Anhang zu Unternehmensrichtlinie CO3000

Verbindliche interne Datenschutzvorschriften

Inhalt

ams OSRAM

Verbindliche interne Datenschutzvorschriften für ams OSRAM Konzerngesellschaften und beitretende Unternehmen zum Schutz personenbezogener Daten

Begriffe

- **Beitretendes Unternehmen** ein mit ams OSRAM verbundenes Unternehmen in Deutschland oder im Ausland, an dem die Konzernmuttergesellschaft von ams OSRAM oder ein verbundenes Unternehmen eine Minderheitsbeteiligung hält und das sich mit Zustimmung des ams OSRAM Co-Hauptsitzes mit Datenschutzverantwortung freiwillig verpflichtet hat, durch Abschluss des Intercompany Agreement die Vorschriften der verbindlichen internen Datenschutzvorschriften einzuhalten;

- **Verbindliche interne Datenschutzvorschriften** die aktuellen verbindlichen internen Datenschutzvorschriften und die darin enthaltenen Bestimmungen;

- **Einwilligung** 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];

- **Verantwortlicher** die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Datenverarbeitung entscheidet;

- Die **Konzern-Datenschutzabteilung (Corporate Data Privacy Department)** die zentrale Abteilung von ams OSRAM, die nach dem aktuellen Organigramm für den konzernweiten Datenschutz verantwortlich ist;

- **Kunden und Lieferanten** natürliche und juristische Personen, mit denen eine Geschäftsbeziehung besteht oder geplant ist;

- **Betroffene Person** 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; juristischen 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);

- **Datenschutzkoordinator (DSK)**, d. h. die Person, die von einem teilnehmenden Unternehmen als verantwortlich für die lokale Umsetzung und Einhaltung der verbindlichen internen Datenschutzvorschriften sowie die Unterstützung des CDPD ernannt wurde;

- **Data Protection Executive (DPE)** einer ams OSRAM Konzerngesellschaft; diese Funktion wird vom CEO 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;

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

- **Land/Länder des EWR** die Mitgliedsstaaten der Europäischen Union (EU) und die anderen Unterzeichner des Abkommens über den Europäischen Wirtschaftsraum (EWR);

- **Datenschutz-Grundverordnung** die Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr;

- **Konzerngesellschaft oder ams OSRAM Konzerngesellschaft** sind deutsche oder ausländische Gesellschaften des ams OSRAM Konzerns und Gesellschaften, an denen die ams OSRAM Konzernmuttergesellschaft direkt oder indirekt eine Mehrheitsbeteiligung hält oder die Mehrheit der Stimmrechte kontrolliert;

- **Intercompany Agreement (ICA),** durch den sich die beitretende ams OSRAM Konzerngesellschaft verpflichtet, die Bestimmungen der verbindlichen internen Datenschutzvorschriften einzuhalten

- **ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung** OSRAM GmbH;

- **ams OSRAM Muttergesellschaft** ams AG;

- **Teilnehmendes Unternehmen** ist eine ams OSRAM Konzerngesellschaft oder ein beitretendes Unternehmen, das dem ICA beitritt und sich damit verpflichtet, die Bestimmungen dieser verbindlichen internen Datenschutzvorschriften einzuhalten;

- **Personenbezogene Daten** sind alle Informationen, die sich auf eine betroffene Person beziehen;

- **Verletzung des Schutzes personenbezogener Daten** 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;

- **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;

- **Auftragsverarbeiter** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

- **Besondere Kategorien personenbezogener Daten** sind Informationen, aus denen rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische und biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung;

- **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 2c) der Datenschutz-Grundverordnung erlassen werden.

- **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;

Zusammenfassung der verbindlichen internen Datenschutzvorschriften von ams OSRAM

Das Primäres Ziel 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.

