For internal use only

Anhang zur Unternehmensrichtlinie CO3000

Verbindliche Interne Daten-schutzvorschriften

Verbindliche Interne Datenschutzvorschriften (“BCR”) für ams OSRAM Konzerngesellschaften und Beitretende Unternehmen zum Schutz Perso-nenbezogener Daten

Kontakte und Gültigkeit
Herausgeber:
Compliance (CO)
Governance Owner:
Dietmar Prechtel (CO)
Experte (Autor):
Stefan Gassner (CO)
Geografischer Geltungsbereich:
Weltweit
Organisatorischer Geltungsbereich:
Alle
Version: **1.4**
Gültig ab:
2025-12-09

Inhaltsverzeichnis

1. Begriffe 3
2. Zusammenfassung der Verbindlichen Internen Datenschutzvorschriften von ams OSRAM 5
3. Inhalt der Richtlinie 5
3.1 Anwendungsbereich der Verbindlichen Internen Datenschutzvorschriften 5
3.2 Grundsätze der Verarbeitung Personenbezogener Daten und Elemente des Datenschutzrahmens 6
3.2.1 Verarbeitung der Daten auf rechtmäßige Weise und nach Treu und Glauben 6
3.2.2 Zweckbindung 6
3.2.3 Transparenz 7
3.2.4 Datenqualität, Datenminimierung und Speicherbegrenzung 8
3.2.5 Weiterübermittlung von Daten 8
3.2.6 Datensicherheit 9
3.2.7 Vertraulichkeit der Datenverarbeitung 9
3.3 Besondere Kategorien Personenbezogener Daten und Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten 10
3.4 Automatisierte Entscheidungsfindung 10
3.5 Verzeichnis von Verarbeitungstätigkeiten 11
3.6 Datenschutz-Folgenabschätzung 11
3.7 Meldung und Dokumentation einer Datenschutzverletzung 11
3.8 Privacy by Design und Privacy by Default 12
3.9 Auftragsverarbeitung 12
3.10 Rechte der Betroffenen Personen 13
3.11 Rechenschaftspflicht 16
3.12 Beschreibung der Datenübermittlung 16
3.13 Verfahrensfragen 17
3.13.1 Verbindlichkeit der Verbindlichen Internen Datenschutzvorschriften 17
3.13.1.1 Verbindlichkeit für Konzerngesellschaften und Teilnehmende Unternehmen 17
3.13.2 Veröffentlichung der verbindlichen internen Datenschutzvorschriften 20
3.13.3 Umsetzung der Verbindlichen Internen Datenschutzvorschriften in den Teilnehmenden Unternehmen 20
3.13.4 Überwachung der Einhaltung der Verbindlichen Internen Datenschutzvorschriften 21
3.13.5 Schulung 21
3.13.6 Internes Beschwerdeverfahren 22
3.13.7 Überprüfung der Verbindlichen Internen Datenschutzvorschriften 23
3.13.8 Aktualisierung der Verbindlichen Internen Datenschutzvorschriften und Change-Management 24
3.13.9 Gegenseitige Unterstützung und Zusammenarbeit mit Aufsichtsbehörden 24
3.13.10 Zusammenhänge zwischen den Verbindlichen Internen Datenschutzvorschriften und lokalen gesetzlichen Vorschriften 25
3.13.11 Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Verbindlichen Internen Datenschutzvorschriften auswirken 25
3.13.12 Pflichten des Datenimporteurs bei Auskunftsersuchen staatlicher Stellen 27
3.14 Nichteinhaltung der Verbindlichen Internen Datenschutzvorschriften 29
3.15 Haftung 29
3.16 Kontakt 30
Versionsverlauf 31
Anhang I zu den Verbindlichen Internen Datenschutzvorschriften 32

1. Begriffe

- **ams OSRAM oder ams OSRAM Konzern** steht für alle ams OSRAM Konzerngesellschaften;
- **ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung:** OSRAM GmbH;
- **ams OSRAM Muttergesellschaft:** ams-OSRAM AG;
- **Auftragsverarbeiter** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die Personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
- **Beitretendes Unternehmen** ist ein mit ams OSRAM verbundenes Unternehmen in Deutschland oder im Ausland, an der die ams OSRAM Muttergesellschaft oder ein mit der ams OSRAM Muttergesellschaft verbundenes Unternehmen eine Minderheitsbeteiligung hält und das sich mit Zustimmung des ams OSRAM Co-Hauptsitzes mit Datenschutzverantwortung freiwillig verpflichtet hat, durch Abschluss eines Intercompany Agreements die Vorschriften der Verbindlichen Internen Datenschutzvorschriften einzuhalten;
- **Betroffene Person** ist jede identifizierte oder identifizierbare natürliche Person, deren Daten verarbeitet werden. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann; juristische Personen können durch eine entsprechende Vereinbarung zwischen dem datenübermittelnden Unternehmen und dem Datenempfänger in den Anwendungsbereich der Verbindlichen Internen Datenschutzvorschriften einbezogen werden (insofern gelten auch sie als betroffene Personen);
- **Besondere Kategorien Personenbezogener Daten** umfassen Informationen, die die ethnische Herkunft, Rasse, politische Ansichten, religiöse oder weltanschauliche Überzeugungen oder die Mitgliedschaft in einer Gewerkschaft offenbaren. Dazu gehören auch genetische und biometrische Daten zur eindeutigen Identifizierung einer Person, Gesundheitsdaten sowie Informationen über das Sexualleben oder die sexuelle Orientierung.
- **Data Protection Executive (DPE)** einer ams OSRAM Konzerngesellschaft: Diese Funktion wird von einem gesetzlichen Vertreter der entsprechenden ams OSRAM Konzerngesellschaft ausgeführt;
- **Datenschutzbeauftragter (DSB):** Die von einem Teilnehmenden Unternehmen ernannte Person, die die Geschäftsführung bei Fragen zur lokalen Umsetzung und Einhaltung der Datenschutz-Grundverordnung und anderer geltender Datenschutzbestimmungen überwacht und berät und deren Ernennung unter bestimmten, in der Verordnung festgelegten Bedingungen zwingend vorgesehen ist;
- **Datenschutz-Grundverordnung (DSGVO)** ist die Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung Personenbezogener Daten und zum freien Datenverkehr;
- **Datenschutzkoordinator (DSK)** ist die Person, die von einem Teilnehmenden Unternehmen als verantwortlich für die lokale Umsetzung und Einhaltung der Verbindlichen Internen Datenschutzvorschriften sowie für die Unterstützung der Konzern-Datenschutzabteilung ernannt wurde;
- **Dritter** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der Betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Personenbezogenen Daten zu verarbeiten;

- **Drittland** ist ein Land außerhalb der der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (EWR);
- **Einwilligung** ist eine freiwillige, für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die Betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden Personenbezogenen Daten einverstanden ist[1];
- **Inter-Company Agreement (ICA):** Vertrag, durch dessen Abschluss sich die ams OSRAM Konzerngesellschaft oder ein Beitretendes Unternehmen verpflichtet, die Bestimmungen der Verbindlichen Internen Datenschutzvorschriften einzuhalten;
- Die **Konzern-Datenschutzabteilung (CDPD)** ist die zentrale Abteilung von ams OSRAM, die nach dem aktuellen Organigramm für den konzernweiten Datenschutz verantwortlich ist;
- **Konzerngesellschaft oder ams OSRAM Konzerngesellschaft** sind Gesellschaften, an denen die ams OSRAM Muttergesellschaft direkt oder indirekt eine Mehrheitsbeteiligung hält oder die Mehrheit der Stimmrechte kontrolliert;
- **Kunden und Lieferanten** sind natürliche und juristische Personen, mit denen eine Geschäftsbeziehung besteht oder geplant ist;
- **Land/Länder des EWR** sind die Mitgliedsstaaten der Europäischen Union (EU) und die anderen Unterzeichner des Abkommens über den Europäischen Wirtschaftsraum (EWR);
- **Personenbezogene Daten** sind alle Informationen, die sich auf eine Betroffene Person beziehen;
- **Teilnehmendes Unternehmen** ist eine ams OSRAM Konzerngesellschaft oder ein Beitretendes Unternehmen, das dem Inter-Company Agreement beitritt und sich damit verpflichtet, die Bestimmungen dieser Verbindlichen Internen Datenschutzvorschriften einzuhalten;
- **Standardvertragsklauseln** sind EU-Standardvertragsklauseln für die Übermittlung Personenbezogener Daten an Drittländer, die am 4. Juni 2021 durch Beschluss 2021/914 der Europäischen Kommission verabschiedet wurden oder andere vertragliche Vorkehrungen, die von der Europäischen Kommission gemäß Artikel 46 Absatz 2 (c) der Datenschutz-Grundverordnung erlassen werden;
- **Verantwortlicher** ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Datenverarbeitung entscheidet;
- **Verarbeitung Personenbezogener Daten** oder **Datenverarbeitung** ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
- **Verbindliche Interne Datenschutzvorschriften („BCR“)** sind diese Verbindlichen Internen Datenschutzvorschriften und die darin enthaltenen Bestimmungen;

Verletzung des Schutzes Personenbezogener Daten oder **Datenschutzverletzung** ist eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu Personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

[1] Bestimmte nationale Gesetze können besondere Anforderungen für die Einwilligung festlegen, die sich auf die Wirksamkeit der Einwilligung auswirken.

2. Zusammenfassung der Verbindlichen Internen Datenschutzvorschriften von ams OSRAM

Der primäre Zweck dieser Verbindlichen Internen Datenschutzvorschriften ist es, sicherzustellen, dass in allen ams OSRAM Konzerngesellschaften und den Beitretenden Unternehmen ein angemessener Schutz der Personenbezogenen Daten besteht, die im Geschäftsablauf von einem Teilnehmenden Unternehmen an andere Teilnehmende Unternehmen übermittelt werden.

Die folgenden Personenbezogenen Daten fallen in den Anwendungsbereich dieser Verbindlichen Internen Datenschutzvorschriften:

- Alle Personenbezogenen Daten aus der EU/dem EWR, die der Datenschutz-Grundverordnung unterliegen;
- Personenbezogene Daten ungeachtet ihres Herkunftslandes insoweit, als sie von einem (datenerhebenden) Teilnehmenden Unternehmen an ein (empfangendes) Teilnehmendes Unternehmen übermittelt werden.

Zum oben genannten Zweck ist es wesentlich, harmonisierte Datenschutz- und Datensicherheitsstandards für die Verarbeitung personenbezogener Daten im Sinne der Datenschutz-Grundverordnung zu etablieren. Damit wird sichergestellt, dass – in Bezug auf die personenbezogenen Daten, die in den Geltungsbereich dieser Verbindlichen Internen Datenschutzvorschriften fallen – ein angemessenes Datenschutzniveau und geeignete Garantien im Sinne der Datenschutz-Grundverordnung bezüglich des Schutzes der Privatsphäre und der Ausübung der damit verbundenen Rechte gewährleistet werden.

Diese Verbindlichen Internen Datenschutzvorschriften bilden den generellen und allgemein gültigen regulatorischen Rahmen für die Verarbeitung Personenbezogener Daten von Mitarbeitern, Kunden, Lieferanten, Aktionären, Geschäftspartnern oder zukünftigen Geschäftspartnern und anderen Betroffenen Personen, die in deren Anwendungsbereich fallen, durch ams OSRAM Konzerngesellschaften oder Beitretende Unternehmen. Die vorliegenden Verbindlichen Internen Datenschutzvorschriften geben die Situation zum Zeitpunkt ihrer letzten Überprüfung und die geltenden internationalen Datenschutzanforderungen wieder, insbesondere die Anforderungen der Datenschutz-Grundverordnung, der einschlägigen Richtlinien, der Arbeitspapiere der ehemaligen Artikel-29-Datenschutzgruppe und des Europäischen Datenschutzausschusses.

3. Inhalt der Richtlinie

3.1 Anwendungsbereich der Verbindlichen Internen Datenschutzvorschriften

Alle ams OSRAM Konzerngesellschaften und alle Beitretenden Unternehmen weltweit fallen in den Anwendungsbereich der Verbindlichen Internen Datenschutzvorschriften. Die Verbindlichen Internen Datenschutzvorschriften gelten für die Verarbeitung

- aller Personenbezogenen Daten aus der EU/dem EWR, die der Datenschutz-Grundverordnung unterliegen;
- Personenbezogener Daten ungeachtet ihres Herkunftslandes insoweit, als sie von einem (datenerhebenden) Teilnehmenden Unternehmen an ein (empfangendes) Teilnehmendes Unternehmen übermittelt werden

von Mitarbeitern, Kunden, Lieferanten, Aktionären, Geschäftspartnern oder potenziellen Geschäftspartnern und anderen Betroffenen Personen durch ams OSRAM Konzerngesellschaften oder Beitretende Unternehmen. Es fallen nicht nur Personenbezogene Daten der Teilnehmenden Unternehmen in einem Land des EWR unter diese Verbindlichen Internen Datenschutzvorschriften, sondern ALLE Personenbezogenen Daten, die von einem Teilnehmenden Unternehmen stammen, sobald diese Daten an ein anderes Teilnehmendes Unternehmen übermittelt werden (einschließlich Personenbezogener Daten von Teilnehmenden Unternehmen mit Sitz außerhalb des EWR, wenn diese Daten an ein anderes Teilnehmendes Unternehmen übermittelt werden). Der Anwendungsbereich

der Verbindlichen Internen Datenschutzvorschriftenumfasst die Übermittlung Personenbezogener Daten zwischen Teilnehmenden Unternehmen außerhalb des EWR.

Eine Liste aller Teilnehmenden Unternehmen ist den Verbindlichen Internen Datenschutzvorschriften als Anhang I beigefügt.

3.2 Grundsätze der Verarbeitung Personenbezogener Daten und Elemente des Datenschutzrahmens

Die folgenden Grundsätze und Elemente des Datenschutzrahmens leiten sich insbesondere aus der Datenschutz-Grundverordnung ab und müssen berücksichtigt werden, wenn Personenbezogene Daten durch Teilnehmende Unternehmen im Anwendungsbereich dieser Verbindlichen Internen Datenschutzvorschriften verarbeitet werden:

3.2.1 Verarbeitung der Daten auf rechtmäßige Weise und nach Treu und Glauben

Personenbezogene Daten werden rechtmäßig unter Einhaltung der entsprechenden gesetzlichen Vorschriften und unter Wahrung der in diesen Verbindlichen Internen Datenschutzvorschriften festgelegten Grundsätze verarbeitet.

Die Verarbeitung ist nur dann zulässig, wenn zumindest eine der folgenden Voraussetzungen erfüllt ist:

- die Betroffene Person hat in die Verarbeitung der Personenbezogenen Daten für einen oder mehrere bestimmte Zwecke eingewilligt; oder
- die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die Betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der Betroffenen Person erfolgen; oder
- die Datenverarbeitung ist für die Einhaltung gesetzlicher Verpflichtungen, denen der Verantwortliche unterliegt, notwendig; oder
- die Datenverarbeitung ist zum Schutz lebenswichtiger Interessen der Betroffenen Person oder einer anderen natürlichen Person erforderlich; oder
- die Datenverarbeitung ist für die Erbringung einer Aufgabe im öffentlichen Interesse oder für die Ausübung einer dem Verantwortlichen übertragenen öffentlichen Gewalt erforderlich; oder
- die Datenverarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der Betroffenen Person, die den Schutz Personenbezogener Daten erfordern, überwiegen;
- die Datenverarbeitung ist durch nationales Recht vorgeschrieben oder zulässig, welches für das Teilnehmende Unternehmen gilt, das die Daten ursprünglich übermittelt hat.

