Light is OSRAM

OSRAM BCR

Binding Corporate Rules[1] (BCR)
BCR en matière de protection des données à caractère personnel applicables aux sociétés du groupe OSRAM et aux entreprises adoptantes

Termes et définitions

- **Entreprise adoptante :** une société associée au groupe OSRAM, située en Allemagne ou dans un pays tiers, et dont la société mère du groupe OSRAM ou une société affiliée au groupe détient une participation minoritaire et qui, avec l'approbation de la société mère, s'est engagée volontairement à se conformer aux BCR en concluant un contrat d'adoption
- **Binding Corporate Rules (BCR) :** les présentes « Règles d'entreprise contraignantes » et leurs dispositions
- **Chief Data Protection Officer (CDPO) :** le Délégué à la protection des données au niveau du groupe OSRAM
- **Consentement :** toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement [2]
- **Responsable du traitement (Controller) :** une personne physique ou morale, une autorité publique, un service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données
- **Clients et fournisseurs :** des personnes physiques et morales avec lesquelles OSRAM entretient une relation d'affaires ou envisage d'entrer en relation d'affaires
- **Personne concernée :** une personne physique identifiée ou identifiable dont des données à caractère personnel sont traitées. Est censée être une «personne physique identifiable» une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant ; afin d'appliquer les BCR à des personnes légales, il est impératif que la société transférant des données et la société destinataire concluent un accord pertinent (à cet égard, la société transférante et la société destinataire sont également considérées comme des « personnes concernées »)
- **Data Protection Coordinator (DPC)** : personne désignée par une société participante afin d'implémenter les BCR et d'assurer la conformité avec celles-ci
- **Data Protection Executive (DPE)** : directeur à la protection des données à caractère personnel d'une société du groupe OSRAM ; ce rôle est assumé par le CEO de la société OSRAM correspondante

[1] *Règles contraignantes d'entreprise*

[2] *Certaines législations nationales stipulent des exigences spécifiques en matière de consentement pouvant porter atteinte à sa validité*

- **Department for Data Protection (DDP) :** département central d'OSRAM responsable de la protection des données à caractère personnel au niveau Groupe (voir l'organigramme actuellement en vigueur)
- **États membres de l'EEE :** les États membres de l'Union européenne (UE) et d'autres pays signataires du Traité sur l'Espace Economique Européen
- **Directive européenne sur la protection des données (EU Data Protection Directive) :** Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
- **Société du groupe ou société du groupe OSRAM :** la société mère du groupe OSRAM et des sociétés situées en Allemagne ou dans un pays tiers, et dont la société mère du groupe OSRAM détient, directement ou indirectement, une participation majoritaire, ou possède ou dispose de la majorité des droits de vote
- **Société mère du Groupe** : OSRAM GmbH
- **Société participante :** société du groupe OSRAM tenue d'implémenter les présentes BCR ; ou une entreprise adoptante s'engageant volontairement à se conformer aux dispositions des BCR en concluant un contrat d'adoption
- **Données à caractère personnel :** toute information se rapportant à une personne physique identifiée ou identifiable (dénommée «personne concernée»)
- **Traitement de données à caractère personnel** ou **traitement de données :** toute opération et tout ensemble d'opérations, effectuées ou non à l'aide de procédés automatisés, et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, la conservation, l'adaptation, l'altération, la lecture, l'extraction, l'utilisation, la communication par transmission, de même que le blocage, la suppression ou la destruction
- **Sous-traitant (Processor) :** une personne physique ou morale qui traite des données à caractère personnel pour le compte du Responsable du traitement (Controller)
- **Partie tierce (tiers) :** une personne physique ou morale ou un organisme autre que la personne concernée, le Responsable du traitement ou le Sous-traitant

Résumé des BCR

Les présentes BCR ont pour but principal d'assurer que toutes les sociétés du groupe OSRAM et toutes les entreprises adoptantes atteignent un niveau adéquat de protection des données à caractère personnel transférées par une société participante à d'autres sociétés participantes dans le cadre de leurs relations d'affaires. Les BCR s'appliquent aux données à caractère personnel suivantes :

- toutes les données à caractère personnel en provenance d'un État membre de l'UE / l'EEE soumis aux exigences de la Directive européenne sur la protection des données
- données à caractère personnel en provenance de n'importe quel pays d'origine, dans la mesure où elles sont transférées par une société participante (« collecteur des données ») à une autre société participante (« destinataire des données »)

À ce titre, il est essentiel d'établir des standards uniformes de protection des données à caractère personnel et de sécurité de traitement en conformité avec la Directive européenne sur la protection des données. En ce qui concerne les données à caractère personnel tombant dans le champ d'application de ces BCR, il faut assurer un niveau adéquat de protection et des garanties suffisantes conformément à la Directive européenne sur la protection des données en vue de protéger la vie privée et de faire valoir les droits y afférents.