Zu diesem Zweck ist die Schaffung harmonisierter Datenschutz- und Datensicherheitsstandards für die Verarbeitung der personenbezogenen Daten im Sinne der Datenschutz-Grundverordnung wesentlich, sodass damit – im Hinblick auf die personenbezogenen Daten im Anwendungsbereich dieser verbindlichen internen Datenschutzvorschriften – im Sinne der Datenschutz-Grundverordnung bezüglich des Schutzes der Privatsphäre und der Ausübung der damit verbundenen Rechte ein angemessenes Datenschutzniveau und geeignete Garantien gewährleistet wird.

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 durch ams OSRAM Konzerngesellschaften oder beitretende Unternehmen im Anwendungsbereich dieser Datenschutzvorschriften. 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 EU-Datenschutzgruppe nach Artikel 29 und des Europäischen Datenschutzausschusses und der Grundsätze zum Schutz der Privatsphäre der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre (im Folgenden „Entschließung von Madrid“) vom 5. November 2009.

1. Inhalt der Richtlinie

1.1 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 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).

1.2 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 die Entschließung von Madrid vom 5. November 2009 sollte berücksichtigt werden, wenn personenbezogene Daten durch teilnehmende Unternehmen im Anwendungsbereich dieser verbindlichen internen Datenschutzvorschriften verarbeitet werden:

1.2.1 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 Datenverarbeitung ist für die Erfüllung eines Vertrags erforderlich, bei dem die betroffene Person eine Vertragspartei ist oder um auf Verlangen der betroffenen Person vor Vertragsabschluss Schritte zu unternehmen; 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.

1.2.2 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.

1.2.3 Transparenz

Alle teilnehmenden Unternehmen verarbeiten die personenbezogenen Daten auf transparente Weise. Betroffene Personen, deren Daten von einem teilnehmenden Unternehmen verarbeitet werden erhalten gemäß Artikel 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 Möglichkeit, wie eine Kopie der Vorkehrungen zu erhalten ist, oder 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 Bestehen eines Rechts, 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 Bestehen eines Rechts, 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 mögliche Folgen die Nichtbereitstellung hätte;
- das Vorhandensein einer automatisierten Entscheidungsfindung – einschließlich Profiling – und, zumindest in diesen Fällen, aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person;
- aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen (sofern die personenbezogenen Daten nicht direkt von der betroffenen Person erhoben wurden).

Diese verbindlichen internen Datenschutzvorschriften werden allen betroffenen Personen, die die in Unterabschnitt 1.2.18.1.3 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.

1.2.4 Datenqualität, Datenminimierung und begrenzte Speicherung

Personenbezogene Daten müssen sachlich korrekt sein und – falls notwendig – 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 vom Grundsatz der Datensparsamkeit geleitet zu sein. Es ist das Ziel, nur die erforderlichen personenbezogenen 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 steht. 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. Wenn gesetzliche Aufbewahrungsfristen gelten, ist die Verarbeitung der betroffenen Daten eingeschränkt.

1.2.5 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, durch den Datenimporteur an einen externen Verantwortlichen oder Auftragsverarbeiter außerhalb der ams OSRAM Gruppe 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).

1.2.6 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 der 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, Leistungen der Gesundheits- oder Sozialfürsorge oder für Behandlungen oder für die Verwaltung des Gesundheits- oder Sozialwesens und der Leistungen aufgrund geltender lokaler Gesetze oder aufgrund 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.

1.2.7 Automatisierte Entscheidungen im Einzelfall

Wenn personenbezogene Daten zum Zweck der automatisierten Entscheidung im Einzelfall 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 benachteiligen, dürfen nicht ausschließlich aufgrund eines automatisierten Einzelverfahrens getroffen werden, welches die persönlichen Eigenschaften der Person bewerten soll, d. h., Entscheidungen dürfen nicht ausschließlich auf der Nutzung von Informationstechnologie beruhen. 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. wenn die betroffene Person Informationen über die Logik erhält, wie eine solche Entscheidung zustande kommt, sowie die Möglichkeit zur Prüfung und Stellungnahme hat. Falls die betroffene Person eine Stellungnahme einreicht, muss der Verantwortliche seine Entscheidung überprüfen; oder

- sie durch geltendes lokales Gesetz zulässig ist; oder

- die Entscheidung auf der ausdrücklichen Einwilligung der betroffenen Person beruht.