Der Verantwortliche muss einfache, schnelle und effiziente Verfahren einrichten, die es der Betroffenen Person ermöglichen, ihre Einwilligung jederzeit zu widerrufen.

Alle Teilnehmenden Unternehmen verarbeiten die Personenbezogenen Daten nach Treu und Glauben. Die Datenverarbeitung hat so zu erfolgen, wie es die Betroffenen Personen vernünftigerweise erwarten können und es dürfen keine ungerechtfertigten nachteiligen Auswirkungen für sie entstehen.

3.2.2 Zweckbindung

Personenbezogene Daten werden ausschließlich für die angegebenen, ausdrücklichen und berechtigten Zwecke verarbeitet. Personenbezogene Daten werden unter keinen Umständen auf eine Weise verarbeitet, die nicht kompatibel mit den berechtigten Zwecken ist, für die diese Daten erhoben wurden. Die Teilnehmenden Unternehmen sind verpflichtet, sich bei der Speicherung und weiteren Verarbeitung oder Verwendung von

Daten, die ihnen von einem anderen Teilnehmenden Unternehmen übermittelt wurden, an den Zweck der Datenübermittlung zu halten; der Zweck der Datenverarbeitung darf nur geändert werden, wenn die Betroffene Person einwilligt oder, soweit es in dem Land zulässig ist, dessen Gesetzen das Teilnehmende, ursprünglich übermittelnde Unternehmen unterliegt.

3.2.3 Transparenz

Alle Teilnehmenden Unternehmen verarbeiten die Personenbezogenen Daten auf transparente Weise. Betroffene Personen, deren Daten von einem Teilnehmenden Unternehmen verarbeitet werden erhalten gemäß Artikeln 13 und 14 der Datenschutz-Grundverordnung von dem Teilnehmenden Unternehmen die folgenden Informationen (gegebenenfalls in Absprache mit dem übermittelnden Unternehmen):

- den Namen und die Kontaktdaten des Verantwortlichen sowie des übermittelnden Unternehmens;
- gegebenenfalls die Kontaktdaten des DSB des betreffenden Teilnehmenden Unternehmens;
- Kategorien der betroffenen Personenbezogenen Daten;
- Empfänger oder Kategorien der Empfänger der Personenbezogenen Daten;
- den Zweck, für den die Personenbezogenen Daten verarbeitet werden, sowie die Rechtsgrundlage für die Verarbeitung;
- gegebenenfalls die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
- gegebenenfalls einen Verweis auf die geeigneten Vorkehrungen, die zum Schutz der an Empfänger in Drittländern oder internationale Organisationen übermittelten Personenbezogenen Daten getroffen wurden sowie die Information, wie eine Kopie der Beschreibung dieser Vorkehrungen zu erhalten bzw. wo sie verfügbar ist;
- die Dauer, für die die Personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Recht, beim Verantwortlichen Zugang zu Personenbezogenen Daten und deren Berichtigung oder Löschung oder die Einschränkung der Verarbeitung in Bezug auf die Betroffene Person zu beantragen oder der Verarbeitung zu widersprechen, sowie das Recht auf Datenübertragbarkeit;
- wenn die Verarbeitung auf einer Einwilligung der Betroffenen Person beruht, das Recht, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- ob die Bereitstellung der Personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die Betroffene Person verpflichtet ist, die Personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte;
- das Bestehen einer automatisierten Entscheidungsfindung – einschließlich Profiling – und, zumindest in diesen Fällen, aussagekräftige Informationen über die zugrundeliegende Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung auf die Betroffene Person;
- die Quelle, aus der die Personenbezogenen Daten stammen, einschließlich öffentlich zugänglicher Quellen (es sei denn, es handelt sich um Personenbezogene Daten, die direkt von der Betroffenen Person erhoben wurden).

Diese Verbindlichen Internen Datenschutzvorschriften werden allen Betroffenen Personen, die die in Unterabschnitt 3.13.1.3 festgelegten Rechte als Drittbegünstigte haben,

zusammen mit den in diesem Unterabschnitt aufgeführten Informationen zur Verfügung gestellt.

Soweit die Personenbezogenen Daten nicht direkt bei der Betroffenen Person erhoben wurden, müssen diese Informationen ausnahmsweise nicht erteilt werden, wenn die Betroffene Person bereits über Informationen verfügt oder wenn dies mit einem unverhältnismäßigen Aufwand verbunden wäre.

3.2.4 Datenqualität, Datenminimierung und Speicherbegrenzung

Personenbezogene Daten müssen sachlich korrekt sein und auf dem neuesten Stand gehalten werden. Es müssen geeignete Maßnahmen ergriffen werden, um falsche oder unvollständige Daten zu berichtigen oder zu löschen.

Die Datenverarbeitung hat dem Grundsatz der Datensparsamkeit zu folgen. Es ist das Ziel, nur erforderliche Personenbezogene Daten zu erheben, zu verarbeiten und zu verwenden, d. h. so wenig Personenbezogene Daten wie möglich. Insbesondere sind die Daten zu anonymisieren, sofern Kosten und Aufwand in einem angemessenen Verhältnis zum gewünschten Zweck stehen. Statistische Auswertungen oder Studien, die auf anonymisierten Daten beruhen, sind datenschutzrechtlich nicht relevant, sofern diese Daten nicht zur Identifizierung der Betroffenen Person verwendet werden können.

Personenbezogene Daten, die nicht länger für die geschäftlichen Zwecke benötigt werden, für die sie ursprünglich erhoben und gespeichert wurden, sind zu löschen. Sollten gesetzliche Aufbewahrungsfristen gelten, wird die Verarbeitung der entsprechenden Daten eingeschränkt.

3.2.5 Weiterübermittlung von Daten

Die Übermittlung Personenbezogener Daten von einem Teilnehmenden an ein nicht Teilnehmendes Unternehmen ist nur unter folgenden Bedingungen zulässig:

- wenn die empfangende Stelle ein Auftragsverarbeiter ist, sind die Bedingungen aus Artikel 28 der Datenschutz-Grundverordnung erfüllt.

- wenn die empfangende Stelle ein Verantwortlicher ist, der gemeinsam mit dem Teilnehmenden Unternehmen über die Zwecke und Mittel der Datenverarbeitung entscheidet, sind die Anforderungen aus Artikel 26 der Datenschutz-Grundverordnung erfüllt.

Weitere Übermittlungen Personenbezogener Daten, die ein Teilnehmendes Unternehmen mit Sitz in einem Nicht-EWR-Land (= Datenimporteur) von einem anderen Teilnehmenden Unternehmen mit Sitz in einem EWR-Land (= Datenexporteur) erhalten hat, an einen externen Verantwortlichen oder Auftragsverarbeiter außerhalb von ams OSRAM mit Sitz in einem Nicht-EWR-Land ohne angemessenes Datenschutzniveau sind nur zulässig, wenn (i) die empfangende Stelle mit einem angemessenen Datenschutzniveau für Personenbezogene Daten im Sinne der Artikel 45-48 der Datenschutz-Grundverordnung ausgestattet ist, z. B. durch den Abschluss von Standardvertragsklauseln oder (ii) Ausnahmeregelungen für bestimmte Situationen gemäß Artikel 49 der Datenschutz-Grundverordnung angewandt werden.

Wenn durch den betreffenden Angemessenheitsbeschluss der Europäischen Kommission kein angemessenes Schutzniveau für die Personenbezogenen Informationen im Empfängerland dieses externen Verantwortlichen oder Auftragsverarbeiters festgestellt wurde, muss der Datenimporteur vor der Übermittlung die Einhaltung zusätzlicher Anforderungen sicherstellen, die im Schrems-II-Urteil des Europäischen Gerichtshofes festgelegt sind (z. B. Durchführung einer Datentransfer-Folgenabschätzung und Festlegung zusätzlicher technischer und organisatorischer Maßnahmen).

3.2.6 Datensicherheit

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ergreifen die Teilnehmenden Unternehmen geeignete technische und organisatorische Maßnahmen, um die erforderliche Datensicherheit zu gewährleisten, damit Personenbezogene Daten vor versehentlicher oder unrechtmäßiger Löschung, unbefugter Verwendung, Veränderung, Verlust, Zerstörung sowie vor unbefugter Weitergabe oder unbefugtem Zugriff geschützt werden. Besondere Kategorien Personenbezogener Daten sind besonders zu schützen.

Die Sicherheitsmaßnahmen gewährleisten ein Sicherheitsniveau, das den Verarbeitungsrisiken und der Art der geschützten Daten entspricht, und sollen sich am Stand der Technik im Bereich Datensicherheit orientieren.

Die bereitzustellenden Sicherheitsmaßnahmen beziehen sich insbesondere auf Computer (Server und Arbeitsplatzrechner), Netzwerke, Kommunikationsverbindungen und Anwendungen. Um ein angemessenes Niveau technischer und organisatorischer Maßnahmen zum Datenschutz zu gewährleisten, hat die Konzernleitung ein Information Security Management System (ISMS) eingeführt (beschrieben in der Unternehmensrichtlinie IT3000), welches für den gesamten ams OSRAM Konzern bindend ist. Die aktuelle Version der Richtlinie sowie die dazugehörigen Dokumente befinden sich im Corporate Prozesshaus unter https://security/rules.

Bestimmte Maßnahmen, die zum angemessenen Schutz Personenbezogener Daten eingesetzt werden, sind u. a. die Pseudonymisierung und Verschlüsselung Personenbezogener Daten, Zugangskontrollen, Systemzugangskontrollen, Datenzugangskontrollen, Übertragungskontrollen, Eingabekontrollen, Transportkontrollen, Speicherkontrollen, Arbeitsplatzkontrollen, Verfügbarkeits- und Wiederherstellungskontrollen sowie Segregationskontrollen zur Gewährleistung

- der fortwährenden Vertraulichkeit, Integrität, Verfügbarkeit und Resilienz von Verarbeitungssystemen und -services;
- der Fähigkeit, bei einem physischen oder technischen Zwischenfall Personenbezogene Daten zügig wieder verfügbar und zugänglich zu machen;
- eines Prozesses für die regelmäßige Prüfung, Einschätzung und Bewertung der Wirksamkeit der technischen und organisatorischen Maßnahmen, welche die Sicherheit der Verarbeitung gewährleisten.

Alle Arbeitsplatzcomputer – einschließlich Mobilgeräte (z. B. Laptops) – sind passwortgeschützt. Das interne ams OSRAM Netz verfügt über ein Firewall-System, um interne Firmeninhalte vor unbefugtem Zugriff von außen zu schützen. Die Übermittlung Personenbezogener Daten innerhalb des firmeneigenen Netzwerks erfolgt grundsätzlich verschlüsselt – soweit die Art und der Verwendungszweck der Personenbezogenen Daten dies erfordern.

3.2.7 Vertraulichkeit der Datenverarbeitung

Nur Personal der Teilnehmenden Unternehmen, das berechtigt ist und eine besondere Einweisung für die Einhaltung der Datenschutzanforderungen erhalten hat, darf Personenbezogene Daten erheben, verarbeiten oder verwenden. Die Zugriffsberechtigung des einzelnen Mitarbeiters wird entsprechend der Art und des Umfangs seines jeweiligen Aufgabenfelds beschränkt. Es ist dem Mitarbeiter untersagt, Personenbezogene Daten für private Zwecke zu nutzen und Personenbezogene Daten zu übermitteln oder auf andere Weise unbefugten Personen zugänglich zu machen. Unbefugte Personen in diesem Zusammenhang umfassen beispielsweise andere Mitarbeiter, soweit sie die Personenbezogenen Daten nicht benötigen, um ihnen zugewiesene Fachaufgaben zu erledigen. Die Verpflichtung zur Verschwiegenheit bleibt auch über die Beendigung des Arbeitsverhältnisses des betreffenden Mitarbeiters hinaus bestehen.

3.3 Besondere Kategorien Personenbezogener Daten und Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten

Besondere Kategorien Personenbezogener Daten dürfen grundsätzlich nicht verarbeitet werden. Ist die Verarbeitung Besonderer Kategorien Personenbezogener Daten notwendig, muss die ausdrückliche Einwilligung der Betroffenen Person eingeholt werden, soweit nicht

- die Verarbeitung zur Erfüllung von Pflichten und Ausübung bestimmter Rechte des Verantwortlichen oder der Betroffenen Person im Bereich der Beschäftigung und Sozialversicherung und sozialer Schutzrechte insoweit erforderlich ist, als sie durch geltendes lokales Recht oder einen Tarifvertrag nach geltendem lokalen Recht zur angemessenen Wahrung fundamentaler Rechte und Interessen der Betroffenen Person zulässig ist;
- die Betroffene Person aus physischen oder rechtlichen Gründen ihre Einwilligung nicht erteilen kann (z. B. bei medizinischen Notfällen) und die Verarbeitung zum Schutz lebenswichtiger Interessen der Betroffenen Person oder einer anderen natürlichen Person erforderlich ist; oder
- die Betroffene Person die fraglichen Daten bereits offenkundig öffentlich gemacht hat; oder
- die Verarbeitung der Daten zur Begründung, Ausübung oder Verteidigung von Rechtsansprüchen notwendig ist;
- die Verarbeitung notwendig ist für Zwecke der Präventiv- oder Arbeitsmedizin, die Beurteilung der Arbeitsfähigkeit des Arbeitnehmers, die medizinische Diagnose und Behandlung, Leistungen der Gesundheits- oder Sozialfürsorge, die Verwaltung des Gesundheits- oder Sozialwesens, Leistungen aufgrund geltender lokaler Gesetze oder die Erfüllung von Verträgen mit einem Angehörigen der Gesundheitsberufe, der dem Berufsgeheimnis unterliegt.

Vor der Verarbeitung der Besonderen Kategorien Personenbezogener Daten ist der verantwortliche DSB oder DSK des Teilnehmenden Unternehmens oder die Konzern-Datenschutzabteilung zu konsultieren.

Die Verarbeitung Personenbezogener Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten wird in der Regel nicht durchgeführt. Ist eine Verarbeitung dieser Daten notwendig, ist sie nur zulässig nach vorheriger Beratung mit der Konzern-Datenschutzabteilung unter der Kontrolle der zuständigen Aufsichtsbehörde oder vorbehaltlich angemessener Vorkehrungen, wie sie in der Datenschutz-Grundverordnung und anderen anwendbaren Datenschutzbestimmungen vorgesehen sind.

