
- Soweit es sich um besondere Arten personenbezogener Daten handelt, muss der Betroffene seine aus-

drückliche Zustimmung zur Weiterübermittlung der Daten erteilt haben.

1.2.6 Besondere Arten personenbezogener Daten

Die Verarbeitung besonderer Arten personenbezogener Daten, also von Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben, ist grundsätzlich untersagt.

Sollte die Verarbeitung besonderer Arten personenbezogener Daten erforderlich sein, muss der Betroffene hierin ausdrücklich einwilligen, es sei denn,

- der Betroffene ist nicht in der Lage, seine Einwilligung zu geben (z. B. medizinischer Notfall) und die Verarbeitung ist erforderlich, um die vitalen Interessen des Betroffenen oder einer anderen Person zu wahren; oder
- die Verarbeitung ist erforderlich im Zusammenhang mit medizinischer Diagnose, Gesundheitsvorsorge oder der Behandlung oder der Verwaltung von Gesundheitsdiensten ; wobei die Datenverarbeitung durch medizinisches Personal erfolgt, das dem Berufsgeheimnis unterworfen ist oder durch sonstiges, einer entsprechenden Geheimhaltungspflicht unterworfenes Personal, oder
- der Betroffene hat die betreffenden Daten bereits selber öffentlich gemacht; oder
- die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich, wenn kein Grund zur Annahme besteht, dass schutzwürdige Interessen des Betroffenen an dem Ausschluss der Verarbeitung überwiegen; oder
- die Verarbeitung ist nach dem für die übermittelnde teilnehmende Gesellschaft anwendbaren nationalen Recht ausdrücklich gesetzlich erlaubt (z. B. zum Zweck der Erfassung bzw. des Schutzes von Minderheiten), und bei der Verarbeitung der Daten werden zusätzliche Garantien im Sinne der EU-Datenschutzrichtlinie, wie insbesondere angemessene Sicherheitsmaßnahmen für diese Daten, erbracht.

Vor der Verarbeitung besonderer Arten personenbezogener Daten ist der zuständige Datenschutzbeauftragte bzw. DPC der teilnehmenden Gesellschaft zu konsultieren

1.2.7 Automatisierte Einzelentscheidungen

Werden personenbezogene Daten mit dem Ziel verarbeitet, eine automatisierte Einzelentscheidung zu treffen, müssen die berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet werden. Entscheidungen, die für den Betroffenen negative rechtliche Folgen nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten, die der Bewertung einzelner Persönlichkeitsmerkmale dient, gestützt, d.h. nicht ausschließlich durch Verwendung von Informationstechnik getroffen werden. Automatisierte Verfahren dürfen grundsätzlich nur als Hilfsmittel für eine solche Entscheidung genutzt werden.

Eine Ausnahme gilt nur, wenn

- die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertrages getroffen wird und die berechtigten Interessen des Betroffenen durch Information über die Logik der Entscheidung und die Möglichkeit zur Stellungnahme gewahrt werden, wobei für den Fall einer Stellungnahme des Betroffenen die verantwortliche Stelle verpflichtet ist, ihre Entscheidung zu überprüfen; oder
- sofern diese durch ein Gesetz zugelassen ist.

1.2.8 Datensicherheit

Die Verantwortlichen Stellen haben die zur Gewährleistung der erforderlichen Datensicherheit angemessenen technisch-organisatorischen Maßnahmen zu treffen, die die personenbezogenen Daten gegen unbeabsichtigte oder unrechtmäßige Löschung, unrechtmäßige Verwendung, Veränderung, gegen Verlust, Zerstörung und gegen unberechtigte Weitergabe oder unberechtigten Zugriff schützen. Besondere Arten personenbezogener Daten sind besonders zu schützen.

Die Sicherheitsmaßnahmen sollen ein der Art der verarbeiteten Daten sowie den mit ihrer Verarbeitung verbundenen Risiken angemessenes Sicherheitsniveau herstellen und sich dabei am Stand der Technik in der Datensicherheit orientieren.

Die vorzusehenden Sicherheitsmaßnahmen beziehen sich insbesondere auf Rechner (Server und Arbeitsplatzrechner), Netze bzw. Kommunikationsverbindungen sowie Applikationen.

Zur Sicherstellung eines angemessenen Niveaus technischer und organisatorischer Maßnahmen für den Datenschutz sind die **Regeln zur Informationssicherheit** (OSRAM Richtlinie IM3000) konzernweit verbindlich eingeführt. Das aktuell gültige Regelwerk zur Informationssicherheit ist im Intranet abrufbar.

Zum angemessenen Schutz personenbezogener Daten werden insbesondere Zutrittskontrollen, Zugangskontrollen, Zugriffskontrollen, Weitergabekontrollen, Eingabekontrollen, Auftragskontrollen, Verfügbarkeitskontrollen und Trennungskontrollen eingesetzt.

Alle Arbeitsplatzrechner – inklusive mobiler Geräte (z.B. Laptops) - sind passwortgeschützt. Das OSRAM-Intranet verfügt über ein Firewallsystem zum Schutz vor unberechtigtem externem Zugriff auf unternehmensinterne Inhalte. Die Übermittlung personenbezogener Daten innerhalb des unternehmenseigenen Netzwerks erfolgt – soweit aufgrund der Natur und des Verwendungszwecks der personenbezogenen Daten erforderlich – in der Regel verschlüsselt.