1.2.8. Verzeichnis von Verarbeitungstätigkeiten

Alle teilnehmenden Unternehmen müssen ein Verzeichnis der Verarbeitungstätigkeiten, die im betreffenden Unternehmen ausgeführt werden, dokumentieren und führen. Jeder DSK oder DSB ist verantwortlich dafür, dass das Verzeichnis der Verarbeitungstätigkeiten regelmäßig dokumentiert und geprüft 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.

1.2.9. Datenschutz-Folgenabschätzung

Hat Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge, so führen die teilnehmenden Unternehmen eine Abschätzung der Folgen 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 Abschätzung müssen beachtet werden.

Legt eine Datenschutz-Folgenabschätzung nahe, dass die Verarbeitung zu einem hohen Risiko führen würde, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, darf der Verantwortliche nicht mit der Verarbeitung beginnen oder diese weiterführen, sondern muss gemäß Artikel 36 der Datenschutz-Grundverordnung die zuständige Aufsichtsbehörde konsultieren.

1.2.10 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 sind gleichzeitig bestrebt, sich am Stand der Technik im Bereich Datensicherheit zu 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 (Richtlinie IT3), welches für die gesamte ams OSRAM Gruppe bindend ist. Die aktuelle Version der Richtlinie sowie die dazugehörigen Dokumente befinden sich im Corporate Process House 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 -leistungen;

- 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.

1.2.11 Vertraulichkeit der Datenverarbeitung

Nur Personal der teilnehmenden Unternehmen, das berechtigt ist und eine besondere Einweisung in 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. Zu den unbefugten Personen zählen in diesem Zusammenhang beispielsweise andere Mitarbeiter insoweit, als sie die personenbezogenen Daten nicht benötigen, um ihre besonderen Aufgaben zu erfüllen. Die Verpflichtung zur Vertraulichkeit besteht auch über das Ende des Beschäftigungsverhältnisses mit dem entsprechenden Mitarbeiter weiter.

1.2.12 Meldung 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.

Die Konzern-Datenschutzabteilung wird die Art der Datenschutzverletzung und Kategorie der betroffenen Daten/Personen sowie die Folgen für die Rechte und Freiheiten der betroffenen Personen bewerten und festlegen, ob die betreffende Datenschutzverletzung wahrscheinlich zu einem (hohen) Risiko für die Rechte und Freiheiten natürlicher Personen führt.

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 werden und den betreffenden Behörden auf Verlangen vorgelegt werden.

1.2.13 „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 Technikgestaltung (by design) und datenschutzfreundliche Voreinstellungen (by default) gerecht zu werden.

Zu diesem Zweck verabschieden die teilnehmenden Unternehmen interne Richtlinien und setzen Maßnahmen um, die unter anderem eine Minimierung der Verarbeitung und schnellstmögliche Pseudonymisierung personenbezogener Daten zum Ziel haben sowie der betroffenen Person die Überwachung der Datenverarbeitung und dem Verantwortlichen die Entwicklung und Verbesserung von Sicherheitsfunktionen 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 für (i) die Menge der erhobenen personenbezogenen Daten, (ii) den Umfang ihrer Verarbeitung, (iii) die Dauer der Speicherung und (iv) die Zugriffsmöglichkeiten.

1.2.14 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 vertraglichen Rahmen und entsprechend der dokumentierten Anweisungen des Verantwortlichen zu verarbeiten. Die Verarbeitung von Daten für eigene Zwecke des Auftragsverarbeiters oder für Dritte wird vertraglich untersagt, sofern die Verarbeitung nicht durch lokal geltende Gesetze vorgeschrieben ist; in diesem Fall informiert der Auftragsverarbeiter den Verantwortlichen vor der Verarbeitung im lokal geltenden gesetzlichen Umfang über diese gesetzliche Vorschrift;