3.4 Automatisierte Entscheidungsfindung

Wenn Personenbezogene Daten zum Zweck der automatisierten Entscheidungsfindung verarbeitet werden, müssen die berechtigten Interessen der Betroffenen Person durch geeignete Maßnahmen gewahrt bleiben. Entscheidungen, die für die Betroffene Person nachteilige rechtliche Folgen haben oder die Betroffene Person anderweitig benachteiligen, dürfen nicht ausschließlich aufgrund eines automatisierten Einzelverfahrens getroffen werden, welches die persönlichen Eigenschaften der Person bewerten soll. Das bedeutet, dass Entscheidungen nicht ausschließlich auf der Nutzung von Informationstechnologie beruhen dürfen. Automatisierte Verfahren dürfen grundsätzlich nur als Hilfsmittel im Entscheidungsprozess verwendet werden.

Eine Ausnahme von diesem Grundsatz gilt, wenn:

- die Entscheidung im Zusammenhang mit dem Abschluss oder der Erfüllung eines Vertrags getroffen wird und die berechtigten Interessen der Betroffenen Person angemessen gewahrt werden, d. h. indem ihr Informationen über die zugrundeliegende Logik, wie eine solche Entscheidung zustande kommt, be-

reitgestellt werden und ihr die Möglichkeit gegeben wird, die Entscheidung zu überprüfen und diesbezüglich eine Stellungnahme abzugeben. Falls die Betroffene Person eine Stellungnahme abgibt, muss der jeweilige Verantwortliche seine Entscheidung überprüfen; oder

- sie durch geltendes lokales Gesetz zulässig ist; oder
- die Entscheidung auf der ausdrücklichen Einwilligung der Betroffenen Person beruht.

3.5 Verzeichnis von Verarbeitungstätigkeiten

Alle Teilnehmenden Unternehmen müssen ein Verzeichnis der Verarbeitungstätigkeiten, die im jeweiligen Unternehmen ausgeführt werden, dokumentieren und pflegen. Jeder DSK oder DSB ist verantwortlich dafür, dass das Verzeichnis der Verarbeitungstätigkeiten dokumentiert und regelmäßig angepasst wird. Die Konzern-Datenschutzabteilung ermöglicht den Teilnehmenden Unternehmen Zugang zu einem elektronischen System, in dem das Verzeichnis geführt werden sollte. Außerdem stellt die Konzern-Datenschutzabteilung den Teilnehmenden Unternehmen Vorlagen und Anweisungen zur Führung des Verzeichnisses zur Verfügung und überwacht die Einhaltung dieser Verpflichtung.

3.6 Datenschutz-Folgenabschätzung

Wenn eine Verarbeitungstätigkeit unter Berücksichtigung der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen Personen mit sich bringt, führen die Teilnehmenden Unternehmen eine Datenschutz-Folgenabschätzungen gemäß Artikel 35 der Datenschutz-Grundverordnung und der dazu von den Aufsichtsbehörden herausgegebenen Leitlinien durch. Die Konzern-Datenschutzabteilung bietet den DSK und DSB Leitlinien und Methoden für die Durchführung solcher Datenschutz-Folgenabschätzungen an.

Die rechtlichen Anforderungen hinsichtlich der Inhalte einer solchen Folgenabschätzung müssen beachtet werden.

Wenn eine Datenschutz-Folgenabschätzung ergibt, dass die Verarbeitung trotz Maßnahmen des Verantwortlichen zur Risikominderung dennoch ein hohes Risiko darstellen würde, darf der Verantwortliche die Verarbeitung weder beginnen noch fortsetzen und muss hierzu die zuständige Aufsichtsbehörde gemäß Artikel 36 der Datenschutz-Grundverordnung konsultieren.

3.7 Meldung und Dokumentation einer Datenschutzverletzung

Alle Teilnehmenden Unternehmen verpflichten sich, die Konzern-Datenschutzabteilung unverzüglich über eine (vermutete) Datenschutzverletzung zu informieren, die Personenbezogene Daten im Sinne dieser Verbindlichen Internen Datenschutzvorschriften betrifft. Handelt es sich bei dem Teilnehmenden Unternehmen um einen Auftragsverarbeiter, informiert es zusätzlich das Teilnehmende Unternehmen in seiner Funktion als Verantwortlicher.

Die Konzern-Datenschutzabteilung beurteilt die Art der Datenschutzverletzung, die Kategorien der betroffenen Daten und Personen sowie die Folgen für die Rechte und Freiheiten der Betroffenen Personen und stellt fest, ob die betreffende Datenschutzverletzung voraussichtlich ein (hohes) Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Eine Verletzung des Schutzes Personenbezogener Daten muss der zuständigen Datenschutzbehörde unverzüglich, spätestens jedoch binnen 72 Stunden, nachdem die Verletzung bekannt wurde, gemeldet werden, es sei denn, die Verletzung des Schutzes Personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen.

Im Falle einer Verletzung des Schutzes Personenbezogener Daten, die voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der Betroffenen Person zur Folge hat, wird die Betroffene Person unverzüglich über die Verletzung des Schutzes Personenbezogener Daten informiert.

Bei Bedarf koordiniert die Konzern-Datenschutzabteilung gemeinsam mit dem jeweiligen DSK/DSB die Meldung der Datenschutzverletzung an die Aufsichtsbehörde und/oder die Betroffenen Personen und stellt sicher, dass alle Datenschutzverletzungen angemessen dokumentiert und den betreffenden Behörden auf Anfrage vorgelegt werden.

Jede Verletzung des Schutzes Personenbezogener Daten muss dokumentiert werden (einschließlich der Fakten im Zusammenhang mit der Verletzung des Schutzes Personenbezogener Daten, ihrer Auswirkungen und der ergriffenen Korrekturmaßnahmen). Die Dokumentation ist der zuständigen Datenschutzbehörde auf Anfrage zur Verfügung zu stellen, um ihr zu ermöglichen, die Einhaltung der DSGVO zu überprüfen.

3.8 Privacy by Design und Privacy by Default

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos der Verarbeitung für die Rechte und Freiheiten natürlicher Personen ergreift jedes Teilnehmende Unternehmen geeignete technische und organisatorische Maßnahmen, um den Grundsätzen des Datenschutzes durch technische Gestaltung („Privacy by Design“) und datenschutzfreundliche Voreinstellungen („Privacy by Default“) gerecht zu werden.

Zu diesem Zweck sollen die Teilnehmenden Unternehmen interne Richtlinien verabschieden und Maßnahmen umsetzen, die unter anderem darauf abzielen, die Menge der verarbeiteten Personenbezogenen Daten zu minimieren, Personenbezogene Daten so weit wie möglich zu pseudonymisieren, Transparenz über die Funktionen und die Verarbeitung personenbezogener Daten zu gewährleisten und der Betroffenen Person die Überwachung der Datenverarbeitung sowie dem jeweiligen Verantwortlichen die Erstellung und Verbesserung von Sicherheitsmerkmalen zu ermöglichen.

Prozesse und Verfahren werden so konzipiert, entwickelt und umgesetzt, dass standardmäßig nur die Personenbezogenen Daten verarbeitet werden, die für einen bestimmten Zweck der Verarbeitung notwendig sind. Diese Verpflichtung gilt in Bezug auf (i) die Menge der erhobenen Personenbezogenen Daten, (ii) den Umfang ihrer Verarbeitung, (iii) die Dauer ihrer Speicherung und (iv) ihre Zugriffsmöglichkeiten.

3.9 Auftragsverarbeitung

Beauftragen Teilnehmende Unternehmen gemäß diesen Verbindlichen Internen Datenschutzvorschriften ein anderes Unternehmen mit der Verarbeitung Personenbezogener Daten, müssen die folgenden Anforderungen erfüllt werden:

- Der Auftragsverarbeiter wird vom Verantwortlichen sorgfältig ausgewählt; es wird nur ein Auftragsverarbeiter ausgewählt, der die notwendigen Garantien für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen bietet, die für eine Datenverarbeitung gemäß den Datenschutzbestimmungen erforderlich sind und die einen Schutz der Rechte der Betroffenen Personen sicherstellen;
- Der Verantwortliche stellt sicher und überprüft regelmäßig, dass der Auftragsverarbeiter die vereinbarten technischen und organisatorischen Sicherheitsmaßnahmen in vollem Umfang einhält;
- Der Leistungsumfang der Auftragsverarbeitung wird in einem schriftlichen oder anderweitig dokumentierten Vertrag geregelt, in dem die Rechte und Pflichten des Auftragsverarbeiters eindeutig definiert sind;

- Der Auftragsverarbeiter wird vertraglich dazu verpflichtet, die Daten, die er vom Verantwortlichen erhält, nur im Rahmen des Vertrags und gemäß den dokumentierten Anweisungen des Verantwortlichen zu verarbeiten. Die Verarbeitung Personenbezogener Daten für eigene Zwecke des Auftragsverarbeiters oder für Zwecke Dritter ist vertraglich untersagt, es sei denn, dass die Verarbeitung nach geltendem lokalen Recht erforderlich ist. In diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen vor der Verarbeitung über diese gesetzliche Anforderung, soweit dies nach geltendem lokalen Recht zulässig ist;
- Der Auftragsverarbeiter stellt sicher, dass sich die Personen, die zur Verarbeitung der Personenbezogenen Daten befugt sind, zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;
- Der Auftragsverarbeiter beauftragt ohne vorherige schriftliche gesonderte oder allgemeine schriftliche Genehmigung keinen weiteren Auftragsverarbeiter (Unterauftragsverarbeiter). Im vorstehenden Fall informiert der Auftragsverarbeiter den Verantwortlichen über alle beabsichtigten Änderungen hinsichtlich der zusätzlichen Beauftragung oder des Ersatzes anderer Auftragsverarbeiter und gibt somit dem Verantwortlichen Gelegenheit, gegen diese Änderungen Einspruch zu erheben. Der ursprüngliche Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen für die Pflichterfüllung und die Einhaltung der Bestimmungen der Datenschutz-Grundverordnung und anderer anwendbarer Datenschutzbestimmungen durch Unterauftragsverarbeiter vollständig haftbar;
- Unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen, unterstützt dieser den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen, soweit dies möglich ist, damit der Verantwortliche seine Verpflichtung zur Beantwortung von Betroffenenanfragen erfüllen kann;
- Unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen unterstützt dieser den Verantwortlichen bei der Umsetzung geeigneter technischer und organisatorischer Maßnahmen, informiert den Verantwortlichen unverzüglich über jede Datenschutzverletzung und stellt die für die Meldung von Datenschutzverletzungen an Aufsichtsbehörden und/oder betroffene Personen erforderlichen Informationen bereit. Außerdem unterstützt er den Verantwortlichen auf andere Weise bei der Einhaltung der Verpflichtungen gemäß Artikeln 32 bis 36 der Datenschutz-Grundverordnung;
- Der Auftragsverarbeiter hat je nach Wahl des Verantwortlichen entweder alle Personenbezogenen Daten nach Beendigung der Erbringung der mit der Verarbeitung verbundenen Dienstleistungen zu löschen oder an den Verantwortlichen zurückzugeben. Vorhandene Kopien sind zu löschen, es sei denn, dass geltende lokale Gesetze eine weitere Speicherung der personenbezogenen Daten erfordern;
- Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die notwendig sind, um die Einhaltung der in einem schriftlichen Vertrag zwischen ihnen festgelegten Verpflichtungen bzw. der geltenden Datenschutzbestimmungen zu gewährleisten. Auch Überprüfungen, einschließlich Inspektionen, die vom Verantwortlichen oder einem anderen vom Verantwortlichen beauftragten Prüfer durchgeführt werden, sind zu ermöglichen;
- Der Verantwortliche behält die Verantwortung für die Rechtmäßigkeit der Verarbeitung und bleibt der Ansprechpartner für Betroffene Personen und Aufsichtsbehörden.

3.10 Rechte der Betroffenen Personen

Betroffene Personen haben bezüglich ihrer Personenbezogenen Daten, die von einem Teilnehmenden Unternehmen im Rahmen dieser Verbindlichen Internen Datenschutzvorschriften verarbeitet werden, die folgenden unabdingbaren Rechte:

- Die Betroffene Person kann **Informationen über die Personenbezogenen Daten**, die über sie gespeichert sind, und den Zweck der Verarbeitung fordern. Die Betroffene Person hat außerdem das Recht auf Informationen über die Identität des Verantwortlichen, die Kategorien der Betroffenen Personenbezogenen Daten, die Empfänger oder Kategorien von Empfängern, denen die Daten offengelegt werden oder offengelegt werden können, sowie über die Quellen, aus denen die Daten stammen, wenn sie nicht von der Betroffenen Person erhoben wurden. Das Recht auf Informationen schließt auch die vorgesehene Dauer der Speicherung der Personenbezogenen Daten und die zugrundeliegende Logik des Profilings und der automatisierten Verarbeitung ein, soweit automatisierte Entscheidungen Betroffen sind. Die Betroffene Person erhält darüber hinaus Informationen über die Rechte, die sie gemäß diesem Abschnitt hat, einschließlich des Rechts, Beschwerde bei einer Aufsichtsbehörde einzureichen.

  Die oben genannten Informationen müssen auf verständliche Weise bereitgestellt werden; d. h. die Betroffene Person hat einen Anspruch auf eine Kopie ihrer verarbeiteten Personenbezogenen Daten oder zumindest auf Angaben zu diesen Daten in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie klarer und einfacher Sprache. Stellt die Betroffene Person die Anfrage elektronisch und, so weit nicht anders von ihr gefordert, wird die Information in allgemein üblicher elektronischer Form bereitgestellt. Sind Anfragen der Betroffenen Person offenkundig unbegründet oder unverhältnismäßig, insbesondere aufgrund ihres Wiederholungscharakters, kann der Verantwortliche entweder (i) eine angemessene Gebühr für die Kosten der Zusammenstellung und Bereitstellung der Informationen erheben oder (ii) es ablehnen, der Anfrage nachzukommen.

- Die Betroffene Person kann eine **Berichtigung** fordern, falls ihre Personenbezogenen Daten falsch oder unvollständig sind.

- Die Betroffene Person hat das **Recht auf Löschung** ihrer Personenbezogenen Daten, (i) wenn die Datenverarbeitung unrechtmäßig war oder in der Zwischenzeit unrechtmäßig geworden ist, (ii) sobald die Daten nicht länger für den Verarbeitungszweck benötigt werden, (iii) wenn die Betroffene Person ihre Einwilligung für die Verarbeitung widerruft, vorausgesetzt, dass es keinen anderen rechtlichen Grund für die Verarbeitung gibt, (iv) falls die Betroffene Person Einspruch gegen die Verarbeitung erhebt und es keine übergeordneten rechtmäßigen Gründe für die Verarbeitung gibt, oder (v) wenn die Löschungsverpflichtung durch lokale Gesetze festgelegt ist, denen der Verantwortliche unterliegt.

  Begründete Ansprüche der Betroffenen Person auf Löschung sind zu erfüllen, es sei denn, die Verarbeitung ist erforderlich für (i) die Erfüllung einer rechtlichen Verpflichtung, die durch lokales Recht festgelegt ist und der der Verantwortliche unterliegt, oder für (ii) die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Falls gesetzliche Aufbewahrungsfristen gelten oder Personenbezogene Daten nicht gelöscht werden können, kann auf Anfrage der Betroffenen Person die Verarbeitung der betroffenen Daten eingeschränkt werden.