1.2.9 Vertraulichkeit der Datenverarbeitung

Nur befugte und auf die Einhaltung des Datenschutzes besonders hingewiesene Mitarbeiter dürfen personenbezogene Daten erheben, verarbeiten oder nutzen. Die Zugriffsberechtigung des jeweiligen Mitarbeiters ist dabei nach Art und Umfang seines spezifischen Tätigkeitsfeldes zu begrenzen. Es ist dem Mitarbeiter untersagt, personenbezogene Daten für private Zwecke zu nutzen, an Unbefugte zu übermitteln oder diesen auf andere Weise zugänglich zu machen. Unbefugt in diesem Sinne sind z. B. auch andere Mitarbeiter, sofern und soweit diese die personenbezogenen Daten nicht zur Erledigung der ihnen obliegenden Fachaufgaben benötigen. Die Vertraulichkeitsverpflichtung besteht über das Ende des Beschäftigungsverhältnisses des betroffenen Mitarbeiters hinaus fort.

1.2.10 Datenverarbeitung im Auftrag

Wenn teilnehmende Gesellschaften eine andere Gesellschaft mit der Verarbeitung personenbezogener Daten im Rahmen dieser BCR beauftragen, sind folgende Maßgaben zu beachten:

- Der Auftragsdatenverarbeiter ist von der Verantwortlichen Stelle sorgfältig auszuwählen; es ist ein Auftragsdatenverarbeiter auszuwählen, der die für die datenschutzgerechte Verarbeitung erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen gewährleisten kann;
- Die Verantwortliche Stelle hat dafür Sorge zu tragen und sich regelmäßig davon zu überzeugen, dass der Auftragsdatenverarbeiter die vereinbarten technischen und organisatorischen Sicherheitsmaßnahmen vollumfänglich einhält;
- Die Durchführung der Datenverarbeitung im Auftrag muss in einem schriftlich oder anderweitig dokumentierten Vertrag geregelt werden, in dem die Rechte und Pflichten des Auftragsdatenverarbeiters eindeutig festgelegt werden;
- Der Auftragsdatenverarbeiter ist vertraglich zu verpflichten, die vom Auftraggeber erhaltenen Daten nur im Rahmen des Auftrages und der vom Auftraggeber erteilten Weisungen zu verarbeiten. Verarbeitungen zu eigenen Zwecken oder zu Zwecken Dritter müssen vertraglich ausgeschlossen werden;
- Der Auftraggeber bleibt für die Zulässigkeit der Verarbeitung verantwortlich und ist weiterhin Ansprechpartner für den Betroffenen.

1.2.11 Materielle Rechte des Betroffenen

Der Betroffene hat hinsichtlich seiner im Geltungsbereich dieser BCR durch eine teilnehmende Gesellschaft verarbeiteten personenbezogenen Daten die nachfolgend aufgeführten, unabdingbaren Rechte.

- Der Betroffene kann **Auskunft** über die zu seiner Person gespeicherten Daten, deren Herkunft sowie den Zweck der Verarbeitung verlangen. Der Betroffene kann ferner Auskunft über die Identität der Verantwortlichen Stelle sowie – im Falle einer Übermittlung personenbezogener Daten - Auskunft über die Empfänger oder Kategorien von Empfängern verlangen. Das Auskunftsrecht umfasst weiterhin den logischen Aufbau automatisierter Verarbeitungen, soweit automatisierte Entscheidungen betroffen sind. Die Auskunft hat in verständlicher Form zu erfolgen, d.h. der Betroffene hat Anspruch auf eine

Kopie der über ihn verarbeiteten personenbezogenen Daten bzw. auf die Darstellung dieser Daten in einer nachvollziehbaren Form. Sofern dies gemäß dem für die übermittelnde teilnehmende Gesellschaft anwendbaren nationalen Recht zulässig ist, entfällt das Auskunftsrecht des Betroffenen, wenn damit eine erhebliche Gefährdung der Geschäftszwecke – wie insbesondere die Offenbarung von Geschäftsgeheimnissen - verbunden wäre und das Interesse an der Wahrung der Geschäftsgeheimnisse gegenüber dem Auskunftsinteresse des Betroffenen überwiegt. Lokalrechtliche Vorschriften können das Auskunftsrecht des Betroffenen überdies beschränken, wenn dieses innerhalb kurzer Zeit wiederholt ausgeübt wird, es sei denn, der Betroffene kann einen legitimen Grund für die wiederholte Geltendmachung von Auskunftsansprüchen vorbringen. Die teilnehmende Gesellschaft kann vom Betroffenen für die Auskunftserteilung eine angemessene Gebühr verlangen, sofern und soweit das für die übermittelnde teilnehmende Gesellschaft anwendbare nationale Recht dies gestattet.