- 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 besondere oder allgemeine schriftliche Genehmigung keinen anderen 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 die Gelegenheit, gegen diese Änderungen Einspruch zu erheben. Der ursprüngliche Auftragsverarbeiter bleibt gegenüber dem Verantwortlichen vollständig haftbar für die Pflichterfüllung des Unterauftragsverarbeiters und dessen Einhaltung der Bestimmungen der Datenschutz-Grundverordnung und anderer anwendbarer Datenschutzbestimmungen;

- Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen durch geeignete technische und organisatorische Maßnahmen soweit dies möglich ist, damit der Verantwortliche seine Verpflichtung zur Beantwortung von Anfragen der betroffenen Personen erfüllen kann;

- Unter Berücksichtigung der Art der Verarbeitung und der Informationen, die dem Auftragsverarbeiter zur Verfügung stehen, unterstützt Letzterer den Verantwortlichen bei der Umsetzung geeigneter technischer und organisatorischer Maßnahmen, er informiert den Verantwortlichen umgehend über alle Datenschutzverletzungen und stellt die Informationen zur Verfügung, die für die Meldung der Datenschutzverletzung an Aufsichtsbehörden und/oder betroffene Personen erforderlich sind und er unterstützt den Verantwortlichen anderweitig, um die Einhaltung der Verpflichtungen gemäß Artikel 32 und 36 der Datenschutz-Grundverordnung sicherzustellen;

- Je nach Wahl des Verantwortlichen löscht der Auftragsverarbeiter nach dem Ende der Verarbeitungen alle personenbezogenen Daten oder er gibt sie an den Verantwortlichen zurück und er löscht vorhandene Kopien, sofern die lokal geltenden Gesetze nicht die Aufbewahrung der personenbezogenen Daten verlangen;

- Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die notwendig sind, um die Einhaltung der Verpflichtungen nachzuweisen, die in einem schriftlichen Vertrag, der zwischen ihnen geschlossen wurde und in den anwendbaren Datenschutzbestimmungen festgelegt sind, und er ermöglicht Überprüfungen sowie Inspektionen durch den Verantwortlichen oder einen anderen, vom Verantwortlichen beauftragten Prüfer bzw. trägt dazu bei;

- Der Verantwortliche behält die Verantwortung für die Rechtmäßigkeit der Verarbeitung und bleibt der Ansprechpartner für betroffene Personen und Aufsichtsbehörden.

1.2.15 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 logische Struktur des Profiling 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 soweit 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) oder 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.

Der berechtigten Forderungen der betroffenen Person nach Löschung ist nachzukommen, es sei denn, die Verarbeitung ist (i) für die Einhaltung einer gesetzlichen Verpflichtung nach lokalen Gesetzen, denen der Verantwortliche unterliegt, oder (ii) für die Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich. Falls gesetzliche Aufbewahrungsfristen gelten oder die Daten nicht gelöscht werden können, kann die Einschränkung der Verarbeitung der fraglichen Daten auf Anfrage der betroffenen Person verwendet werden.

- Die betroffene Person hat das Recht, die Verarbeitung personenbezogener Daten einschränken zu lassen, wenn (i) die Richtigkeit der personenbezogenen Daten bestritten wird und der Verantwortliche Zeit erhält, in der er die Richtigkeit der personenbezogenen Daten überprüfen kann; (ii) die Verarbeitung unrechtmäßig ist und die betroffene Person der Löschung der personenbezogenen Daten widerspricht und stattdessen die Einschränkung ihrer Verwendung verlangt; (iii) der Verantwortliche die Daten nicht mehr zum Zweck der Verarbeitung benötigt, sie aber von der betroffenen Person für die Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt werden oder (iv) falls die betroffene Person der Verarbeitung widersprochen hat und die Prüfung, ob die berechtigten Gründe des Verantwortlichen schwerer wiegen als die der betroffenen Person, noch aussteht.