Ces BCR constituent le cadre général et généralement applicable pour le traitement des données à caractère personnel tombant dans leur champ d'application. Elles s'appliquent au traitement, par des sociétés du groupe OSRAM ou par des entreprises adoptantes, des données à caractère personnel d'employés, de clients, de fournisseurs, d'actionnaires, de partenaires commerciaux (existants ou futurs) et d'autres personnes concernées. Les présentes BCR reflètent la situation au moment de leur entrée en vigueur ainsi que les exigences internationales actuellement en vigueur en matière de protection des données. Ces BCR spécifient également les exigences de la Directive européenne sur la protection des données, les documents de travail relatifs à l'article 29 de la Directive 95/46/CE « Groupe de protection des personnes à l'égard du traitement des données à caractère personnel » et les principes établis par la « Conférence Internationale des Commissaires à la Protection des Données et de la Vie Privée » (« Résolution de Madrid ») en date du 5 novembre 2009.

1. Champ d'application des BCR

Les BCR s'appliquent à toutes les sociétés du groupe OSRAM et toutes les entreprises adoptantes dans le monde entier. Le traitement des données suivantes tombe dans le champ d'application des BCR :

- toutes les données à caractère personnel en provenance d'un État membre de l'UE / l'EEE soumis aux exigences de la Directive européenne sur la protection des données
- données à caractère personnel en provenance de n'importe quel pays d'origine, dans la mesure où elles sont transférées par une société participante (« collecteur des données ») à une autre société participante (« destinataire des données »)

c'est-à-dire des données à caractère personnel qui fournissent des informations sur des employés, clients, fournisseurs, actionnaires, partenaires commerciaux (existants ou futurs) et d'autres personnes concernées, et qui sont traitées par des sociétés du groupe OSRAM ou des entreprises adoptantes.

Ces BCR ne s'appliquent pas uniquement aux données à caractère personnel en provenance de sociétés participantes situées dans un pays membre de l'EEE, mais à **TOUTES** les données fournies par une société participante, dans la mesure où celles-ci sont transférées à une autre société participante (à l'inclusion des données à caractère personnel transmises par des sociétés participantes situées hors de l'EEE, à condition que ces données soient transmises à une autre société participante).

2. Principes fondamentaux relatifs au traitement de données à caractère personnel

Les principes suivants sont basés sur la « Directive européenne sur la protection des données » et la « Résolution de Madrid » en date du 5 novembre 2009. Ils s'appliquent au traitement de données à caractère personnel par des sociétés participantes conformément aux BCR.

2.1 Légitimité et légalité du traitement de données

Il est impératif que les données à caractère personnel soient traitées en conformité avec les dispositions légales en vigueur et les principes des BCR.

Pour que le traitement de données soit licite, il est impératif que les conditions suivantes soient remplies :

- la personne concernée a donné un consentement libre, juridiquement valable et sans équivoque ; ou

- le traitement des données est nécessaire afin d'établir, d'exécuter ou de terminer un contrat ou une relation de confiance similaire avec une personne concernée ; ou
- le traitement est indispensable en vue de sauvegarder les intérêts légitimes du Responsable du traitement et il n'y a aucune raison de supposer que la personne concernée présente un intérêt supérieur légitime empêchant le traitement de ses données ; ou
- le traitement est stipulé ou autorisé par les lois et réglementations nationales applicables à la société participante ayant transféré les données ; ou
- le traitement est nécessaire afin d'assurer la conformité aux obligations légales auxquelles le Responsable du traitement est soumis ; ou
- le traitement est nécessaire, exceptionnellement, afin de protéger la vie, la santé ou la sécurité d'une personne concernée.

Le Responsable du traitement est tenu de mettre en œuvre des procédures simples, rapides et efficaces permettant à la personne concernée de retirer son consentement à tout moment.