- Die Betroffene Person hat das Recht, die Verarbeitung Personenbezogener Daten **einschränken** zu lassen, wenn (i) die Richtigkeit der personenbezogenen Daten bestritten wird, für einen Zeitraum, der es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen; (ii) die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung ihrer Nutzung verlangt; (iii) der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht mehr benötigt, sie jedoch von der Betroffenen Person zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt werden oder (iv) falls die Betroffene Person der Verarbeitung widersprochen hat und die Überprüfung, ob die berechtigten Gründe des Verantwortlichen die der betroffenen Person überwiegen, noch aussteht.

- Die Betroffene Person hat das **Recht auf eine Benachrichtigung** bezüglich der Berichtigung, Löschung oder Einschränkung ihrer Personenbezogenen Daten.
- Die Betroffene Person hat das Recht, ihre Personenbezogenen Daten, die sie dem Verantwortlichen zur Verfügung gestellt hat, in strukturierter, allgemein üblicher und maschinenlesbarer Form zu erhalten und hat das Recht, diese Daten einem anderen Verantwortlichen zu übermitteln („**Recht auf Datenportabilität**"), vorausgesetzt, (i) die Verarbeitung der Daten erfolgt durch Einwilligung der Betroffenen Person oder alternativ aufgrund des Vertrags mit der Betroffenen Person und (ii) die Verarbeitung erfolgt anhand von automatisierten Mitteln.
- Die Betroffene Person hat **das Recht, nicht einer Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung** – einschließlich Profiling – **beruht** („automatisierte Entscheidungsfindung") und für diese Person Rechtswirksamkeit hat, es sei denn, die Entscheidung (i) ist notwendig für den Abschluss oder die Erfüllung eines Vertrags, (ii) beruht auf der ausdrücklichen Einwilligung der Betroffenen Person oder (iii) ist nach geltendem lokalen Recht zulässig.
- Die Betroffene Person hat **das Recht**, jederzeit aus Gründen, die sich aus ihrer besonderen Situation ergeben, **der Verarbeitung** ihrer Personenbezogenen Daten **zu widersprechen**, wenn diese auf dem berechtigten Interesse des Verantwortlichen beruht oder für die Erfüllung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt erforderlich ist, die dem Verantwortlichen übertragen wurde. Der Verantwortliche darf die betreffenden Personenbezogenen Daten nicht mehr verarbeiten, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der Betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
- Die Betroffene Person hat das Recht, jederzeit der Verarbeitung ihrer Personenbezogenen Daten für Direktmarketingzwecke, einschließlich Profiling, soweit es mit solchem Direktmarketing in Verbindung steht, zu widersprechen. Wenn die Betroffene Person der Verarbeitung für Direktmarketingzwecke widerspricht, dürfen die Personenbezogenen Daten für diese Zwecke nicht mehr verarbeitet werden.
- Die Betroffene Person hat **das Recht, eine Beschwerde einzulegen oder einen Anspruch zur Durchsetzung ihrer Rechte als Drittbegünstigter geltend zu machen**. Eine solche Beschwerde kann insbesondere bei der für ams OSRAM zuständigen Aufsichtsbehörde, bei einer Aufsichtsbehörde im EWR-Land, in dem die Person ihren gewöhnlichen Aufenthaltsort bzw. ihren Arbeitsplatz hat, oder in dem Land, in welchem der mutmaßliche Verstoß stattgefunden hat, eingereicht werden. Eine rechtliche Klage kann auch vor einem Gericht des Mitgliedstaats erhoben werden, in dem der Datenexporteur oder ams OSRAM Co-Headquarter mit Datenschutzverantwortung bzw. eine Niederlassung hat, oder in dem die Betroffene Person ihren gewöhnlichen Aufenthaltsort hat (je nach Wahl der Betroffenen Person). In dieser Hinsicht kann die Betroffene Person durch eine Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht vertreten werden, die ordnungsgemäß nach dem Recht eines Mitgliedstaats gegründet ist, deren satzungsmäßige Ziele im öffentlichen Interesse liegen und die im Bereich des Schutzes der Rechte und Freiheiten von Betroffenen Personen in Bezug auf den Schutz ihrer Personenbezogenen Daten tätig ist. Die Betroffene Person wird angehalten, zunächst die in den Verbindlichen Internen Datenschutzvorschriften festgelegten Beschwerdeverfahren zu befolgen, bevor sie Beschwerde einreicht oder anderweitige Rechtsmittel ergreift. Dies gilt unbeschadet der Rechte und Rechtsmittel, die der Betroffenen Person nach geltendem Recht zustehen.
- Wenn die Datenverarbeitung auf einer Einwilligung der Betroffenen Person basiert, hat diese **das Recht, ihre Einwilligung jederzeit zu widerrufen**.

Die Betroffene Person kann die oben genannten Rechte schriftlich gegenüber dem Teilnehmenden Unternehmen, dem zuständigen DSK/DSB des Teilnehmenden Unternehmens oder der Konzern-Datenschutzabteilung geltend machen. Der berechtigte Antrag der Betroffenen Person wird von der kontaktierten Stelle innerhalb eines angemessenen Zeitraums schriftlich beantwortet (eine E-Mail ist ausreichend).

Das Teilnehmende Unternehmen hat der Betroffenen Person die Ausübung der oben aufgeführten Rechte zu ermöglichen. Zu diesem Zweck beantwortet das Teilnehmende Unternehmen oder die Konzern-Datenschutzabteilung die Anfrage der Betroffenen Person ohne unzumutbare Verzögerung und in jedem Fall innerhalb eines Monats nach Eingang der Anfrage. Unter Berücksichtigung der Komplexität und der Anzahl der Anfragen kann diese Frist um höchstens zwei (2) weitere Monate verlängert werden. Die Betroffene Person wird hierüber innerhalb eines Monats nach Eingang der Anfrage informiert.

3.11 Rechenschaftspflicht

Alle Teilnehmenden Unternehmen werden aufgefordert, Maßnahmen zu ergreifen, die die Einhaltung der Anforderungen der Verbindlichen Internen Datenschutzvorschriften, der Datenschutz-Grundverordnung und anderer geltender Datenschutzbestimmungen belegen, insbesondere durch eine entsprechende Dokumentation. Zu diesem Zweck werden sie (i) Datenschutz- und Informationssicherheitsrichtlinien und -bestimmungen wahren und umsetzen, (ii) ein Verzeichnis der Kategorien von Verarbeitungstätigkeiten führen (diese Verzeichnisse enthalten insbesondere den Namen und die Kontaktdaten des Verantwortlichen oder Auftragsverarbeiters, sowie gegebenfalls des Datenschutzbeauftragten, die Zwecke der Verarbeitung, die bestehenden Löschfristen und eine allgemeine Beschreibung der Kategorien Betroffener Personen und Personenbezogener Daten, die Empfänger, gegenüber denen die Personenbezogenen Daten offengelegt worden sind oder werden, die getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung und die erfolgten Übermittlungen in Drittländer einschließlich der bestehenden Garantien zur Datensicherheit. Diese Verzeichnisse werden schriftlich, oder elektronisch dokumentiert und der Aufsichtsbehörde auf Anfrage zur Verfügung gestellt.), (iii) wo notwendig die Anforderungen des Datenschutzes durch technische Gestaltung („Privacy by Design“) und datenschutzfreundliche Voreinstellungen („Privacy by Default“) einhalten, (iv) schriftliche Verträge mit Datenauftragsverarbeitern oder sonstigen Verantwortlichen abschließen, (v) einen DSB benennen sowie (vi) eine Datenschutz-Folgenabschätzung für Verarbeitungsvorgänge, die voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen mit sich bringen, vornehmen. Geht aus einer Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern das Teilnehmende Unternehmen keine Maßnahmen zur Eindämmung des Risikos trifft, wird vor der Verarbeitung die zuständige Aufsichtsbehörde konsultiert.

Die Rechenschaftspflichten sind fortlaufend und die getroffenen Maßnahmen sind regelmäßig zu überprüfen und zu aktualisieren.

3.12 Beschreibung der Datenübermittlung

ams OSRAM verfügt über eine komplexe Konzernstruktur mit einer Vielzahl an Teilnehmenden Unternehmen, zwischen denen Personenbezogene Daten für zahlreiche Zwecke ausgetauscht werden. Der Datenaustausch findet zwischen Teilnehmenden Unternehmen statt, die ihren Sitz in einem EWR-Land haben, ebenso wie mit Teilnehmenden Unternehmen mit Sitz außerhalb des EWR. Der Bedarf zum Austausch von Daten innerhalb des ams OSRAM Konzerns betrifft Personenbezogene Daten von Mitarbeitern, bestehenden und potenziellen Kunden, Lieferanten, Dienstleistern, Aktionären, sonstigen Geschäfts- und Vertragsparteien sowie Bewerbern und Beschwerdeführern. Dazu gehören – je nach Verwendungszweck – Mitarbeiter- und Vertragsstammdaten, Beschäftigungsdaten und -historie, Daten zu Schulungen oder Ausbildungen, Mitarbeiterbewertungen, Bank- und Kreditkarteninformationen, Kommunikationsinformationen, einige Besondere Kategorien Personenbezogener Daten (z. B. Informationen über Familienstand, Religionszugehörigkeit, physische und psychische Gesundheit), etc. Diese Daten

werden innerhalb der konsolidierten ams OSRAM Konzerngesellschaften ausschließlich im Rahmen üblicher Geschäftszwecke sowie für interne Verwaltungszwecke verarbeitet und übermittelt.

Die Datenübermittlung erfolgt zum Zweck der Personalbeschaffung, der Personalverwaltung und -entwicklung, für Compliance-Zwecke, zur Ausführung und Umsetzung von Aufträgen und Projekten für externe und interne Kunden, zur Verarbeitung von Bestellungen und Arbeitsaufträgen mit Lieferanten und Dienstleistern, zur Erfüllung von Berichtspflichten, für die Erfüllung von Verbindlichkeiten aus Lieferungen und Leistungen oder den Einzug von Forderungen aus Lieferungen und Leistungen, für das Rechnungswesen, für interne Kommunikationszwecke, zur kostensenkenden Konsolidierung und Bündelung von IT-Prozessen in bestimmten Regionen sowie im Zusammenhang mit der Kooperation und Koordination von Konzerngesellschaften auf regionaler und globaler Ebene bei globalen Geschäftsvorgängen und Projekten.

3.13 Verfahrensfragen

3.13.1 Verbindlichkeit der Verbindlichen Internen Datenschutzvorschriften

Die Verbindlichen Internen Datenschutzvorschriften sind umfassend verbindlich.

3.13.1.1 Verbindlichkeit für Konzerngesellschaften und Teilnehmende Unternehmen

Verbindliche Interne Datenschutzvorschriften wurden von den Governance-Verantwortlichen des ams OSRAM Konzerns verabschiedet und durch die Veröffentlichung der Unternehmensrichtlinie CO3000 (die Verbindlichen Internen Datenschutzvorschriften für ams OSRAM Konzerngesellschaften und Beitretende Unternehmen zum Schutz Personenbezogener Daten zum Schutz Personenbezogener Daten) in Kraft gesetzt.

Die Verantwortung für die Umsetzung der Verbindlichen Internen Datenschutzvorschriften im Teilnehmenden Unternehmen liegt bei seiner Geschäftsführung, die Ausführung in Einzelfällen liegt bei der Stelle innerhalb dieses Unternehmens, welche die Personenbezogenen Daten als Teil ihrer besonderen Funktion verarbeitet. In den ams OSRAM Konzerngesellschaften liegt die Verantwortung beim gesetzlichen Vertreter der jeweiligen ams OSRAM Konzerngesellschaft in seiner/ihrer Funktion als Data Protection Executive (DPE).

Die Verbindlichen Internen Datenschutzvorschriften sind von allen ams OSRAM Konzerngesellschaften sowie allen Beitretenden Unternehmen bindend zu wahren und einzuhalten.

Um den Beitritt zu den Verbindlichen Internen Datenschutzvorschriften und deren Umsetzung zu dokumentieren, muss bei Konzerngesellschaften die Geschäftsführung der Konzerngesellschaft dem Inter-Company Agreement beitreten. Durch Unterzeichnung des Inter-Company Agreements und die nachfolgende Annahme der betreffenden Bewerbung durch den ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung werden die Bestimmungen der Verbindlichen Internen Datenschutzvorschriften für die jeweilige Konzerngesellschaft individuell verbindlich. Das Inter-Company Agreement wird von der Geschäftsführung der Konzerngesellschaft unterzeichnet und an die Konzern-Datenschutzabteilung im ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung zurückgeschickt. Das Inter-Company Agreement wird von der Konzern-Datenschutzabteilung gepflegt und bei Bedarf aktualisiert.

Grundsätzlich müssen alle ams OSRAM Konzerngesellschaften die Verbindlichen Internen Datenschutzvorschriften unterzeichnen und umsetzen, außer der ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung hat eine Ausnahme von der Umsetzung der Verbindlichen Internen Datenschutzvorschriften aus triftigem Grund gewährt (z. B. keine Geschäftstätigkeit, keine Mitarbeiter, keine Verarbeitung Personenbezogener Daten, bevorstehende Auflösung oder Veräußerung). Die betreffende ams OSRAM Konzerngesellschaft muss den Antrag auf eine Ausnahme unter Angabe des Grundes per E-Mail an

die Konzern-Datenschutzabteilung übermitteln. Die Konzern-Datenschutzabteilung wird über die Berechtigung des Antrags entscheiden und der Konzerngesellschaft ihre Entscheidung mitteilen. In diesem Fall sind Datenübermittlungen zwischen dieser ams OSRAM Konzerngesellschaft und anderen ams OSRAM Konzerngesellschaften nur möglich, wenn sonstige geeignete Vorkehrungen getroffen werden, die gemäß Artikel 45-48 der Datenschutz-Grundverordnung ein angemessenes Schutzniveau für die Personenbezogenen Daten gewährleisten.

Beitretende Unternehmen, d. h. die Unternehmen, die keine ams OSRAM Konzerngesellschaften sind, an denen die ams OSRAM Muttergesellschaft eine direkte oder indirekte Beteiligung hält, können sich freiwillig verpflichten, die Bestimmungen der Verbindlichen Internen Datenschutzvorschriften einzuhalten, wenn die Konzern-Datenschutzabteilung einem solchen Antrag zustimmt. Ob anderen Unternehmen als den ams OSRAM Konzerngesellschaften die freiwillige Teilnahme am Prozess der Verbindlichen Internen Datenschutzvorschriften gewährt wird, liegt im Ermessen der Konzern-Datenschutzabteilung.

Um die Annahme und Umsetzung der Verbindlichen Internen Datenschutzvorschriften durch das Beitretende Unternehmen zu dokumentieren wird zwischen dem ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung und dem Beitretenden Unternehmen ein Inter-Company Agreement geschlossen; die Verbindlichen Internen Datenschutzvorschriften sind dem Inter-Company Agreement als Anhang beigefügt. Mit Abschluss des Inter-Company Agreements werden die Bestimmungen der Verbindlichen Internen Datenschutzvorschriften für das Beitretende Unternehmen verbindlich. Der Text des Inter-Company Agreements wird von der Konzern-Datenschutzabteilung gepflegt.