- 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, 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 mit automatisierten Mitteln. • Die betroffene Person hat das Recht, nicht einer Entscheidung unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruht 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, aus Gründen, die mit ihrer Situation zusammenhängen, gegen die Verarbeitung ihrer personenbezogenen Daten, die auf dem berechtigten Interesse des Verantwortlichen beruht oder der Erfüllung einer Aufgabe im öffentlichen Interesse dient oder in Ausübung einer öffentlichen Gewalt, die dem Verantwortlichen übertragen wurde, vorgenommen wird, jederzeit Einspruch zu erheben. Der Verantwortliche darf die fraglichen personenbezogenen Daten nicht länger verarbeiten, außer er bringt zwingende berechtigte Gründe für die Verarbeitung vor, die Vorrang haben vor den Interessen, Rechten und Freiheiten der betroffenen Person oder zur Feststellung, Ausübung oder Verteidigung von Rechtsansprüchen.

  Die betroffene Person hat das Recht, jederzeit Einspruch gegen die Verarbeitung ihrer personenbezogenen Daten zu Marketingzwecken zu erheben, einschließlich eines Profiling insoweit, als es mit einem solchen Direktmarketing verbunden ist. Erhebt die betroffene Person Einspruch gegen die Verarbeitung für Direktmarketingzwecke, können die personenbezogenen Daten nicht länger für diese Zwecke verarbeitet werden.

- Die betroffene Person hat das Recht, Beschwerde bei einer Aufsichtsbehörde einzureichen.

- Die betroffene Person hat das Recht auf wirksame Rechtsmittel, wenn sie der Ansicht ist, dass es infolge einer nicht mit der Datenschutz-Grundverordnung in Einklang stehenden Verarbeitung ihrer personenbezogenen Daten zu einer Verletzung ihrer Rechte aus der Datenschutz-Grundverordnung gekommen ist.

- 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 (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 die Anfrage der betroffenen Person ohne unzumutbare Verzögerung und in jedem Fall innerhalb eines Monats nach Eingang der Anfrage.

1.2.16 Rechenschaftspflicht

Alle teilnehmenden Unternehmen werden aufgefordert, Maßnahmen zu ergreifen, die die Einhaltung der Anforderungen 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, (iii) wo notwendig die Anforderungen des Datenschutzes durch Technikgestaltung (by design) und datenschutzfreundliche Voreinstellungen (by default) einhalten, (iv) schriftliche Verträge mit Datenauftragsverarbeitern oder sonstigen Verantwortlichen abschließen, (v) einen DSB benennen sowie (vi) eine Datenschutz-Folgenabschätzung vornehmen.

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

1.2.17 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 Land des EWR haben, ebenso wie mit teilnehmenden Unternehmen mit Sitz außerhalb des EWR. Der Bedarf zum Austausch von Daten innerhalb der ams OSRAM Gruppe 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 Konzerngesellschaften von ams OSRAM ausschließlich im Rahmen üblicher Geschäftszwecke sowie für interne Verwaltungszwecke verarbeitet und übermittelt.

Die Datenübermittlung erfolgt daher zum Zweck der Personalbeschaffung, der Personalverwaltung und -entwicklung, für Compliancezwecke, 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.

1.2.18 Verfahrensfragen

1.2.18.1 Verbindlichkeit der verbindlichen internen Datenschutzvorschriften

Die verbindlichen internen Datenschutzvorschriften sind umfassend verbindlich

1.2.18.1.1 Verbindlichkeit für Konzerngesellschaften und teilnehmende Unternehmen

Die verbindlichen internen Datenschutzvorschriften wurden von den Governance-Verantwortlichen des OSRAM Konzerns verabschiedet und durch die Veröffentlichung der Unternehmensrichtlinie CO3000 (verbindliche interne Datenschutzvorschriften 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 CEO der ams OSRAM Konzerngesellschaft in seiner/ihrer Funktion als Data Protection Executive.

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 ICA beitreten. Durch Unterzeichnung des ICA 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 ICA wird von der Geschäftsführung der Konzerngesellschaft unterzeichnet und an die Konzern-Datenschutzabteilung im ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung zurückgeschickt. Das ICA liegt den verbindlichen internen Datenschutzvorschriften als Anhang bei.