2.2 Finalités du traitement de données

Les données à caractère personnel ne doivent être traitées que pour des finalités clairement définies, explicites et légitimes. En aucun cas, les données à caractère personnel ne doivent être traitées d'une manière incompatible avec les finalités légitimes pour lesquelles elles ont été collectées. Lors de l'enregistrement, du traitement ou de l'utilisation des données transférées par une autre société participante, les sociétés destinataires s'engagent à respecter la finalité des données transmises ; le traitement des données pour d'autres finalités sans consentement exprès de la personne concernée est illicite, à moins qu'il ne soit autorisé par la législation nationale à laquelle la société transférante est soumise.

2.3 Transparence du traitement de données

Chaque société participante est tenue de traiter les données à caractère personnel de manière transparente. La société participante est tenue de fournir les informations suivantes à la personne concernée par le traitement (en consultation avec la société transférante, le cas échéant) :

- identité du Responsable du traitement et de la société transférante
- catégories de destinataires ou identité de l'organisme destinataire
- finalités du traitement
- origine des données (à l'exception de données à caractère personnel reçues directement de la personne concernée)
- droit de la personne concernée de s'opposer au traitement de ses données à caractère personnel à des fins publicitaires
- autres informations dans la mesure nécessaire pour des raisons d'équité, tels les droits à l'information et les droits à la rectification ou la suppression de données à caractère personnel.

Lorsque les données à caractère personnel n'ont pas été reçues directement de la personne concernée, le droit à l'information ne s'applique pas si la personne concernée a déjà été informée ou si l'information exige des efforts disproportionnés.

2.4 Qualité et minimisation des données

Les données à caractère personnel doivent être factuellement exactes et mises à jour le cas échéant. Il est essentiel de mettre en œuvre des mesures propres à assurer que toutes données incorrectes ou incomplètes sont rectifiées ou supprimées.

Les données à caractère personnel doivent être traitées selon le principe de minimisation des données, c'est-à-dire que la collecte, le traitement et l'utilisation des données à caractère personnel doivent être limités au minimum nécessaire. Notamment, les données doivent être anonymisées, pour peu que les coûts et efforts nécessaires soient raisonnables par rapport à la finalité prévue. Les évaluations statistiques ou études effectuées sur la base de données anonymisées ne sont pas visées par les lois et réglementations en matière de protection des données, à moins que les données ne permettent d'identifier la personne concernée.

Il est nécessaire de supprimer toutes les données à caractère personnel qui ne sont plus nécessaires pour les finalités des affaires pour lesquelles elles ont été collectées et sauvegardées. Si des périodes de conservation sont prescrites par la loi, les données doivent être bloquées au lieu d'être supprimées.

2.5 Transfert ultérieur de données

Le transfert de données à caractère personnel par une société participante à une société non participante n'est licite que si les conditions suivantes sont remplies :

- l'organisme destinataire est en mesure d'assurer un niveau adéquat de protection de données à caractère personnel au sens des articles 25 et 26 de la Directive européenne sur la protection des données. Par exemple, par la conclusion d'un contrat type UE (Clauses contractuelles types de la Commission européenne pour des sous-traitants de données 2010/87/UE ou Clauses contractuelles types de la Commission européenne pour des Responsables du traitement 2011/497/UE ou 2004/915/UE), ou encore, par la conclusion d'autres accords contractuels pertinents entre l'organisme transférant et l'organisme destinataire
- si l'organisme destinataire est un sous-traitant de données, les conditions prévues aux articles 16 et 17 de la Directive européenne sur la protection des données doivent également être satisfaites

Lorsqu'une société participante située dans un pays hors de l'EEE (= importateur de données) a reçu des données à caractère personnel d'une autre société participante située dans un pays EEE (= exportateur de données), l'importateur s'abstient de transférer ultérieurement ces données à un destinataire externe responsable du traitement pour le compte d'une société non OSRAM, située dans un pays hors de l'EEE, et incapable d'assurer un niveau adéquat de protection des données – à moins que les conditions suivantes ne soient remplies :

- avant un transfert ultérieur de données à caractère personnel, la personne concernée a été informée, sous forme intelligible, sur les finalités, l'exportateur des données, le destinataire, le pays destinataire, de même que sur le niveau non adéquat de protection des données par le destinataire ; et
- la personne concernée a eu l'occasion de s'opposer au transfert ultérieur de ses données à caractère personnel ; ou
- pour des données à caractère personnel appartenant à des catégories spécifiques, la personne concernée a donné son consentement préalable, juridiquement valable et sans équivoque, au transfert ultérieur de ses données.