Die Konzern-Datenschutzabteilung führt im ams OSRAM Intranet ein elektronisches Register der Teilnehmenden Unternehmen, die sich durch einen Beitritt zum Inter-Company Agreement verpflichtet haben, die Bestimmungen der Verbindlichen Internen Datenschutzvorschriften einzuhalten, sowie auch ihrer Kontaktdaten. Die aktuelle Version des elektronischen Registers (Statusübersicht) kann jederzeit im Intranet eingesehen werden (verlinkt unter https://privacy.ams-osram.com) und wird als Anhang zu den Verbindlichen Internen Datenschutzvorschriften beigefügt.

In der Statusübersicht sind auch die Konzerngesellschaften enthalten und gekennzeichnet, denen ausnahmsweise aus triftigem Grund eine Ausnahme von der Verpflichtung zur Unterzeichnung und Umsetzung der Verbindlichen Internen Datenschutzvorschriften gewährt wurde. Die Statusübersicht erfasst und kennzeichnet auch die Konzerngesellschaften, die ihrer Verpflichtung zur Annahme und Umsetzung der Verbindlichen Internen Datenschutzvorschriften (noch) nicht nachgekommen sind.

Wenn eine Konzerngesellschaft dem Inter-Company Agreement zu den Verbindlichen Internen Datenschutzvorschriften (noch) nicht beigetreten ist, muss die Rechtmäßigkeit der Datenübermittlung durch geeignete Vorkehrungen wie die Unterzeichnung und Umsetzung der Standardvertragsklauseln gewährleistet werden.

Die Verpflichtung zur Einhaltung der Verbindlichen Internen Datenschutzvorschriften kann durch Widerruf, Aufhebung oder Kündigung seitens des ams OSRAM Co-Hauptsitzes mit Datenschutzverantwortung oder seitens des Teilnehmenden Unternehmens beendet werden. Der Verlust des Status als Konzerngesellschaft bedeutet nicht automatisch ein Ende der Verpflichtungen, die sich aus den Verbindlichen Internen Datenschutzvorschriften ergeben. In diesem Fall ist eine Kündigung der Verbindlichen Internen Datenschutzvorschriften durch den ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung oder durch die (frühere) Konzerngesellschaft notwendig. Auch bei Widerruf/Aufhebung des Inter-Company Agreements oder bei Kündigung der Verbindlichen Internen Datenschutzvorschriften bleiben die Verpflichtungen aus diesen Verbindlichen Internen Datenschutzvorschriften bezüglich der Personenbezogenen Daten, die bis zum Widerruf, der Aufhebung oder Kündigung verarbeitet wurden, bestehen, bis diese Daten vom betreffenden Unternehmen gemäß den gesetzlichen Vorschriften gelöscht wurden.

3.13.1.2 Verbindlichkeit gegenüber Mitarbeitern Teilnehmender Unternehmen

Die Bestimmungen der Verbindlichen Internen Datenschutzvorschriften sind für Mitarbeiter der Teilnehmenden Unternehmen ebenfalls verbindlich. Der CEO des jeweiligen Teilnehmenden Unternehmens ist verpflichtet, durch geeignete Mittel sicherzustellen, dass die Verbindlichen Internen Datenschutzvorschriften für die Mitarbeiter eine verbindliche Rechtswirkung haben.

Die Verbindlichen Internen Datenschutzvorschriften und alle sonstigen internen Datenschutzbestimmungen stehen den Mitarbeitern der Teilnehmenden Unternehmen jederzeit zur Verfügung.

Die Teilnehmenden Unternehmen informieren ihre Mitarbeiter darüber, dass eine Nichteinhaltung der Bestimmungen der Verbindlichen Internen Datenschutzvorschriften für die Mitarbeiter zu disziplinarischen oder arbeitsrechtlichen Maßnahmen (z. B. Abmahnung, Kündigung) führen kann.

3.13.1.3 Verbindlichkeit gegenüber Betroffenen Personen

Einige Bestimmungen der Verbindlichen Internen Datenschutzvorschriften sind im Wege der Drittbegünstigung auch gegenüber Betroffenen Personen verbindlich. Drittbegünstigenden Charakter haben die Bestimmungen in folgenden Abschnitten: Abschnitte 3.2 – 3.4, 3.7, 3.8, 3.10, 3.13.1.3, 3.13.2, 3.13.6, 3.13.8, 3.13.9 and 3.15.

Betroffene Personen sind berechtigt, die Einhaltung eines der oben genannten drittbegünstigenden Rechte durch ein Teilnehmendes Unternehmen mit einer Beschwerde bei der zuständigen Aufsichtsbehörde oder mit anderen Rechtsmitteln bei den zuständigen Gerichten durchzusetzen. Betroffene Personen können dabei Schadenersatz geltend machen.

Es steht den Betroffenen Personen frei, ihre Ansprüche einzureichen:

- bei der Aufsichtsbehörde oder den Gerichten des EWR-Landes, in dem das Teilnehmende Unternehmen, welches die Daten übermittelt hat, seinen Sitz hat; oder
- bei der zuständigen Aufsichtsbehörde oder den Gerichten des EWR-Landes, in dem die Betroffene Person ihren gewöhnlichen Aufenthalt oder Arbeitsplatz hat, wenn die Betroffene Person im EWR ansässig ist; oder
- bei der zuständigen Aufsichtsbehörde oder den Gerichten des EWR-Landes des Ortes des mutmaßlichen Verstoßes; oder
- bei der Aufsichtsbehörde oder den Gerichten des EWR-Landes, in dem der ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung seinen Sitz hat; oder
- bei der zuständigen Aufsichtsbehörde.

Das bedeutet, dass bei einem Verstoß gegen die Bestimmungen der Verbindlichen Internen Datenschutzvorschriften durch ein Teilnehmendes Unternehmen mit Sitz außerhalb des EWR auch Gerichte und Behörden innerhalb des EWR zuständig sind. In diesen Fällen hat die Betroffene Person dieselben Rechte gegenüber dem ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung, als ob dieses selbst und nicht das Teilnehmende Unternehmen außerhalb des EWR gegen die Bestimmungen verstoßen hätte.

Um die Drittbegünstigung der Betroffenen Personen auch in den Ländern sicherzustellen, in denen eine Einräumung der Drittbegünstigung nach den Verbindlichen Internen Datenschutzvorschriften möglicherweise nicht ausreicht, wird ams OSRAM im notwendigen Umfang zusätzliche vertragliche Vereinbarungen mit den betreffenden Unternehmen ausarbeiten. Eine Drittbegünstigungsklausel, die den Betroffenen Personen die notwendigen Rechte einräumt, ist im Inter-Company Agreement enthalten, den die Konzern-

und beitretenden Unternehmen unterzeichnen, um ihre Akzeptanz und Umsetzung der Verbindlichen Internen Datenschutzvorschriften anzuzeigen.

3.13.2 Veröffentlichung der verbindlichen internen Datenschutzvorschriften

Die Verbindlichen Internen Datenschutzvorschriften und die Drittbegünstigungsklausel sind den Betroffenen Personen leicht zugänglich. Die Betroffene Person kann den zuständigen DSK oder DSB des Teilnehmenden Unternehmens oder alternativ den ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung direkt kontaktieren. Zusammen mit Informationen aus Unterabschnitt 3.2.3 (Transparenz) wird ams OSRAM die Verbindlichen Internen Datenschutzvorschriften den Betroffenen Personen auf angemessene Weise zugänglich machen, insbesondere durch die Veröffentlichung der aktuellsten Version auf der ams OSRAM Internet-Seite. Zusätzliche einschlägige Dokumente zu den Verbindlichen Internen Datenschutzvorschriften – d. h. die Anhänge, auf die dort Bezug genommen wird – werden der Betroffenen Person auf Anfrage an die Konzern-Datenschutzabteilung zur Verfügung gestellt.

3.13.3 Umsetzung der Verbindlichen Internen Datenschutzvorschriften in den Teilnehmenden Unternehmen

Die Geschäftsführung eines Teilnehmenden Unternehmens – oder der CEO eines Teilnehmenden Unternehmens in seiner Funktion als Data Protection Executive – ist für die ordnungsgemäße Umsetzung und Einhaltung der Verbindlichen Internen Datenschutzvorschriften verantwortlich. Die Geschäftsführung des Teilnehmenden Unternehmens kann diese Aufgabe – jedoch nicht die Verantwortung – an den DSK oder den DSB delegieren.

ams OSRAM hat ein weltweites Netzwerk von DSK und DSB etabliert. Durch den Beitritt zum Inter-Company Agreement zu den Verbindlichen Internen Datenschutzvorschriften ernennt jedes Teilnehmende Unternehmen einen DSK oder, falls erforderlich, einen DSB und schickt die Kontaktdaten des DSK oder DSB an die Konzern-Datenschutzabteilung. Das Teilnehmende Unternehmen teilt der Konzern-Datenschutzabteilung unverzüglich jede Änderung der Identität des DSK oder DSB mit.

Der DSK oder DSB (i) dient als lokaler Kontakt für Betroffene Personen, d. h. im Rahmen des Beschwerdeverfahrens, (ii) überwacht die Umsetzung und Einhaltung der Verbindlichen Internen Datenschutzvorschriften, (iii) berät Mitarbeiter in Datenschutzfragen, (iv) fördert die Zusammenarbeit zwischen der Konzern-Datenschutzabteilung, der Prüfungsabteilung oder Aufsichtsbehörden und einem Teilnehmenden Unternehmen bei Fragen und (v) führt und aktualisiert notwendige Verzeichnisse von Verarbeitungstätigkeiten und Datenschutz-Folgenabschätzungen für Zwecke der Rechenschaftspflicht.

Der DSB/DSK berichtet einmal jährlich an die Geschäftsführung des betreffenden Teilnehmenden Unternehmens und der DSK berichtet regelmäßig – mindestens einmal jährlich – an die Konzern-Datenschutzabteilung. Der DSK/DSB berichtet über Angelegenheiten, die insbesondere den Umsetzungsgrad der Verbindlichen Internen Datenschutzvorschriften im jeweiligen Teilnehmenden Unternehmen beinhalten.

Der Leiter der Konzern-Datenschutzabteilung steht der Abteilung vor und koordiniert und leitet alle DSK/DSB der Teilnehmenden Unternehmen. Der Leiter der Konzern-Datenschutzabteilung berichtet an den Head of Compliance von ams OSRAM, der Head of Compliance berichtet an den CFO. Der Leiter der Konzern-Datenschutzabteilung koordiniert und treibt die konzernweite Umsetzung der Verbindlichen Internen Datenschutzvorschriften in den Teilnehmenden Unternehmen voran, insbesondere das Einsammeln der Inter-Company Agreements, berät und leitet die DSK bezüglich der Umsetzung dieser Verbindlichen Internen Datenschutzvorschriften und der Einholung und Auswertung der regelmäßigen Berichte der DSK/DSB in Hinsicht auf Datenschutz und Implementierungsstatus der Verbindlichen Internen Datenschutzvorschriften.

Darüber hinaus ist der Leiter der Konzern-Datenschutzabteilung zuständig für die Erstellung und Bereitstellung geeigneter Schulungen zu den Verbindlichen Internen Daten-

schutzvorschriften für die Teilnehmenden Unternehmen. Zusätzlich überwacht der Leiter der Konzern-Datenschutzabteilung die Aktualisierung der Verbindlichen Internen Datenschutzvorschriften und Meldung der Aktualisierungen an die zuständigen Aufsichtsbehörden. Die Konzern-Datenschutzabteilung unterstützt den Leiter der Abteilung bei der Erfüllung seiner Aufgaben.

Der Leiter der Konzern-Datenschutzabteilung sowie auch Mitglieder der Konzern-Datenschutzabteilung können anhand der in Abschnitt 3.16 genannten Kontaktdaten direkt angesprochen werden.

Der Leiter der Konzern-Datenschutzabteilung berichtet einmal jährlich zusammen mit den Datenschutzbeauftragten der ams OSRAM Muttergesellschaft und des ams OSRAM Co-Hauptsitzes mit Datenschutzverantwortung an den Vorstand der ams OSRAM Muttergesellschaft. Dieser Bericht beinhaltet insbesondere den Umsetzungsgrad der Verbindlichen Internen Datenschutzvorschriften in allen Teilnehmenden Unternehmen.

3.13.4 Überwachung der Einhaltung der Verbindlichen Internen Datenschutzvorschriften

Die Einhaltung der Verbindlichen Internen Datenschutzvorschriften durch die Teilnehmenden Unternehmen unterliegt einer regelmäßigen Prüfung in erster Linie durch den DSK oder den DSB, der von der Geschäftsführung des Teilnehmenden Unternehmens ernannt wurde. Die Geschäftsführung des Teilnehmenden Unternehmens unterstützt den DSK bei der Ausübung seiner Pflichten und bindet ihn bei Beschwerden von Betroffenen Personen, dass die Verbindlichen Internen Datenschutzvorschriften nicht eingehalten worden seien, mit ein.

Bei Verstößen gegen den Datenschutz und Problemen von grundlegender Bedeutung, zieht der DSK/DSB den Leiter der Konzern-Datenschutzabteilung hinzu und berücksichtigt dessen Rat und Entscheidungen bei der Behebung von Verletzungen des Schutzes Personenbezogener Daten und anderen Problemen.

Der ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung ist dazu berechtigt, stichprobenartig die Arbeit des DSK im Zusammenhang mit der Umsetzung und Einhaltung der Verbindlichen Internen Datenschutzvorschriften des Teilnehmenden Unternehmens zu prüfen, entweder durch die Anforderung einer schriftlichen Selbsteinschätzung des DSK/DSB oder im Rahmen eines Überprüfungsgesprächs. Der Inhalt des Überprüfungsgesprächs wird durch den Prüfer dokumentiert.

Jedes Teilnehmende Unternehmen, das Daten übermittelt, hat das Recht, in Einzelfällen die Datenverarbeitung beim empfangenden Teilnehmenden Unternehmen zu prüfen. Dabei übt das übermittelnde Unternehmen alle Rechte aus, die der Betroffenen Person zugesichert wurden und es unterstützt Betroffene Personen, denen durch einen Verstoß gegen die Pflichten der Verbindlichen Internen Datenschutzvorschriften ein Schaden entstanden ist, bei der Sicherung ihrer Rechte gegenüber dem dafür verantwortlichen Unternehmen.