Grundsätzlich müssen alle ams OSRAM Konzerngesellschaften die verbindlichen internen Datenschutzvorschriften unterzeichnen und umsetzen, außer ein 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 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. Unternehmen die keine ams OSRAM Konzerngesellschaften sind, an denen die Konzernmuttergesellschaft von ams OSRAM 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 ICA geschlossen; die verbindlichen internen Datenschutzvorschriften sind dem ICA als Anhang beigefügt. Mit Abschluss des ICA werden die Bestimmungen der verbindlichen internen Datenschutzvorschriften für das beitretende Unternehmen individuell verbindlich. Der Text des ICA liegt den verbindlichen internen Datenschutzvorschriften als Anhang bei.

Die Konzern-Datenschutzabteilung führt im ams OSRAM Intranet ein elektronisches Verzeichnis der teilnehmenden Unternehmen, die sich durch einen Beitritt zum ICA verpflichtet haben, die Bestimmungen der verbindlichen internen Datenschutzvorschriften einzuhalten, und ihrer Kontaktdaten.

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. Die Statusübersicht liegt den verbindlichen internen Datenschutzvorschriften als Anhang bei.

Wenn eine Konzerngesellschaft dem ICA 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 das ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung oder durch die (frühere) Konzerngesellschaft notwendig. Auch bei Widerruf/Aufhebung des ICA oder bei Kündigung der verbindlichen internen Datenschutzvorschriften bleiben die Verpflichtungen aus diesen 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.

1.2.18.1.2 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 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.

1.2.18.1.3 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 1.2.1. – 1.2.7, 1.2.10 – 1.2.15, 1.2.18.1.3, 1.2.18.2, 1.2.18.6, 1.2.18.9, 1.2.18.10 und 1.2.19.

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 Mitgliedsstaates, in dem die betroffene Person ihren gewöhnlichen Aufenthalt oder Arbeitsplatz hat, wenn die betroffene Person in dem EWR-Land wohnt; 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 ICA enthalten, den die Konzern- und beitretenden Unternehmen unterzeichnen, um ihre Akzeptanz und Umsetzung der verbindlichen internen Datenschutzvorschriften anzuzeigen.

1.2.18.2 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 1.2.3 (Transparenz) wird ams OSRAM die verbindlichen internen Datenschutzvorschriften den betroffenen Personen auf angemessene Weise zugänglich machen, insbesondere durch die Veröffentlichung der aktuellen 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.

1.2.18.3 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 ICA 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 CIO des ams OSRAM Co-Hauptsitzes mit Datenschutzverantwortung, der CIO 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 ICAs, berät und leitet die DSK bezüglich der Umsetzung dieser Datenschutzvorschriften und der Einholung und Auswertung der regelmäßigen Berichte der DSK/DSB hinsichtlich 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 Datenschutzvorschriften 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 berichtet einmal jährlich an die Geschäftsführung des ams OSRAM Co-Hauptsitz mit Datenschutzverantwortung. Dieser Bericht beinhaltet insbesondere den Umsetzungsgrad der verbindlichen internen Datenschutzvorschriften in allen teilnehmenden Unternehmen.

1.2.18.4 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.

1.2.18.5 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 Datenschutzvorschriften geeignete Informationen und Schulungen zum ordnungsgemäßen Umgang und Schutz personenbezogener Daten vermittelt werden. 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 in geeigneten Intervallen regelmäßig 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.

1.2.18.6 Internes Beschwerdeverfahren

Betroffene Personen können jederzeit die zuständige interne Beschwerdeabteilung (Konzern-Datenschutzabteilung, Kontaktdaten siehe Abschnitt 1.2.20 Kontakt) oder den zuständigen Datenschutz-Ansprechpartner des teilnehmenden Unternehmens (meist der DSK/DSB) kontaktieren, wenn sie sich über einen Verstoß gegen die verbindlichen internen Datenschutzvorschriften durch ein teilnehmendes Unternehmen beschweren möchten oder Fragen haben. 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.