- Der Betroffene kann **Berichtigung** seiner personenbezogenen Daten verlangen, wenn sich herausstellt, dass diese unrichtig oder unvollständig sind.
- Der Betroffene hat ein Recht auf **Sperrung** seiner personenbezogenen Daten, wenn sich weder deren Richtigkeit noch deren Unrichtigkeit feststellen lässt.
- Der Betroffene hat einen Anspruch auf **Löschung** seiner personenbezogenen Daten, wenn die Datenverarbeitung unzulässig war oder in der Zwischenzeit unzulässig geworden ist oder sobald die Daten für den Verarbeitungszweck nicht mehr erforderlich sind. Berechtigte Löschungsansprüche des Betroffenen sind innerhalb angemessener Frist umzusetzen, sofern und soweit keine gesetzlichen Aufbewahrungsfristen oder vertragliche Verpflichtungen einer Löschung entgegenstehen. Im Falle gesetzlicher Aufbewahrungsfristen kann der Betroffene statt der Löschung eine Sperrung seiner Daten verlangen. Gleiches gilt, wenn die Löschung der Daten unmöglich wäre.
- Der Betroffene hat das Recht, der Verarbeitung seiner personenbezogenen Daten zu Werbezwecken sowie zu Zwecken der Markt- und/oder Meinungsforschung kostenfrei zu **widersprechen**. Der Betroffene ist über sein Widerspruchsrecht zu informieren.
- Der Betroffene hat ferner ein **allgemeines Widerspruchsrecht** gegen die Verarbeitung seiner personenbezogenen Daten, wenn ein schutzwürdiges Interesse des Betroffenen aufgrund seiner besonderen persönlichen Situation das legitime Interesse der Verantwortlichen Stelle an einer Verarbeitung der personenbezogenen Daten überwiegt.

Der Betroffene kann die vorgenannten Rechte gegenüber der teilnehmenden Gesellschaft, dem zuständigen DPC der teilnehmenden Gesellschaft oder aber gegenüber der für den konzernweiten Datenschutz zuständigen zentralen Abteilung (DS Abteilung) der OSRAM Konzernobergesellschaft schriftlich geltend machen. Das berechtigte Ersuchen des Betroffenen ist von der kontaktierten Stelle innerhalb einer angemessenen Frist zu beantworten, und zwar grundsätzlich in schriftlicher Form (E-Mail ist ausreichend).

1.2.12 Beschreibung der Datentransfers

OSRAM verfügt über eine komplexe Konzernstruktur mit einer Vielzahl von teilnehmenden Gesellschaften, zwischen denen personenbezogene Daten für eine Vielzahl von Zwecken ausgetauscht werden. Ein Datenaustausch erfolgt dabei sowohl zwischen teilnehmenden Gesellschaften mit Sitz in einem EWR-Land als auch mit oder zwischen teilnehmenden Gesellschaften mit Sitz außerhalb des EWR.

Betroffen von den konzernweiten Datenaustauschnotwendigkeiten sind personenbezogene Daten von Mitarbeitern, Kunden, Lieferanten, Aktionären und sonstigen Geschäfts- und Vertragspartnern. Hierunter fallen – je nach Verwendungszweck - z.B. Namen, Global Identifier, Geburtsdatum, Staatsangehörigkeit, Familienstand, Geschlecht, Kontaktdaten, Adressdaten, Kontodaten, Bankverbindung, Religionszugehörigkeit, Informationen zu Ausbildung, Kenntnissen und Fähigkeiten, Werdegang, Eintrittsdatum, Funktionsstufe etc.

Verarbeitet und übermittelt werden diese Daten im Konzernverbund ausschließlich im Rahmen normaler Geschäftszwecke sowie für Zwecke interner Administration. Die Übermittlung erfolgt somit für Zwecke der Personalgewinnung, Personalverwaltung und Personalentwicklung, für Compliance-Zwecke, zur Abwicklung und Durchführung von Aufträgen und Projekten bei – externen und internen - Kunden, zur Abwicklung von Bestellungen und Beauftragungen bei Lieferanten und Dienstleistern, zur Erfüllung von Berichtspflichten, zur Erfüllung oder zum Einziehen von Verbindlichkeiten, zur Abrechnung, zum Zwecke der internen Kommunikation, zum Zwecke der kostensenkenden Konsolidierung und Bündelung von IT-Prozessen in bestimmten Regionen, sowie im Zusammenhang mit der Kooperation und Koordination von Konzerngesellschaften auf regionaler oder auf globaler Ebene im Zuge globaler Geschäftsvorgänge und Projekte.

1.2.13 Verfahrensfragen

1.2.13.1 Verbindlichkeit der BCR

Die BCR haben einen umfassend verbindlichen Charakter.

1.2.13.1.1 Verbindlichkeit für Konzerngesellschaften und teilnehmende Gesellschaften

Die BCR sind durch die zuständigen Governance Owner des OSRAM Konzerns verabschiedet und durch die Veröffentlichung als Richtlinie IM4000 (BCR zum Schutz personenbezogener Daten) in Kraft gesetzt worden.

Die Verantwortung für die Umsetzung der BCR in der teilnehmenden Gesellschaft liegt bei der Leitung der teilnehmenden Gesellschaft, die Ausführung im Einzelfall liegt jeweils bei der Stelle innerhalb dieser Gesellschaft, die personenbezogene Daten im Rahmen ihrer Fachaufgabe verarbeitet. Bei OSRAM-Konzerngesellschaften liegt die Verantwortung beim CEO der OSRAM-Konzerngesellschaft in seiner Eigenschaft als Data Protection Executive („DPE“).