3.13.5 Schulung

Ein wesentlicher Aspekt der ordnungsgemäßen Umsetzung der Verbindlichen Internen Datenschutzvorschriften ist die geeignete Bereitstellung von Informationen und Unterweisung von Mitarbeitern. Dazu gehört die Information der Mitarbeiter, dass Verstöße gegen die Verbindlichen Internen Datenschutzvorschriften straf-, haftungs- oder arbeitsrechtliche Konsequenzen haben können.

ams OSRAM bietet spezielle Informations- und Schulungsmaßnahmen zu den Verbindlichen Internen Datenschutzvorschriften an, in denen den Mitarbeitern Teilnehmender Unternehmen im Zusammenhang mit der Umsetzung dieser Verbindlichen Internen Datenschutzvorschriften geeignete Informationen und Schulungen zum ordnungsgemäßen Umgang und Schutz Personenbezogener Daten vermittelt werden. Die Schulung sollte sich unter anderem mit den Verfahren zur Bearbeitung von Anfragen öffentlicher Behör-

den in Bezug auf den Zugriff auf Personenbezogene Daten befassen. Diese Schulungsmaßnahmen richten sich insbesondere an Mitarbeiter, die ständig oder regelmäßig mit Personenbezogenen Daten umgehen. Für diese Mitarbeiter ist die Schulungsteilnahme verpflichtend. Die Schulungen zu den Verbindlichen Internen Datenschutzvorschriften werden mindestens alle drei (3) Jahre wiederholt.

Zu den Informations- und Schulungsmaßnahmen zählen beispielsweise die Bereitstellung von webbasierten Schulungen, geeigneten Präsentationen und Schulungsunterlagen zum Selbststudium, Präsenzschulungen und die Organisation von Workshops, die speziell auf Mitarbeiter zugeschnitten sind.

Die erfolgreiche Teilnahme von Mitarbeitern an Schulungen ist zu dokumentieren.

Weitere Einzelheiten werden in einem detaillierten Schulungskonzept beschrieben.

3.13.6 Internes Beschwerdeverfahren

Betroffene Personen können jederzeit die zuständige interne Beschwerdeabteilung (die Konzern-Datenschutzabteilung, Kontaktdaten siehe Abschnitt 3.16 Kontakt) oder das Teilnehmende Unternehmen (siehe Kontaktinformationen im Anhang I) kontaktieren, wenn sie sich über einen Verstoß gegen die Verbindlichen Internen Datenschutzvorschriften durch ein Teilnehmendes Unternehmen beschweren möchten oder Fragen haben. Beschwerden Betroffener Personen können in elektronischer oder schriftlicher Form eingereicht werden. Unabhängig von der Art der Einreichung werden alle Beschwerden oder Anfragen an die Konzern-Datenschutzabteilung weitergeleitet und von dieser bearbeitet. Die Betroffene Person erhält von der kontaktierten Stelle umgehend eine Eingangsbestätigung für die Beschwerde, die innerhalb eines angemessenen Zeitraums beantwortet wird, in jedem Fall innerhalb eines (1) Monats nach Beschwerdeeingang. Unter Berücksichtigung der Komplexität und der Anzahl der Anfragen kann diese Frist um höchstens zwei (2) weitere Monate verlängert werden. Die Betroffene Person wird hierüber innerhalb eines Monats nach Eingang der Anfrage informiert.

Den mit der Beschwerdeverarbeitung befassten Mitarbeiter in der zuständigen Beschwerdeabteilung wird bei der Ausübung dieser Funktion eine angemessene Unabhängigkeit zugestanden.

Wenn eine Beschwerde berechtigt ist, ergreift ams OSRAM unverzüglich Maßnahmen, um den Verstoß gegen die Verbindlichen Internen Datenschutzvorschriften zu beenden und die Risiken für die Rechte und Freiheiten der Betroffenen Personen zu mindern. Die Konzern-Datenschutzabteilung oder in bestimmten Fällen der lokale DSK/DSB informiert die Betroffene Person in der schriftlichen/elektronischen Antwort auf die Beschwerde innerhalb der oben genannten Fristen über die Maßnahmen, die zur Beendigung des Verstoßes ergriffen wurden.

Im Falle einer Zurückweisung der Beschwerde, einer Verzögerung bei der Beantwortung innerhalb der in diesem Unterabschnitt festgelegten Fristen oder wenn die Betroffene Person mit der Antwort nicht zufrieden ist, kann sie eine Beschwerde bei der zuständigen Aufsichtsbehörde einreichen oder andere Rechtsmittel bei den zuständigen Gerichten gemäß Unterabschnitt 3.13.1.3 dieser Verbindlichen Internen Datenschutzvorschriften ergreifen. Die Inanspruchnahme eines solchen Rechtsmittels ist unabhängig von der Ausübung des internen Beschwerdeverfahrens von ams OSRAM möglich.

Bei einer Untersuchung sind das Teilnehmende Unternehmen und die Konzern-Datenschutzabteilung dazu verpflichtet, mit den Aufsichtsbehörden des Landes zu kooperieren, die sich mit einer Betroffenenbeschwerde befassen, und deren Beurteilung zu respektieren.

Die ams OSRAM interne Verfahrensweise in Bezug auf Form der Beschwerde, Verarbeitungszeitraum, Schritte nach Annahme und/oder Zurückweisung der Beschwerde und weitere Rechtsmittel werden in einem separaten Beschwerdemanagementkonzept beschrieben.

3.13.7 Überprüfung der Verbindlichen Internen Datenschutzvorschriften

ams OSRAM hat das bestehende interne Prüfungs- und Kontrollsystem um eine Überprüfung der Verbindlichen Internen Datenschutzvorschriften ergänzt, um sicherzustellen, dass die Einhaltung des geforderten, angemessenen Datenschutzniveaus in den Teilnehmenden Unternehmen regelmäßig überprüft wird. Darüber hinaus führt die ams OSRAM Corporate Audit Abteilung im Rahmen ihres risikobasierten Prüfplans regelmäßig Prozessüberprüfungen durch, die die Wirksamkeit und Effizienz der Datenschutzorganisation und -prozesse, einschließlich der Regelungen der Verbindlichen Internen Datenschutzvorschriften, analysiert. Die primäre Verantwortung für die Durchführung der Überprüfungen sowie regelmäßiger und ad-hoc-Überprüfungen der Verbindlichen Internen Datenschutzvorschriften liegt bei der ams OSRAM Corporate Audit Abteilung. Alternativ und bei Bedarf kann die Überprüfung der Verbindlichen Internen Datenschutzvorschriften auch durch einen anerkannten externen Prüfer durchgeführt werden. Die Unabhängigkeit der mit der Überprüfung der Verbindlichen Internen Datenschutzvorschriften betrauten Personen bei der Wahrnehmung ihrer Aufgaben wird gewährleistet.

Einmal jährlich findet in den Teilnehmenden Unternehmen eine Überprüfung der Verbindlichen Internen Datenschutzvorschriften in Form einer Selbsteinschätzung (Ausfüllen eines Online-Fragebogens) statt. Der Leiter der Konzern-Datenschutzabteilung und ams OSRAM Corporate Audit werden über die Ergebnisse informiert.

Unter besonderen Umständen (z. B. Hinweise auf Nichteinhaltung der Verbindlichen Internen Datenschutzvorschriften, Datenschutzvorfälle, Beschwerden von Betroffenen Personen, Defizite, die durch Selbsteinschätzungen zu den Verbindlichen Internen Datenschutzvorschriften aufgedeckt wurden), kann der DSK/DSB, die Konzern-Datenschutzabteilung oder die Abteilung Informationssicherheit (IT SEC) oder eine andere kompetente Abteilung von ams OSRAM zusätzliche ad-hoc-Überprüfungen fordern, die außerhalb des regelmäßigen Prüfungsplans für die Verbindlichen Internen Datenschutzvorschriften liegen.

Die Überprüfung der Verbindlichen Internen Datenschutzvorschriften umfasst alle Aspekte der Verbindlichen Internen Datenschutzvorschriften (z. B. Anwendungen, Datenbanken, IT-Systeme, die Personenbezogene Daten verarbeiten oder deren Weiterübermittlungen, Entscheidungen über die Anforderungen nationaler Gesetze, die mit den Verbindlichen Internen Datenschutzvorschriften im Widerspruch stehen, Überprüfung der Vertragsbedingungen für die Übermittlungen von Daten an Verantwortliche oder Auftragsverarbeiter außerhalb des Konzerns, Korrekturmaßnahmen, usw.) einschließlich Methoden und Aktionspläne, die sicherstellen, dass Korrekturmaßnahmen umgesetzt wurden. Kommt eine Überprüfung zu dem Schluss, dass Korrekturmaßnahmen eingeleitet werden müssen, um einen Verstoß gegen die Verbindlichen Internen Datenschutzvorschriften zu beheben, stellt ams OSRAM Corporate Audit ebenfalls sicher, dass diese notwendigen Korrekturmaßnahmen umgesetzt werden.

Die Ergebnisse der Überprüfung der Verbindlichen Internen Datenschutzvorschriften werden dem DSK/DSB, der Konzern-Datenschutzabteilung, der Geschäftsleitung des jeweils Teilnehmenden Unternehmens und dem Vorstand der ams OSRAM Muttergesellschaft mitgeteilt. Die Ergebnisse der Überprüfung der Verbindlichen Internen Datenschutzvorschriften werden auf Anfrage der zuständigen Aufsichtsbehörde zur Verfügung gestellt. ams OSRAM kann im erforderlichen Umfang Teile der Prüfdaten unkenntlich machen, um vertrauliche Unternehmensinformationen zu schützen.

Die zuständige Aufsichtsbehörde hat das Recht, eine eigene Überprüfung der Verbindlichen Internen Datenschutzvorschriften eines Teilnehmenden Unternehmens durchzuführen. Die Behörde kann diese entweder selbst durchführen oder durch einen anerkannten unabhängigen Prüfer durchführen lassen. Eine offizielle Überprüfung der Verbindlichen Internen Datenschutzvorschriften ist ausschließlich auf deren Einhaltung im Teilnehmenden Unternehmen begrenzt. Einschränkungen aufgrund von Vertraulichkeitsvereinbarungen oder Betriebs- und Geschäftsgeheimnissen werden berücksichtigt.

3.13.8 Aktualisierung der Verbindlichen Internen Datenschutzvorschriften und Change-Management

ams OSRAM behält sich das Recht vor, diese Verbindlichen Internen Datenschutzvorschriften jederzeit zu ändern und/oder zu aktualisieren. Eine Aktualisierung der Verbindlichen Internen Datenschutzvorschriften kann insbesondere infolge veränderter gesetzlicher Anforderungen, erheblicher struktureller Veränderung im ams OSRAM Konzern oder infolge von Auflagen der zuständigen Aufsichtsbehörden notwendig sein.

Grundlegende Änderungen der Verbindlichen Internen Datenschutzvorschriften werden unter Umständen eine erneute Genehmigung durch die zuständigen Aufsichtsbehörden erfordern.

Alle sonstigen Änderungen der Verbindlichen Internen Datenschutzvorschriften sind ohne erneute Genehmigung möglich, vorausgesetzt, dass die Konzern-Datenschutzabteilung ein aktuelles Verzeichnis aller Teilnehmenden Unternehmen führt, eine Übersicht und Dokumentation über die Aktualisierung der Vorschriften hat und auf Anfrage die notwendigen Informationen an die Betroffenen Personen oder Aufsichtsbehörden weitergibt. Die Liste aller Teilnehmenden Unternehmen befindet sich im ams OSRAM Intranet (verlinkt unter https://privacy.ams-osram.com) oder im Anhang I zu den Verbindlichen Internen Datenschutzvorschriften.

Etwaige Änderungen der Verbindlichen Internen Datenschutzvorschriften oder der Liste der Teilnehmenden Unternehmen sind unverzüglich allen an den Verbindlichen Internen Datenschutzvorschriften Teilnehmenden Unternehmen mitzuteilen und einmal jährlich an die zuständige Aufsichtsbehörde zu melden.

Wenn eine Änderung möglicherweise das Schutzniveau der Verbindlichen Internen Datenschutzvorschriften beeinträchtigen oder die Verbindlichen Internen Datenschutzvorschriften erheblich beeinflussen würde (z. B. Änderungen des verbindlichen Charakters, Änderung des/der haftbaren Teilnehmende Unternehmens/Unternehmen), muss sie der zuständigen Aufsichtsbehörde zusammen mit kurzen Erläuterungen der Gründe für die Aktualisierung vorab mitgeteilt werden. In diesem Fall wird die zuständige Aufsichtsbehörde auch beurteilen, ob die vorgenommenen Änderungen einer neuen Genehmigung bedürfen.

Die Konzern-Datenschutzabteilung führt eine Liste aller Änderungen/Aktualisierungen der Verbindlichen Internen Datenschutzvorschriften seit ihrem Inkrafttreten. Sie führt ebenfalls eine regelmäßig aktualisierte Liste aller Teilnehmenden Unternehmen, die effektiv an die Verbindlichen Internen Datenschutzvorschriften gebunden sind (Statusübersicht, vgl. Abschnitt 3.13.1.1). Die entsprechende Liste Teilnehmender Unternehmen befindet sich im ams OSRAM Intranet und im Anhang I zu den Verbindlichen Internen Datenschutzvorschriften.

3.13.9 Gegenseitige Unterstützung und Zusammenarbeit mit Aufsichtsbehörden

Alle Teilnehmenden Unternehmen werden bei Anfragen und Beschwerden von Betroffenen Personen bezüglich einer Nichteinhaltung der Verbindlichen Internen Datenschutzvorschriften vertrauensvoll zusammenarbeiten und sich unterstützen.

Des Weiteren verpflichten sich die Teilnehmenden Unternehmen, uneingeschränkt mit den zuständigen Aufsichtsbehörden zu kooperieren, sich Audits und Inspektionen (auch bei Bedarf vor Ort) zu unterziehen und deren Ratschläge zu berücksichtigen sowie deren Entscheidungen bei allen Fragen im Zusammenhang mit der Auslegung oder Umsetzung der Verbindlichen Internen Datenschutzvorschriften zu befolgen. Sie werden Anfragen der Aufsichtsbehörde dazu innerhalb eines angemessenen Zeitrahmens und in angemessener Weise beantworten und dem Rat und den Entscheidungen der zuständigen Aufsichtsbehörde bezüglich der Umsetzung der Verbindlichen Internen Datenschutzvorschriften folgen.

Die Teilnehmenden Unternehmen stellen der zuständigen Datenschutzbehörde auf Anfrage sämtliche Informationen zu den von den Verbindlichen Internen Datenschutzvorschriften erfassten Verarbeitungstätigkeiten zur Verfügung.

Das Recht, gegen eine Entscheidung der Aufsichtsbehörde Berufung einzulegen, bleibt unberührt. Die Teilnehmenden Unternehmen erkennen an, dass die Gerichte des jeweiligen EWR-Landes der Aufsichtsbehörde hierfür gemäß ihrem jeweiligen Verfahrensrecht zuständig sind. Die Teilnehmenden Unternehmen verpflichten sich, sich der Gerichtsbarkeit dieses Gerichts zu unterwerfen.