In der Eingangsbestätigung wird die betroffene Person darüber informiert, welche Stelle – d. h. die Konzern-Datenschutzabteilung oder der DSK/DSB – die Beschwerde behandelt.

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

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

Weitere Einzelheiten – Form der Beschwerde, Verarbeitungszeitraum, Verfahren nach Annahme und/oder Zurückweisung der Beschwerde, weitere Rechtsmittel – werden in einem separaten Beschwerdemanagementkonzept beschrieben.

1.2.18.7 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.

Die primäre Verantwortung für die Durchführung der papierbasierten Überprüfungen sowie regelmäßiger und ad-hoc-Überprüfungen der verbindlichen internen Datenschutzvorschriften liegt bei der Prüfungsabteilung von ams OSRAM. Alternativ und bei Bedarf kann die Überprüfung der verbindlichen internen Datenschutzvorschriften auch durch einen anerkannten externen Prüfer durchgeführt werden.

Die Intervalle der regelmäßigen Überprüfungen der verbindlichen internen Datenschutzvorschriften werden von der Prüfungsabteilung von ams OSRAM im Kontext ihres gesamten Prüfungsplans festgelegt und geplant.

Einmal jährlich findet in den teilnehmenden Unternehmen eine regelmäßige, papierbasierte Überprüfung der verbindlichen internen Datenschutzvorschriften in Form einer Selbsteinschätzung (Ausfüllen eines Fragebogens) statt. Der Leiter der Konzern-Datenschutzabteilung erhält die Auswertung dieser regelmäßigen Selbsteinschätzungen. Die Prüfungsabteilung von ams OSRAM wird über die Ergebnisse informiert.

Unter besonderen Umständen (d. h. Datenschutzvorfälle, Beschwerden von betroffenen Personen, Defizite, die durch Selbsteinschätzungen zu den verbindlichen internen Datenschutzvorschriften aufgedeckt wurden), kann die Konzern-Datenschutzabteilung oder die Abteilung Informationssicherheit (IT DIS) von ams OSRAM zusätzliche ad-hoc-Überprüfungen fordern, die außerhalb des regelmäßigen Prüfungsplans für die verbindlichen internen Datenschutzvorschriften liegen.

Eine Überprüfung umfasst alle Aspekte der verbindlichen internen Datenschutzvorschriften. Kommt eine Überprüfung zu dem Schluss, dass Korrekturmaßnahmen eingeleitet werden müssen, um einen Verstoß gegen die verbindlichen internen Datenschutzvorschriften zu beheben, stellt die Überprüfung ebenfalls sicher, dass diese notwendigen Korrekturmaßnahmen umgesetzt werden.

Der Leiter der Konzern-Datenschutzabteilung, das verantwortliche Geschäftsführungsmitglied der Konzernmuttergesellschaft von ams OSRAM und die Geschäftsführung des geprüften teilnehmenden Unternehmens erhalten den vollständigen Prüfbericht. 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 die Einhaltung der Datenschutzvorschriften im teilnehmenden Unternehmen begrenzt. Einschränkungen aufgrund von Vertraulichkeitsvereinbarungen oder Betriebs- und Geschäftsgeheimnissen werden berücksichtigt.

Die Einzelheiten der Überprüfung werden in einem separaten Prüfkonzept für verbindliche interne Datenschutzvorschriften beschrieben.

1.2.18.8 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 tätigen ams OSRAM Konzerngesellschaften sowie der Annahmestatus der verbindlichen internen Datenschutzvorschriften befindet sich im ams OSRAM Intranet.

Änderungen an den verbindlichen internen Datenschutzvorschriften sind ohne erneute Genehmigung möglich, wenn keine Übermittlung an ein neues teilnehmendes Unternehmen vorgenommen wird bis dieses an die verbindlichen internen Datenschutzvorschriften gebunden ist und deren Einhaltung sicherstellen kann.

Änderungen der verbindlichen internen Datenschutzvorschriften oder der Liste der teilnehmenden Unternehmen sollten einmal jährlich an die zuständige Aufsichtsbehörde gemeldet werden.