Die BCR sind von allen OSRAM Konzerngesellschaften sowie von den beitretenden Gesellschaften verbindlich zu beachten und einzuhalten. Zur Dokumentation der Anerkennung und Umsetzung der BCR ist im Falle von Konzerngesellschaften von der Leitung der jeweiligen Konzerngesellschaft eine ausdrückliche schriftliche Verpflichtungserklärung auf die Regelungen der BCR abzugeben. Mit Abgabe dieser schriftlichen Verpflichtungserklärung sind die BCR-Regelungen für die Konzerngesellschaft individuell verbindlich. Die Verpflichtungserklärung ist durch die Leitung der Konzerngesellschaft zu unterzeichnen und an die DS Abteilung der OSRAM Konzernobergesellschaft zurückzureichen. Die Verpflichtungserklärung ist den BCR als Anlage beigefügt.

Im Grundsatz sind alle OSRAM-Konzerngesellschaften zu einer Unterzeichnung und Umsetzung der BCR verpflichtet, es sei denn, einer OSRAM-Konzerngesellschaft ist wegen des Vorliegens eines triftigen Grundes (z.B. keine Geschäftstätigkeit, keine Mitarbeiter, keine Verarbeitung personenbezogener Daten, anstehende Liquidation oder Veräußerung) ein Dispens von der Umsetzung der BCR erteilt worden. Ein Dispens muss unter Angabe des Grundes hierfür von der OSRAM-Konzerngesellschaft schriftlich oder per email bei der DS Abteilung beantragt werden. Diese entscheidet über die Begründetheit des Antrags und teilt der Konzerngesellschaft die Entscheidung mit.

Beitretende Gesellschaften, d.h. andere Unternehmen als OSRAM-Konzerngesellschaften, an denen die OSRAM Konzernobergesellschaft direkt oder indirekt beteiligt, können sich auf freiwilliger Basis rechtsverbindlich zur Einhaltung der BCR-Regelungen verpflichten, sofern die Gesellschaft dies wünscht und sofern die DS Abteilung einer solchen Teilnahme zustimmt. Ob anderen Unternehmen als OSRAM-Konzerngesellschaften die Möglichkeit zur freiwilligen Teilnahme am BCR-Verfahren zugebilligt wird, liegt dabei im freien Ermessen der DS Abteilung.

Zur Dokumentation der Anerkennung und Umsetzung der BCR durch eine beitretende Gesellschaft wird zwischen der OSRAM Konzernobergesellschaft und der beitretenden Gesellschaft ein Beitrittsvertrag abgeschlossen, dem die BCR als Anlage beigefügt werden. Mit Abschluss des Beitrittsvertrages sind die BCR-Regelungen für die beitretende Gesellschaft individuell verbindlich. Der Text des Beitrittsvertrags ist diesen BCR als Anlage beigefügt.

Die DS Abteilung führt im OSRAM-Intranet ein elektronisches Verzeichnis der teilnehmenden Gesellschaften, die sich durch Verpflichtungserklärung oder Beitrittsvertrag zur Einhaltung der Regelungen der BCR verpflichtet haben. Dieses elektronische Verzeichnis (**„Statusübersicht**“) ist auf den Intranetseiten jederzeit aktuell abrufbar. In der Statusübersicht werden auch diejenigen Konzerngesellschaften geführt und entsprechend kenntlich gemacht, die aufgrund des Vorliegens eines triftigen Grundes von der Unterzeichnung und Umsetzung der BCR ausnahmsweise durch Dispens befreit wurden. Ferner sind die Konzerngesellschaften in der Statusübersicht erfasst und gekennzeichnet, die ihrer Verpflichtung zur Anerkennung und Umsetzung der BCR (noch) nicht nachgekommen sind.

Hat eine Konzerngesellschaft (noch) keine Verpflichtungserklärung auf die BCR abgegeben, so ist in jedem Einzelfall die Zulässigkeit der Datenübermittlung an diese Konzerngesellschaft zu prüfen und durch geeignete Sondermaßnahmen sicherzustellen, wie beispielsweise durch die Unterzeichnung der EU Standardvertragsklauseln.

Die Verpflichtung zur Einhaltung der BCR kann durch Rücknahme, Widerruf oder Kündigung seitens der OSRAM Konzernobergesellschaft oder seitens der teilnehmenden Gesellschaft beendet werden. Der Verlust des Status einer Konzerngesellschaft führt nicht automatisch zu einer Beendigung der sich aufgrund der BCR ergebenden Verpflichtungen. In diesem Fall ist eine Kündigung der BCR durch die OSRAM Konzernobergesellschaft oder die (ehemalige) Konzerngesellschaft erforderlich. Auch im Falle der Rücknahme bzw. des Widerrufs der Verpflich-

tungserklärung bzw. der Erklärung zum Abschluss des Beitrittsvertrags oder der Kündigung der BCR bleiben die Verpflichtungen aus den BCR im Hinblick auf die bis zu Rücknahme, Widerruf oder Kündigung verarbeiteten personenbezogenen Daten bestehen, bis diese Daten – im Einklang mit den geltenden gesetzlichen Bestimmungen – durch die betroffene Gesellschaft gelöscht wurden.

1.2.13.1.2 Verbindlichkeit gegenüber Mitarbeitern von teilnehmenden Gesellschaften

Auch die Mitarbeiter der teilnehmenden Gesellschaften sind an die Regelungen der BCR gebunden. Der CEO der jeweiligen teilnehmenden Gesellschaft hat die Verpflichtung, die rechtliche Bindungswirkung der BCR für die Mitarbeiter in geeigneter Weise sicherzustellen.