3.13.10 Zusammenhänge zwischen den Verbindlichen Internen Datenschutzvorschriften und lokalen gesetzlichen Vorschriften

Die Rechtmäßigkeit der Verarbeitung Personenbezogener Daten wird auf der Grundlage der geltenden lokalen Gesetze beurteilt, denen das Teilnehmende Unternehmen, welches die Daten ursprünglich übermittelt hat, unterliegt. Sofern die geltenden lokalen Gesetze ein höheres Schutzniveau der Personenbezogenen Daten vorsehen als diese Verbindlichen Internen Datenschutzvorschriften, werden die Daten gemäß den geltenden Gesetzen verarbeitet. Jedes Teilnehmende Unternehmen prüft selbst (z. B. durch den DSK/DSB oder die Rechtsabteilung), ob solche lokalen gesetzlichen Bestimmungen vorliegen (z. B. Datenschutzrecht) und stellt deren Einhaltung sicher. Sehen die geltenden lokalen Gesetze ein niedrigeres Schutzniveau der Personenbezogenen Daten vor als diese Verbindlichen Internen Datenschutzvorschriften, werden die vorliegenden Verbindlichen Internen Datenschutzvorschriften angewendet.

3.13.11 Lokale Rechtsvorschriften und Gepflogenheiten, die sich auf die Einhaltung der Verbindlichen Internen Datenschutzvorschriften auswirken

Alle Teilnehmenden Unternehmen weltweit verpflichten sich, nur dann diese Verbindlichen Internen Datenschutzvorschriften als Instrument für einen Datentransfer zu nutzen, wenn sie zu der Einschätzung gelangt sind, dass die Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland, die für die Verarbeitung der Personenbezogenen Daten durch das als Datenimporteur agierende Teilnehmende Unternehmen gelten, einschließlich aller Anforderungen an die Offenlegung Personenbezogener Daten oder Maßnahmen, die den Zugang zu den Daten durch öffentliche Behörden autorisieren, es nicht daran hindern, seinen Verpflichtungen aus diesen Verbindlichen Internen Datenschutzvorschriften nachzukommen.

Diese Bewertung basiert auf der Annahme, dass Gesetze und Gepflogenheiten, welche den Wesensgehalt der Grundrechte und -freiheiten respektieren und nicht über das hinausgehen, was in einer demokratischen Gesellschaft zum Schutz eines der wesentlichen Ziele notwendig und verhältnismäßig ist, nicht im Widerspruch zu den Verbindlichen Internen Datenschutzvorschriften stehen. Diese wesentlichen Ziele sind:

- die nationale Sicherheit;
- die Landesverteidigung;
- die öffentliche Sicherheit;
- die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit;
- den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Europäischen Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Europäischen Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit;
- den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren;

- die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe;
- Kontroll-, Überwachungs- und Regulierungsfunktionen, die dauerhaft oder vorübergehend mit der Ausübung öffentlicher Gewalt zu den oben genannten Zwecken verbunden sind (mit Ausnahme des Schutzes der Unabhängigkeit der Justiz und des Schutzes von Gerichtsverfahren);
- den Schutz der Betroffenen Person oder der Rechte und Freiheiten anderer Personen;
- die Durchsetzung zivilrechtlicher Ansprüche.

Bei der Bewertung der Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes, welche die Einhaltung der in den Verbindlichen Internen Datenschutzvorschriften enthaltenen Verpflichtungen beeinträchtigen könnten, sollen die Teilnehmenden Unternehmen die folgenden Elemente gebührend berücksichtigen:

- Die besonderen Umstände der Übermittlungen oder der Reihe der Übermittlungen sowie aller geplanten Weiterübermittlungen innerhalb desselben Drittlands oder in ein anderes Drittland, einschließlich
    - der Zwecke, zu denen die Daten übermittelt und verarbeitet werden (z. B. Marketing, Personalwesen, Speicherung, IT-Support, klinische Prüfungen);
    - der Arten der an der Verarbeitung beteiligten Stellen (der Datenimporteur und jeder weitere Empfänger einer etwaigen Weiterübermittlung);
    - der Wirtschaftsbranche, in der die Übermittlung oder die Reihe von Übermittlungen erfolgt;
    - der Kategorien und des Formats der übermittelten Personenbezogenen Daten;
    - des Ortes der Verarbeitung, einschließlich der Speicherung; und
    - der verwendeten Übertragungskanäle.
- Die Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlands, die angesichts der Umstände der Übermittlung relevant sind, einschließlich derjenigen, die die Offenlegung von Daten gegenüber Behörden oder die Gewährung des Zugriffs durch diese Behörden verlangen, und derjenigen, die den Zugang zu diesen Daten während des Transits zwischen dem Land des datenexportierenden Unternehmens und dem Land des datenimportierenden Unternehmens gestatten, sowie die damit verbundenen Beschränkungen und Schutzmaßnahmen.
- Alle relevanten vertraglichen, technischen oder organisatorischen Sicherheitsvorkehrungen, die die Schutzmaßnahmen gemäß den Verbindlichen Internen Datenschutzvorschriften ergänzen, einschließlich der Maßnahmen, die bei der Übertragung und Verarbeitung Personenbezogener Daten im Bestimmungsdrittland angewendet werden.

Sollten über die in den Verbindlichen Internen Datenschutzvorschriften festgelegten Sicherheitsvorkehrungen hinaus zusätzliche Schutzmaßnahmen getroffen werden, verpflichtet sich das jeweils Teilnehmende Unternehmen, den ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung, die Konzern-Datenschutzabteilung und ggfs. den lokalen DSB zu informieren und in die Bewertung solcher Maßnahmen einzubeziehen.

Alle Teilnehmenden Unternehmen sind verpflichtet, Bewertungen der Vereinbarkeit der Gesetze und Praktiken im Bestimmungsdrittland mit diesen Verbindlichen Internen Datenschutzvorschriften sowie der implementierten zusätzlichen Schutzmaßnahmen zeitnah zu dokumentieren. Diese Dokumentation ist den zuständigen Aufsichtsbehörden auf Anfrage vorzulegen.

Wenn das Teilnehmende Unternehmen, das als Datenimporteur auftritt, Grund zu der Annahme hat, dass es Rechtsvorschriften oder Gepflogenheiten unterliegt oder unterworfen wurde, die es daran hindern würden, seinen Verpflichtungen im Rahmen der Verbindlichen Internen Datenschutzvorschriften nachzukommen, einschließlich als Folge einer Änderung der gesetzlichen Anforderungen im Bestimmungsdrittland oder einer Maßnahme wie einem Offenlegungsersuchen, benachrichtigt es unverzüglich das Teilnehmende Unternehmen, das als Datenexporteur agiert. Diese Informationen werden auch an den ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung und an die Konzern-Datenschutzabteilung übermittelt.

Nach Prüfung einer solchen Meldung wird das als Datenexporteur fungierende Teilnehmende Unternehmen gemeinsam mit dem ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung, der Konzern-Datenschutzabteilung und ggfs. dem lokalen DSB umgehend ergänzende Maßnahmen festlegen, die vom Datenexporteur und/oder Datenimporteur umzusetzen sind, um die Einhaltung dieser Verbindlichen Internen Datenschutzvorschriften sicherzustellen. Gleiches gilt für den Fall, in dem das Teilnehmende Unternehmen, das als Datenimporteur auftritt, Grund zu der Annahme hat, dass das datenimportierende Teilnehmende Unternehmen seinen Verpflichtungen aus den Verbindlichen Internen Datenschutzvorschriften nicht mehr nachkommen kann.

Gelangt das beteiligte Unternehmen, das als Datenexporteur fungiert, gemeinsam mit dem ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung, der Konzern-Datenschutzabteilung und ggfs. dem lokalen DSB nach Prüfung der Meldung zur Einschätzung, dass die Verbindlichen Internen Datenschutzvorschriften – selbst in Verbindung mit den ergänzenden Maßnahmen – bei einer Übermittlung oder einer Reihe von Übermittlungen nicht eingehalten werden können, oder falls es von der zuständigen Aufsichtsbehörde dazu angewiesen wird, setzt das beteiligte Unternehmen die betreffende Übermittlung oder Reihe von Übermittlungen sowie alle Übermittlungen, bei denen dieselbe Bewertung und Begründung zu einem ähnlichen Ergebnis führen würde, aus, bis die Einhaltung wieder gewährleistet ist oder die Übermittlung beendet ist.

Die Übermittlung oder eine Reihe der Übermittlungen müssen von dem als Datenexporteur handelnden Teilnehmenden Unternehmen beendet werden, wenn die Verbindlichen Internen Datenschutzvorschriften nicht eingehalten werden können oder die Einhaltung der Verbindlichen Internen Datenschutzvorschriften nicht innerhalb eines (1) Monats nach der Aussetzung wiederhergestellt werden kann. In diesem Fall müssen die vor der Aussetzung übermittelten Personenbezogenen Daten oder etwaige Kopien davon an das als Datenexporteur fungierende Teilnehmende Unternehmen zurückgegeben oder vernichtet werden.

Die Konzern-Datenschutzabteilung verpflichtet sich, die Beurteilung der Rechtsvorschriften und Gepflogenheiten im Bestimmungsdrittland sowie die Ergebnisse dieser Beurteilungen allen beteiligten Unternehmen umgehend mitzuteilen, um sicherzustellen, dass die ermittelten ergänzenden Maßnahmen auf alle ähnlichen Übermittlungen angewendet werden oder, sofern keine wirksamen ergänzenden Maßnahmen umgesetzt werden können, die fraglichen Übermittlungen ausgesetzt oder eingestellt werden.

Alle beteiligten Unternehmen, die sowohl als Datenexporteure als auch als Datenimporteure handeln, verpflichten sich, die Entwicklungen in Drittländern, in die Personenbezogene Daten übermittelt werden, die sich auf die ursprüngliche Beurteilung des Datenschutzniveaus und die Gültigkeit der im Zusammenhang mit einer solchen Übermittlung oder Übermittlungen getroffenen Entscheidungen auswirken könnten, fortlaufend zu beobachten.

3.13.12 Pflichten des Datenimporteurs bei Auskunftsersuchen staatlicher Stellen

Im Falle eines Auskunfts-/Zugriffsersuchen staatlicher Stellen gilt Folgendes:

- Das Teilnehmende Unternehmen, das als Datenimporteur auftritt, verpflichtet sich, das datenexportierende Teilnehmende Unternehmen und die Konzern-

Datenschutzabteilung sowie auch, soweit möglich und wenn nötig mithilfe des Datenexporteurs, die Betroffene Person unverzüglich zu informieren, wenn es:

- ein Ersuchen einer öffentlichen Behörde des Bestimmungslandes oder eines anderen Drittlandes zur Offenlegung von im Rahmen der Verbindlichen Internen Datenschutzvorschriften übermittelten Daten erhält, das rechtlich verbindlich ist. Eine solche Benachrichtigung soll Einzelheiten zu den angefragten Personenbezogenen Daten, zur Rechtsgrundlage für das Ersuchen und die übermittelte Antwort enthalten.
- Kenntnis von einem direkten Zugriff auf Personenbezogene Daten, die im Rahmen der Verbindlichen Internen Datenschutzvorschriften übermittelt werden, durch öffentliche Behörden nach dem Recht des Bestimmungsdrittlandes erlangt. Eine solche Benachrichtigung enthält alle dem Datenimporteur zur Verfügung stehenden Informationen.

- Wenn eine Benachrichtigung des datenexportierenden Teilnehmenden Unternehmens, der Konzern-Datenschutzabteilung oder der Betroffenen Person untersagt ist, bemüht sich das datenimportierende Teilnehmende Unternehmen nach besten Kräften um eine Aufhebung dieses Verbots, um möglichst schnell möglichst viele Daten bereitstellen zu können und dokumentiert diese Bemühungen, damit sie dem Datenexporteur auf Anfrage nachgewiesen werden können.
- Das datenimportierende Teilnehmende Unternehmen stellt dem Teilnehmenden Unternehmen, das als Datenexporteur fungiert, sowie der Konzern-Datenschutzabteilung in regelmäßigen Abständen so viele Informationen wie möglich über die eingegangenen Ersuchen zur Verfügung. Zu diesen Informationen gehören beispielsweise Angaben zur Anzahl der Ersuchen, zur Art der angeforderten Daten, zur ersuchenden Behörde oder zu den Behörden, Informationen darüber, ob Ersuchen angefochten wurden und das Ergebnis solcher Anfechtungen. Wird dem datenimportierenden Teilnehmenden Unternehmen die Bereitstellung dieser Informationen an den Datenexporteur teilweise oder vollständig untersagt, benachrichtigt es den Datenexporteur sowie die Konzern-Datenschutzabteilung unverzüglich darüber. Der Datenimporteur auch dokumentiert und bewahrt diese Informationen, solange die fraglichen Personenbezogenen Daten den Garantien der Verbindlichen Internen Datenschutzvorschriften unterliegen, und stellt sie der zuständigen Aufsichtsbehörde auf Anfrage zur Verfügung.
- Das datenimportierende Teilnehmende Unternehmen überprüft die Rechtmäßigkeit jedes Offenlegungsersuchens, insbesondere im Hinblick auf die der ersuchenden Behörde oder Behörden übertragenen Befugnisse, und widerspricht dem Ersuchen, wenn es bei der Überprüfung zu dem Schluss kommt, dass das Ersuchen nach den Gesetzen des Bestimmungslandes, gemäß geltenden völkerrechtlichen Verpflichtungen und nach den Grundsätzen der Völkercourtoisie rechtswidrig ist. In diesem Zusammenhang versucht das datenimportierende Teilnehmende Unternehmen, gegen das Ersuchen mögliche Rechtsmittel einzulegen. Während der Anfechtung des Ersuchens bemüht sich der Datenimporteur um die Umsetzung einstweiliger Maßnahmen, die darauf abzielen, die Wirkungen des Ersuchens auszusetzen, bis die zuständige Justizbehörde über dessen Begründetheit entschieden hat. In diesem Fall werden keine Informationen weitergegeben, bis der Datenimporteur gemäß den geltenden Verfahrensregeln dazu verpflichtet ist.
- Das datenimportierende Teilnehmende Unternehmen dokumentiert seine rechtliche Bewertung eingehender Auskunftsersuchen und etwaiger Anfechtungen solcher Ersuchen und übermittelt diese Informationen, sofern dies nach dem Recht des Bestimmungslandes angemessen ist, an den Datenexporteur und an die Konzern-Datenschutzabteilung. Auf Anfrage stellt es diese Informationen auch der zuständigen Aufsichtsbehörde zur Verfügung.

- Das datenimportierende Teilnehmende Unternehmen soll bei der Beantwortung eines Offenlegungsersuchens so wenige Informationen bereitstellen, wie dies nach vernünftiger Beurteilung des betreffenden Ersuchens zulässig ist.

Das Teilnehmende Unternehmen stellt sicher, dass die Übermittlung Personenbezogener Daten an öffentliche Behörden nicht auf eine Weise umfangreich, unverhältnismäßig und unterschiedslos erfolgt, die über das in einer demokratischen Gesellschaft Notwendige hinausgeht.