Betrifft eine Änderung möglicherweise das Schutzniveau der verbindlichen internen Datenschutzvorschriften oder die Datenschutzvorschriften selbst in erheblichem Umfang, muss dies der zuständigen Aufsichtsbehörde umgehend mitgeteilt werden.

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 1.2.18.1.1). Die entsprechenden Informationen befinden sich im ams OSRAM Intranet.

Nach der offiziellen Genehmigung der verbindlichen internen Datenschutzvorschriften durch die Aufsichtsbehörde wird die Konzern-Datenschutzabteilung diese Genehmigungsbehörden auf Anfrage, aber mindestens einmal jährlich, über Änderungen der verbindlichen internen Datenschutzvorschriften und der Statusübersicht informieren. Diese Mitteilung enthält eine kurze Erläuterung der Gründe, die diese Änderungen rechtfertigen.

1.2.18.9 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, bei der Umsetzung der verbindlichen internen Datenschutzvorschriften vertrauensvoll mit der zuständigen Aufsichtsbehörde zusammenzuarbeiten. 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.

1.2.18.10 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.

Stehen die Verpflichtungen aus den geltenden lokalen Gesetzen in Konflikt mit den verbindlichen internen Datenschutzvorschriften, informiert das teilnehmende Unternehmen unverzüglich die Konzern-Datenschutzabteilung, soweit dies nicht aus anderen Gründen untersagt ist, wie z. B. einem strafrechtlichen Verbot zur Wahrung der Vertraulichkeit einer strafrechtlichen Untersuchung. Die Konzern-Datenschutzabteilung erfasst den Konflikt in der Statusübersicht (vgl. Abschnitt 1.2.18.1.1).

Die Konzern-Datenschutzabteilung informiert alle teilnehmenden Unternehmen, die zuvor Daten an das fragliche teilnehmende Unternehmen übermittelt haben, über den berichteten Konflikt zwischen den verbindlichen internen Datenschutzvorschriften und dem lokalen Gesetz. Ebenso informiert die Konzern-Datenschutzabteilung die zuständige Aufsichtsbehörde über den regulatorischen Konflikt und sucht gemeinsam mit der Datenschutzbehörde und dem teilnehmenden Unternehmen nach einer praktischen Lösung, die den Grundsätzen der Datenschutz-Grundverordnung so nah wie möglich kommt.

Die zuständige Aufsichtsbehörde ist in jedem Fall zu benachrichtigen, wenn eine gesetzliche Vorschrift, der ein teilnehmendes Unternehmen unterliegt, wahrscheinlich erhebliche nachteilige Auswirkungen auf die von den verbindlichen internen Datenschutzvorschriften vorgesehenen Garantien haben könnte, z. B. im Falle eines rechtlich bindenden Ersuchens einer Vollstreckungsbehörde oder eines staatlichen Sicherheitsorgans um Offenlegung der personenbezogenen Daten.

Wenn die Benachrichtigung der Konzern-Datenschutzabteilung oder der zuständigen Aufsichtsbehörde aus strafrechtlichen Gründen ausgesetzt oder untersagt ist, um die Vertraulichkeit der Ermittlungen der Strafverfolgungsbehörden zu wahren, bemüht sich das teilnehmende Unternehmen nach besten Kräften um das Recht, diese Aussetzung/Untersagung zu umgehen, um so viele Informationen so schnell wie möglich zu übermitteln und dies nachweisen zu können. Ist die Benachrichtigung der zuständigen Aufsichtsbehörde nicht möglich, muss das teilnehmende Unternehmen dieser jährlich allgemeine Informationen zu den erhaltenen Anfragen bereitstellen (z. B. Anzahl der Anträge auf Offenlegung, Art der angeforderten Daten, Antragsteller, falls möglich, etc.).

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.

1.2.19 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.

1.2.20 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 & Compliance Department
Marcel-Breuer-Str. 6
80807 München
Email: privacy@ams-osram.com
Internet: https://www.osram.com