Die BCR-Regelungen sowie alle sonstigen den Datenschutz betreffenden Regelungen stehen den Mitarbeitern der teilnehmenden Unternehmen jederzeit zur Verfügung.

Die teilnehmenden Unternehmen unterrichten ihre Mitarbeiter darüber, dass die Nichteinhaltung der BCR-Regelungen zu disziplinarischen oder arbeitsrechtlichen Maßnahmen (z.B. Abmahnung, Kündigung) gegen die Mitarbeiter führen kann.

1.2.13.1.3 Verbindlichkeit gegenüber Betroffenen

Bestimmte Regelungen der BCR sind – im Wege der Drittbegünstigung - auch gegenüber Betroffenen verbindlich. Drittbegünstigenden Charakter haben die Regelungen in den Ziffern 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 und 1.2.14.

Die Betroffenen sind berechtigt, die Einhaltung eines der vorgenannten drittbegünstigenden Rechte durch eine teilnehmende Gesellschaft durch eine Beschwerde bei der zuständigen Datenschutzaufsicht oder durch die Geltendmachung eines sonstigen Rechtsmittels bei den zuständigen Gerichten durchzusetzen. Die Betroffenen können dabei Schadensersatz geltend machen.

Die Betroffenen können ihre Ansprüche nach ihrer Wahl geltend machen

- am Gerichtsstand der in einem EWR-Land belegenen teilnehmenden Gesellschaft, die die Daten übermittelt hat; oder
- am Gerichtsstand am Hauptsitz der OSRAM Konzernobergesellschaft; oder
- bei der zuständigen Datenschutzaufsichtsbehörde.

Im Falle eines Verstoßes gegen die Regelungen der BCR durch eine teilnehmende Gesellschaft mit Sitz außerhalb des EWR sind somit auch Gerichte und Behörden im EWR zuständig. Dem Betroffenen stehen in diesen Fällen gegenüber der OSRAM Konzernobergesellschaft dieselben Rechte zu, als wenn der Verstoß von der OSRAM Konzernobergesellschaft begangen worden wäre und nicht von einer teilnehmenden Gesellschaft mit Sitz außerhalb des EWR.

Die vorgenannte Zuständigkeit von Gerichten und Behörden im EWR besteht nicht, wenn der Datenempfänger seinen Sitz zwar in einem Land außerhalb des EWR hat, dieses Land jedoch gemäß Entscheidung der EU Kommission über ein angemessenes Datenschutzniveau verfügt.

Um die Drittbegünstigung der Betroffenen auch in den Ländern sicherzustellen, in denen eine Einräumung der Drittbegünstigung im BCR-Dokument womöglich nicht ausreicht, wird OSRAM – soweit erforderlich – entsprechende zusätzliche vertragliche Vereinbarungen mit den betroffenen teilnehmenden Gesellschaften aufsetzen. Eine Drittbegünstigungsklausel, die den Betroffenen die erforderlichen Rechte einräumt, ist in der Verpflichtungserklärung enthalten, die die Konzerngesellschaften als Zeichen ihrer Akzeptanz und Umsetzung der BCR unterschreiben. Gleiches gilt für den Beitrittsvertrag, den die beitretenden Gesellschaften mit der OSRAM Konzernobergesellschaft abschließen.

1.2.13.2 Publizität der BCR

Die BCR und die Drittbegünstigungsklausel sind für die Betroffenen einfach zugänglich. Der Betroffene kann sich entweder an den zuständigen DPC der teilnehmenden Gesellschaft oder aber direkt an die OSRAM Konzernobergesellschaft wenden. OSRAM wird den Betroffenen die BCR in geeigneter Weise zugänglich machen, insbesondere durch die Veröffentlichung der jeweils aktuellen Version der BCR auf den OSRAM Internetseiten. Weitere ein-

schlägige BCR Dokumente – namentlich die Anlagen zu den BCR – werden dem Betroffenen auf Anfrage von der DS Abteilung zur Verfügung gestellt.

1.2.13.3 Umsetzung der BCR in den teilnehmenden Gesellschaften

Die Leitung einer teilnehmenden Gesellschaft - bzw. der CEO einer teilnehmenden Konzerngesellschaft in seiner Eigenschaft als DPE - ist verantwortlich für eine ordnungsgemäße Umsetzung und Befolgung der BCR. Die Leitung der teilnehmenden Gesellschaft kann diese Aufgabe – nicht aber die Verantwortung - auf den DPC delegieren.

OSRAM hat ein weltweites Netzwerk von DPC eingerichtet. Jede teilnehmende Gesellschaft benennt mit Abgabe der Verpflichtungserklärung auf die BCR bzw. mit Abschluss des Beitrittsvertrages zu den BCR einen DPC und übermittelt dessen Kontaktdaten an die DS Abteilung. Änderungen in der Person des DPC sind der DS Abteilung durch die teilnehmende Gesellschaft unverzüglich anzuzeigen.

Der DPC berichtet einmal jährlich an die Leitung der betreffenden teilnehmenden Gesellschaft und - mindestens jährlich - an den CDPO. Dabei berichtet der DPC insbesondere auch jeweils über den Umsetzungsstand der BCR bei der teilnehmenden Gesellschaft.