3.14 Nichteinhaltung der Verbindlichen Internen Datenschutzvorschriften

Die beteiligten Unternehmen verpflichten sich zu Folgendem:

- Eine Übermittlung Personenbezogener Daten an ein Teilnehmendes Unternehmen erfolgt nur dann, wenn ein Teilnehmendes Unternehmen tatsächlich an die Verbindlichen Internen Datenschutzvorschriften gebunden ist und die Einhaltung der Verbindlichen Internen Datenschutzvorschriften sichergestellt werden kann.
- Wenn ein datenimportierendes Teilnehmendes Unternehmen aus irgendeinem Grund nicht in der Lage ist, die Verbindlichen Internen Datenschutzvorschriften einzuhalten, informiert es das datenexportierende Teilnehmende Unternehmen und die Konzern-Datenschutzabteilung unverzüglich darüber.
- Verstößt ein datenimportierendes Teilnehmendes Unternehmen gegen die Verpflichtungen aus den Verbindlichen Internen Datenschutzvorschriften oder ist es nicht möglich, den Verpflichtungen aus den Verbindlichen Internen Datenschutzvorschriften nachzukommen, ist das datenexportierende Teilnehmende Unternehmen verpflichtet, die Übermittlung auszusetzen.
- Das datenimportierende Teilnehmende Unternehmen hat die im Rahmen der Verbindlichen Internen Datenschutzvorschriften übermittelten Daten nach Wahl des datenexportierenden Teilnehmenden Unternehmens unverzüglich vollständig zurückzugeben oder zu löschen. Dies gilt auch für sämtliche Kopien der Personenbezogenen Daten. Bis zur Rückgabe oder Löschung der Daten ist die Einhaltung der Verbindlichen Internen Datenschutzvorschriften sicherzustellen. Ist dem datenimportierenden Teilnehmenden Unternehmen die Rückgabe oder Löschung nach geltendem Recht untersagt, so hat es die Verbindlichen Internen Datenschutzvorschriften weiterhin einzuhalten und die Daten nur insoweit zu verarbeiten, als dies nach dem für es geltenden Recht vorgesehen ist. Die Löschung der Daten ist dem datenexportierenden Teilnehmenden Unternehmen zu bescheinigen. Die Verpflichtungen in diesem Absatz gelten nur in folgenden Fällen:
    - Das datenexportierende Teilnehmende Unternehmen hat die Übermittlung von Daten ausgesetzt und die Einhaltung der Verbindlichen Internen Datenschutzvorschriften wird nicht innerhalb einer angemessenen Frist und in jedem Fall innerhalb eines Monats nach der Aussetzung wiederhergestellt.
    - Das datenimportierende Teilnehmende Unternehmen verstößt erheblich oder/und dauerhaft gegen die Verbindlichen Internen Datenschutzvorschriften.
    - Das datenimportierende Teilnehmende Unternehmen kommt einer verbindlichen Entscheidung eines zuständigen Gerichts oder einer Datenschutzbehörde bezüglich seiner Verpflichtungen aus den verbindlichen internen Datenschutzvorschriften nicht nach.

3.15 Haftung

Jedes Teilnehmende Unternehmen haftet für seine Verstöße gegen die Verbindlichen Internen Datenschutzvorschriften.

Zusätzlich übernimmt der ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung die Haftung für die Nichteinhaltung der Verbindlichen Internen Datenschutzvorschriften von Teilnehmenden Unternehmen, die ihren Sitz außerhalb des EWR haben, einschließlich der Schadensersatzpflicht bei nachgewiesenem Verstoß gegen die Verbindlichen Internen Datenschutzvorschriften und einer daraus folgenden Verletzung der Rechte der Betroffenen Person, die durch diese Nichteinhaltung verursacht wurde. Er sagt weiterhin zu, die erforderlichen Maßnahmen zu ergreifen, um die Verstöße des außerhalb des EWR ansässigen Teilnehmenden Unternehmens gegen die Verbindlichen Internen Datenschutzvorschriften abzustellen.

Die Beweislast liegt beim ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung. Dieser wird beweisen, dass kein Verstoß gegen die Verbindlichen Internen Datenschutzvorschriften stattgefunden hat oder dass das außerhalb des EWR ansässige Teilnehmende Unternehmen nicht für den Verstoß haftbar ist, auf dem die Schadensersatzforderung der Betroffenen Person beruht.

Wenn der ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung nachweisen kann, dass das außerhalb des EWR ansässige Teilnehmende Unternehmen nicht für die Verletzung der Verbindlichen Internen Datenschutzvorschriften haftbar ist, kann er sich von jeglicher Verantwortung entlasten.

3.16 Kontakt

Betroffene Personen können sich mit ihren Anliegen an den DSK/DSB des jeweiligen Teilnehmenden Unternehmens wenden oder an die Konzern-Datenschutzabteilung:

OSRAM GmbH
Corporate Data Privacy Department
Marcel-Breuer-Str. 4
D-80807 München
E-Mail: privacy@ams-osram.com
Internet: https://www.ams-osram.com

Versionsverlauf

Version	Autor	Datum
Erstveröffentlichung, 1.0	Stefan Gassner	18 Mai 2021
Überarbeitung, Ergänzungen und Korrekturen, 1.1: - Anpassung an die „ams OSRAM“ Unternehmensgruppe; - Ergänzung nach Schrems II Rechtsprechung; - Anpassung der Bestimmungen bezüglich des BCR-Audits an die aktuelle Vorgehensweise.	Stefan Gassner	22 November 2022
Überarbeitung, Klarstellungen und Ergänzungen, 1.2: - Anapassung an die Empfehlungen 1/2022 vom EDSA zum Antrag auf Genehmigung und zu den Bestandteilen und Grundsätzen, die in verbindlichen internen Datenschutzvorschriften; - Änderung der Nummerierung.	Stefan Gassner	01 Dezember 2024
Ergänzungen (Versionsverlauf), 1.3.	Stefan Gassner	12 Mai 2025
Ergänzungen (Anpassung der Liste der beteiligten Einheiten), 1.4.	Stefan Gassner	09 Dezember 2025

Anhang I zu den Verbindlichen Internen Datenschutzvorschriften

Liste Teilnehmender ams OSRAM Unternehmen und deren Kontaktdaten (Stand: 09.12.2025):

Bezeichnung	Kontaktinformationen
OSRAM GmbH	Marcel-Breuer-Straße 4, 80807 München, Deutschland
ams-OSRAM AG	Tobelbader Straße 30, 8141 Premstätten, Österreich
ams Italy S.r.l.	Via Mauro Macchi n. 27, 20124 Mailand, Italien
ams R&D UK Limited	Trevean, Yeolmbridge, PL15 8NJ Launceston, Vereinigtes Königreich
ams R&D Spain S.L.	MNO de Vera s/n - Ciudad Politécnica de la Innovación Edificio 9E, Planta 1, Lado Este, 46022 Valencia, Spanien
ams International AG	Eichwiesstrasse 18b, 8645 Jona, Schweiz
ams Sensors Germany GmbH	Göschwitzer Str. 32, 7745 Jena, Deutschland
ams Offer GmbH	Marcel-Breuer-Strasse 4, 80807 München, Deutschland
ams Sensors Netherlands BV	High Tech Campus 41, 5656AE Eindhoven, Niederlande
ams Sensors Belgium BV	Borsbeeksebrug 22, 2600 Antwerpen, Belgien
ams Sensors Portugal	Caminho da Penteada Madeira Tecnopolo 2. andar District Island of Madeira Municipality Funchal Parish Sao Roque, 9020 105 Funchal, Portugal
ams-OSRAM International GmbH	Leibnizstrasse 4, 93055 Regensburg, Deutschland
ams Semiconductors India Pvt. Ltd.	5th Floor, C Block, iLabs, Plot No.18, 500081 Madhapur Hyderabad, Indien
ams Asia Inc.	Carmelray Industrial Park II, No. 2 Makiling Drive CIP II, Brgy. Milagrosa, 4027 Calamba City, Philippinen
OSRAM Opto Semiconductors (China) Co. Ltd.	57, Xi Qing Road, 214000 Wuxi New District, China
ams-OSRAM USA Inc.	651 River Oaks Parkway, 95134 San Jose, USA
OSRAM SYLVANIA INC.	275 W Main St., NH 03244-5233 Hillsboro, USA
OSRAM Ceská republika s.r.o.	Zahradni 46, 792 01 Bruntál, Tschechische Republik
P.T. OSRAM Indonesia	JB Tower Lantai 10, Jalan Kebon Sirih No. 48-50, Gambir, Jakarta Pusat, 10110 Jakarta, Indonesien
OSRAM (Malaysia) Sdn. Bhd.	Lot PT207, Level 4, Uptown 7, Jalan SS 21/39, Damansara Utama, 47400 Petaling Jaya (Selangor), Malaysia
ams-OSRAM Asia Pacific Pte. Ltd.	7000 Ang Mo Kio Avenue 5, #03-00, 569877 Singapur, Singapur
OSRAM Kunshan Display Optic Co. Ltd.	No. 2 Building, No. 179 Waihejing Road, Free Trade Zone, Kunshan Development Zone, 215300 Kunshan, China
ams-OSRAM Japan Ltd.	OSAKI WIZ TOWER 20F, 2-11-1, Osaki, Shinagawa-ku, 141-0032 Tokyo, Japan
ams-OSRAM Korea Ltd.	39 Fl., FKI Tower, 24 Yeoui-Daero, Yeongdeungpo-Gu., 07320 Seoul, Republik Korea
ams-OSRAM Taiwan Ltd.	7F, No. 87 Songjiang Road, Zhongshan District, 10486 Taipei, Taiwan
OSRAM Opto Semiconductors Trading (Wuxi) Co. Ltd.	#1 Xi Qin road, Room 203, Floor 2, 214000 Wuxi, China
Vixar Inc.	2950 Xenium Lane, Suite 104, 55441 Plymouth, USA
OSRAM Comercio de	AV Marcos Penteado De Ulhoa Rodrigues 939, 06460-040 Barueri,

Solucoes de Ilumina-cao Ltda.	Brasilien
OSRAM (Thailand) Co. Ltd.	57 Park Ventures Ecoplex, Level 18, Unit 1809, Wireless Road, Kwaeng Lumpini, Khet Pathumwan, 10330 Bangkok, Thailand
OSRAM S.p.A. - Società Riunite OSRAM Edison Clerici	Via Sant'Uguzzone 29, 20126 Mailand, Italien
OSRAM Asia Pacific Management Company Ltd.	No. 1-3, North Industrial Road, Zumiao Subdistrict, Chancheng District, Foshan, China
OSRAM d.o.o.	Visnjevac 3, 10000 Zagreb, Kroatien
Ring Automotive Limited	Volvox House, Gelderd Road, LS12 6NA Leeds, Vereinigtes Königreich
OSRAM a.s. Zweigniederlassung Österreich	Dresdner Straße 60/PF 344, 1200 Vienna, Österreich
OSRAM a.s. Hungarian Branch Office	Fehervari ut 84/A, 1119 Budapest, Ungarn
OSRAM Sales EOOD	Slatina district, Shipchenski Prohod No 9, fl. 4, ap. 9A, 1111 Sofia, Bulgarien
OSRAM AB	Arenavägen 39, 12178 Stockholm, Schweden
OSRAM a.s.	Komárnanská cesta 7, 940 93 Nové Zámky, Slowakei
OSRAM Romania S.R.L.	24 Italiana Street, Ground floor, 2nd District, Bucharest, Rumänien
OSRAM Oy	Vantaankoskentie 14, 1670 Vantaa, Finnland
OSRAM Lighting S.A.S.U.	18, rue Gaston Romazzotti, 67120 Molsheim, Frankreich
OSRAM Asia Pacific Ltd.	208 Wireless Centre 3 Science Park East Avenue, Science Park, Shatin New Territories, Hong Kong, China
OSRAM Limited	450 Brook Drive, Green Park, Reading, Berkshire, RG2 6UU, Vereinigtes Königreich
OSRAM AS	Lysaker Torg 12, 1366 Lysaker, Norwegen
OSRAM Benelux B.V.	Marten Meesweg 8, 3068AV Rotterdam, Niederlande
OSRAM Lda.	Rua do Alto do Montijo, n° 15, 2790-213 Carnaxide, Portugal
OSRAM Lighting AG	Eichwiesstrasse 18b, 8645 Jona, Schweiz
OSRAM Lighting S.L.	Avda. Leonardo da Vinci,15-17-19, Getafe, 28906 Madrid, Spanien
OSRAM A/S	Dybendalsvænget 3, Klovtofte, 2630 Taastrup, Dänemark
OSRAM Sp. z o.o.	Aleje Jerozolimskie 94, 00-807 Warschau, Polen
OSRAM Lighting Middle East FZE	Office No. 208 – 209, "E" Wing, Dubai Silicon Oasis (DSO), Mohammed Bin Zayed Road, Dubai, Vereinigte Arabische Emirate
OSRAM Teknolojileri Ticaret Anonim Sirketi	Merdivenköy Mah. Dikyol Sokak Business Istanbul / B Blok Bölüm 124, 34394 Istanbul, Türkei
OSRAM China Lighting Ltd.	No. 1 North Industrial Road, 528000 Foshan, China
OSRAM Licht AG	Marcel-Breuer-Straße 4, 80807 München, Deutschland
OSRAM Lighting Pte. Ltd.	7000 Ang Mo Kio Avenue 5, #05-00, 569877 Singapur, Singapur
OSRAM Beteiligungen GmbH	Marcel-Breuer-Str. 4, 80807 München, Deutschland
OSRAM Lighting (Pty) Ltd.	Emerald Park Block 2, 22 Reedbuck Crescent, Corporate Park South, 1685 Midrand, Südafrika
OSRAM Lighting Private Limited	1st Floor, IFFCO Surinder Jhakhar Bhavan Plot No. 3, Sector 32, 122 001 Gurgaon, Indien
OSRAM Co. Ltd.	39 Fl., FKI Tower, 24 Yeoui-Daero, Yeongdeungpo-Gu., 07320 Seoul, Republik Korea
OSRAM S.A. de C.V.	Avenida 1o de Mayo # 120, Piso 5o Oficina 502, 53500 Naucalpan,

	Mexiko
Light Distribution GmbH	An der Bahnbrücke, 89542 Herbrechtingen, Deutschland
OSRAM Ltd.	OSAKI WIZ TOWER 20F, 2-11-1, Osaki, Shinagawa-ku, 141-0032 Tokyo, Japan
Osram Opto Semiconductors (Malaysia) Sdn Bhd	Bayan Lepas, Free Industrial Zone Phase 1, 11900 Penang, Malaysia
OSRAM Taiwan Company Ltd.	7F, No. 87 Songjiang Road, Zhongshan District, 104 Taipei, Taiwan
AMS-OSRAM SENSORS S.R.L.	Str. Jean Louis Calderon Nr.70, Floor 3, District 2, Bucharest, Rumänien
OSRAM Lighting Ltd.	55 Renfrew Drive, Suite 201, L3R 8H3 Markham, Kanada
ams-OSRAM France	4 Rue Piroux, 54000 Nancy, Frankreich
OSRAM Opto Semiconductors Asia Ltd.	Room 303, 3rd Floor, ST. George's Building, 2 ICE House Street Central, Hong Kong, China
Representative office of OSRAM GmbH in the Republic of Kazakhstan	Hadji Mukana 22/5, Medeusky District, 50020 Almaty, Kasachstan
Representative office of OSRAM GmbH in Ukraine	30 V Fizkultury Str., Office 201, Golosiiwsky Raion, 03680 Kiew, Ukraine