Der CDPO steht der DS Abteilung vor und koordiniert und führt alle DPC der teilnehmenden Gesellschaften. Der CDPO untersteht dem CIO der OSRAM Konzernobergesellschaft, der wiederum dem CFO der OSRAM Konzernobergesellschaft unterstellt ist. Der CDPO koordiniert und treibt die konzernweite Umsetzung der BCR bei den teilnehmenden Gesellschaften, insbesondere durch Einholung der Verpflichtungserklärungen und Beitrittsverträge, Beratung und Anleitung der DPC bei der Umsetzung der BCR sowie durch Einholung und Auswertung regelmäßiger Berichte der DPC zum Datenschutz sowie zur BCR-Implementierung. Auch ist er für die Erstellung geeigneter BCR Trainings sowie für die Verfügbarmachung solcher BCR Trainings an die teilnehmenden Gesellschaften verantwortlich. Der CDPO ist ferner für die Aktualisierung der BCR sowie für die Kommunikation solcher Änderungen an die zuständigen Datenschutzaufsichtsbehörden zuständig. Der CDPO wird durch die DS Abteilung bei der Wahrnehmung seiner Aufgaben unterstützt.

Der CDPO berichtet einmal jährlich an die Geschäftsleitung der OSRAM Konzernobergesellschaft. Gegenstand dieses Berichts ist insbesondere auch der Umsetzungsstand der BCR bei allen teilnehmenden Gesellschaften.

1.2.13.4 Überwachung der Einhaltung der BCR

Die Einhaltung der BCR durch die teilnehmenden Gesellschaften wird primär regelmäßig durch den von der Leitung der teilnehmenden Gesellschaft benannten DPC überprüft. Die Leitung der teilnehmenden Gesellschaft unterstützt den DPC bei der Wahrnehmung seiner Aufgaben und bindet ihn im Falle von Beschwerden von Betroffenen wegen Nichteinhaltung der BCR ein.

Im Falle schwerwiegender Datenschutzverstöße sowie bei Problemen von grundlegender Bedeutung konsultiert der jeweilige DPC den CDPO und berücksichtigt dessen Hinweise und Entscheidungen bei der Beseitigung solcher Datenschutzverstöße und Probleme.

Die OSRAM Konzernobergesellschaft ist berechtigt, die Tätigkeit der DPC im Zusammenhang mit der Implementierung und Einhaltung der BCR in der teilnehmenden Gesellschaft stichprobenartig zu prüfen, entweder durch Anfordern eines schriftlichen Self Assessments des DPC oder im Rahmen von Kontrollinterviews. Der Inhalt solcher Kontrollgespräche ist vom Auditor zu dokumentieren.

Jede datenübermittelnde teilnehmende Gesellschaft hat das Recht, die Datenverarbeitung bei der empfangenden teilnehmenden Gesellschaft im Einzelfall zu überprüfen. Die übermittelnde Gesellschaft wird dabei die festgestellten Rechte der Betroffenen wahrnehmen und Betroffene, die durch die Verletzung der sich aus diesen BCR ergebenden Verpflichtungen einen Schaden erlitten haben, bei der Durchsetzung ihrer Rechte gegen die verantwortliche Gesellschaft unterstützen.

1.2.13.5 Schulung

Ein zentraler Aspekt der ordnungsgemäßen Umsetzung der BCR ist die entsprechende Unterrichtung und Instruktion der Mitarbeiter. Hierzu zählt auch der Hinweis, dass Verstöße gegen die BCR strafrechtliche, haftungsrechtliche oder arbeitsrechtliche Konsequenzen für den Mitarbeiter nach sich ziehen können.

OSRAM bietet individuelle Informationen sowie spezielle Schulungsmaßnahmen zu den BCR an, die auf eine angemessene Information und Schulung der Mitarbeiter einer teilnehmenden Gesellschaft zum korrekten Umgang mit sowie zum Schutz personenbezogener Daten im Rahmen der Umsetzung der BCR abzielen. Adressat der Schulungsmaßnahmen sind insbesondere die Mitarbeiter, die ständigen oder regelmäßigen Umgang mit personenbezogenen Daten haben. Für diese Mitarbeiter ist die Teilnahme an den Schulungen verpflichtend. Die Schulungen zu den BCR sind in regelmäßigen, angemessenen Abständen zu wiederholen.

Informations- und Schulungsmaßnahmen können – unter anderem – die Durchführung von Web Based Trainings („WBT"), das Angebot geeigneter Präsentationen und Schulungsmaterialien zum Selbststudium, Präsenzschulungen sowie die Organisation von speziell auf Mitarbeiter zugeschnittenen Workshops umfassen.

Die erfolgreiche Teilnahme der Mitarbeiter an der Schulung ist zu dokumentieren.

Weitere Einzelheiten sind in einem detaillierten Schulungskonzept geregelt.

1.2.13.6 Internes Beschwerdeverfahren

Jeder Betroffene kann sich jederzeit mit Beschwerden wegen Verstoßes gegen die BCR durch eine teilnehmende Gesellschaft sowie mit Fragen an die zuständige interne Beschwerdestelle (DS Abteilung; Kontaktdaten vgl. Nummer 0) oder den lokal zuständigen Datenschutzansprechpartner der teilnehmenden Gesellschaft (i.d.R. der DPC) wenden. Der Eingang der Beschwerde bei der kontaktierten Stelle ist dem Betroffenen zeitnah zu bestätigen und die Beschwerde innerhalb angemessener Frist – spätestens innerhalb von drei (3) Monaten ab Eingang der Beschwerde - zu beantworten. Mit der Eingangsbestätigung wird der Betroffene zugleich darüber informiert, welche konkrete Stelle – d.h. die zentrale DS Abteilung oder der lokale DPC – die Beschwerde bearbeiten wird.

Die bei der zuständigen Beschwerdestelle mit der Beschwerdebearbeitung befassten Mitarbeiter verfügen über ein hinreichendes Maß an Unabhängigkeit bei der Wahrnehmung dieser Aufgabe.

Die teilnehmende Gesellschaft und der CDPO sind bei Anfragen verpflichtet, mit der Datenschutzaufsicht im jeweiligen Land zu kooperieren und deren Entscheidung zu respektieren.

Weitere Einzelheiten – Form der Beschwerde, Bearbeitungsfristen, weiteres Vorgehen bei Anerkennung und/oder Ablehnung der Beschwerde, weiterführende Rechtsbehelfe - sind in einem separaten Beschwerdekonzept geregelt.

1.2.13.7 BCR Audit

OSRAM hat das im Konzern bereits existierende interne Audit- und Kontrollsystem um ein BCR Audit Programm ergänzt, um sicherzustellen, dass die Einhaltung eines angemessenen Datenschutzniveaus nach Maßgabe der BCR-Regelungen in den teilnehmenden Gesellschaften regelmäßig kontrolliert wird.

Die primäre Zuständigkeit für die Durchführung von turnusmäßigen papierbasierten BCR Audits, turnusmäßigen Vor-Ort BCR Audits sowie von anlassbezogenen ad-hoc BCR Audits liegt bei der OSRAM Auditabteilung. Alternativ kann ein BCR Audit im Bedarfsfall auch von einem akkreditierten externen Auditor vorgenommen werden.

Den Zeitplan für die turnusmäßigen BCR Audits legt die OSRAM Auditabteilung im Einklang mit ihrer allgemeinen Audit Zeitplanung fest.

Einmal jährlich findet ein papierbasiertes BCR Audit in Gestalt eines Self Assessments (Ausfüllen eines Fragebogens) durch die teilnehmende Gesellschaft statt. Der CDPO und die OSRAM Auditabteilung erhalten die Ergebnisse dieses turnusmäßigen Self Assessments.

Im Falle besonderer Umstände (z.B. Datenschutzvorfälle, Beschwerden Betroffener, bei Self Assessments festgestellte Defizite) können der CDPO oder die Abteilung für Informationssicherheit (IT DIS) neben den vorgenannten geplanten, turnusmäßigen BCR Audits auch noch weitere ad-hoc BCR Audits beauftragen.

Das BCR Audit bezieht sich auf alle Aspekte der BCR. Soweit ein BCR Audit zu dem Ergebnis kommt, dass Abhilfemaßnahmen wegen eines BCR-Verstoßes zu treffen sind, hat das BCR Audit auch für eine Umsetzung der erforderlichen Abhilfemaßnahmen Sorge zu tragen.

Der CDPO, die Geschäftsleitung des OSRAM Konzerns und die Leitung der geprüften teilnehmenden Gesellschaft erhalten den vollständigen BCR Auditbericht. Die Ergebnisse des BCR Audits werden der zuständigen Daten-

schutzaufsichtsbehörde auf Anfrage zur Verfügung gestellt. Soweit erforderlich, kann OSRAM hierbei Teile der Prüfungsdaten unkenntlich machen, um den Schutz vertraulicher Unternehmensinformationen sicherzustellen.

Die zuständige Datenschutzaufsichtsbehörde hat das Recht, ein eigenes BCR Audit bei einer teilnehmenden Gesellschaft durchzuführen. Die Behörde kann das BCR Audit entweder selber oder mittels eines akkreditierten unabhängigen Auditors durchführen. Ein behördliches BCR Audit beschränkt sich ausschließlich auf die Einhaltung der BCR durch die teilnehmende Gesellschaft. Beschränkungen aus Vertraulichkeitsvereinbarungen oder aus Geschäfts- und Betriebsgeheimnissen sind zu beachten.

Einzelheiten des BCR Audits sind in einem separaten BCR-Audit-Konzept geregelt.

1.2.13.8 BCR Aktualisierung & Change Management

OSRAM behält sich das Recht zu einer jederzeitigen Änderung und/oder Aktualisierung dieser BCR vor. Eine solche Aktualisierung der BCR kann insbesondere durch geänderte rechtliche Anforderungen, durch maßgebliche Änderungen in der Konzernstruktur oder durch Auflagen der zuständigen Datenschutzaufsichtsbehörden geboten sein.

Gravierende Änderungen der BCR bedürfen unter Umständen einer erneuten Genehmigungserteilung durch die zuständigen Datenschutzaufsichtsbehörden. Alle übrigen Änderungen der BCR sind auch ohne solche erneute Genehmigung möglich.

Die DS Abteilung führt eine Übersicht über alle seit Inkrafttreten der BCR vorgenommenen Änderungen / Aktualisierungen der BCR. Sie führt ferner eine regelmäßig aktualisierte Liste aller teilnehmenden Gesellschaften, die wirksam an die BCR gebunden sind („Statusübersicht“, vgl. Abschnitt 1.2.13.1.1).

Änderungen der BCR sowie Änderungen der Statusübersicht teilt der CDPO denjenigen Datenschutzaufsichtsbehörden, die die BCR genehmigt haben auf Anfrage, und nach offizieller Genehmigung der BCR mindestens einmal jährlich mit. Solche Mitteilungen enthalten eine summarische Begründung für die vorgenommenen Änderungen.

1.2.13.9 Kooperation untereinander und mit den Datenschutzaufsichtsbehörden

Alle teilnehmenden Gesellschaften werden bei Anfragen und Beschwerden Betroffener im Hinblick auf die Nichteinhaltung der BCR vertrauensvoll zusammenarbeiten und einander unterstützen.

Die teilnehmenden Gesellschaften verpflichten sich ferner, im Zusammenhang mit der Implementierung der BCR vertrauensvoll mit den zuständigen Datenschutzaufsichtsbehörden zusammenzuarbeiten. Sie werden auf BCR-bezogene Anfragen der Datenschutzaufsichtsbehörde innerhalb angemessener Frist und auf angemessene Weise antworten und die Ratschläge und Entscheidungen der zuständigen Datenschutzaufsichtsbehörde im Hinblick auf die Umsetzung der BCR befolgen.

1.2.13.10 Verhältnis der BCR zu lokalen gesetzlichen Regelungen

Die Zulässigkeit der Verarbeitung personenbezogener Daten beurteilt sich anhand des für die übermittelnde teilnehmende Gesellschaft jeweils anwendbaren lokalen Rechts. Soweit das anwendbare lokale Recht einen stärkeren Schutz personenbezogener Daten vorschreibt als diese BCR, richtet sich die Datenverarbeitung nach dem anwendbaren Recht. Jede teilnehmende Gesellschaft muss selbst prüfen (z. B. durch ihren Datenschutzbeauftragten, DPC oder durch die Rechtsabteilung), ob es solche lokalen gesetzlichen Regelungen (z. B. Datenschutzgesetze) gibt und deren Einhaltung sicherstellen. Sofern das anwendbare lokale Recht ein niedrigeres Schutzniveau für personenbezogene Daten vorsieht als diese BCR, finden die vorliegenden BCR Anwendung.

Falls sich aus dem anwendbaren lokalen Recht ergebende Verpflichtungen im Widerspruch zu den BCR stehen, hat die teilnehmende Gesellschaft unverzüglich den CDPO zu informieren. Er wird den gemeldeten Konflikt in die Statusübersicht (vgl. Abschnitt 1.2.13.1.1) eintragen.

Die DS Abteilung wird alle teilnehmenden Gesellschaften, die zuvor Daten an die betreffende teilnehmende Gesellschaft übermittelt haben, über den gemeldeten Widerspruch der BCR mit dem lokalen Recht informieren. Sie wird ferner die zuständige Datenschutzaufsicht über den Regelkonflikt informieren und gemeinsam mit der Datenschutzaufsicht und der teilnehmenden Gesellschaft nach einer praktikablen Lösung suchen, die den Grundsätzen der EU-Datenschutzrichtlinie möglichst nahekommt.

1.2.14 Haftung

Jede teilnehmende Gesellschaft haftet für die von ihr begangenen Verstöße gegen die BCR.

Die OSRAM Konzernobergesellschaft übernimmt die Haftung für die Nichteinhaltung der BCR durch teilnehmende Gesellschaften mit Sitz außerhalb des EWR, einschließlich der Verpflichtung zur Zahlung von Schadensersatz im Falle eines nachgewiesenen Verstoßes gegen die BCR sowie einer daraus resultierenden Rechtsverletzung des Betroffenen. Sie wird ferner die erforderlichen Abhilfemaßnahmen ergreifen, um Verstöße gegen die BCR durch eine teilnehmende Gesellschaft mit Sitz außerhalb des EWR zu beseitigen.

Die Beweislast trägt die OSRAM Konzernobergesellschaft. Sie muss nachweisen, dass kein Verstoß gegen die BCR vorliegt oder dass der Verstoß gegen die BCR, mit dem der Betroffene seine Schadensersatzforderung begründet, der teilnehmenden Gesellschaft mit Sitz außerhalb des EWR nicht zuzurechnen ist.

Wenn die OSRAM Konzernobergesellschaft nachweisen kann, dass die teilnehmende Gesellschaft mit Sitz außerhalb des EWR nicht für einen BCR-Verstoß haftbar ist, kann sie auch sich selbst von einer diesbezüglichen Verantwortung freizeichnen.

1.2.15 Kontakt

Betroffene können sich mit ihren Anliegen an den DPC der betreffenden teilnehmenden Gesellschaft oder an den OSRAM CDPO (Konzerndatenschutzbeauftragter) wenden:

OSRAM GmbH
Abteilung Datenschutz
Marcel-Breuer-Str. 6
D- 80807 München
Tel.:+49 (0) 89 6213-4978
Fax:+49 (0) 89 6213-2036
Email: datenschutz@osram.com
Internet: http://www.osram.com