2.6 Catégories spécifiques de données à caractère personnel

Il est en général interdit de traiter des données à caractère personnel appartenant à des catégories spécifiques – y compris toutes les informations concernant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses/philosophiques ou l'appartenance à un syndicat, de même que toutes les informations concernant l'état de santé ou la vie sexuelle.

Au cas où le traitement de données à caractère personnel appartenant à des catégories spécifiques serait indispensable, il est nécessaire d'obtenir le consentement de la personne concernée. Toutefois, les exceptions suivantes s'appliquent :

- la personne concernée n'est pas en mesure de donner son consentement (par ex. urgence médicale) et le traitement est indispensable afin de protéger les intérêts vitaux de la personne concernée ou d'une autre personne ; ou
- le traitement des données est nécessaire dans le contexte d'un diagnostic médical, de médecine préventive, de soins ou traitements, ou pour des services de santé nécessitant le traitement de données par un personnel médical soumis au secret professionnel ou par un autre personnel soumis à une obligation adéquate ; ou
- les données en question ont déjà été rendues publiques par la personne concernée ; ou
- le traitement est nécessaire pour déposer ou exercer une action en justice ou pour se défendre – pour autant qu'il n'y a aucune raison de supposer que la personne concernée présente un intérêt légitime supérieur empêchant le traitement de ses données ; ou
- le traitement est expressément autorisé par les lois et réglementations nationales applicables à la société participante ayant transférée les données (par ex. pour des finalités d'enregistrement/de protection de minorités), et des garanties supplémentaires conformément à la Directive européenne sur la protection des données sont fournies pour le traitement, à l'inclusion des mesures de sécurité appropriées à la protection des données.

Avant de traiter des données à caractère personnel appartenant à des catégories spécifiques, il est obligatoire de consulter le Délégué à la protection des données (Data Protection Officer, DPO) compétent ou le DPC de la société participante.

2.7 Décisions individuelles automatisées

En cas de traitement de données à caractère personnel pour des fins de décisions individuelles automatisées, il est indispensable de mettre en œuvre des mesures adéquates afin de protéger les intérêts légitimes de la personne concernée. Il est interdit de prendre des décisions ayant des conséquences juridiques négatives sur une personne concernée, ou portant un préjudice considérable à ses intérêts, exclusivement sur la base de procédés individuels destinés à analyser des caractéristiques personnelles. En d'autres termes : il est interdit de prendre de telles décisions exclusivement sur la base de technologies informatiques. Les procédés automatisés ne doivent généralement servir que de mesure complémentaire soutenant le processus de décision.

Toutefois, les exceptions suivantes s'appliquent :

- la décision est prise afin de conclure ou d'exécuter un contrat et les intérêts légitimes de la personne concernée sont sauvegardés de manière adéquate – en fournissant des informations sur la logique de prise de décision et en donnant à la personne concernée l'occasion de vérifier la décision et de faire des commentaires. Lorsque la personne apporte des commentaires, le Responsable du traitement est tenu de vérifier sa décision ; ou
- dans des cas autorisés par la législation applicable en vigueur.

2.8 Sécurité des données

Les Responsables du traitement sont tenus de mettre en œuvre des mesures techniques et organisationnelles appropriées afin d'assurer un niveau adéquat de sécurité. Notamment, il est indispensable de protéger les données à caractère personnel contre une suppression accidentelle ou illicite, une utilisation non autorisée, une altération, une perte, une destruction ainsi que contre une divulgation ou un accès non autorisés. Les données à caractère personnel appartenant à des catégories spécifiques nécessitent une protection spéciale.

Pour cette raison, il est essentiel d'assurer un niveau de protection adéquat contre les risques dus au traitement et à la nature de ces données en mettant en œuvre des mesures de sécurité correspondant à l'état actuel de la technologie.

Notamment, il est nécessaire de protéger les ordinateurs (serveurs et stations de travail), les réseaux ainsi que les lignes/applications de communication.

OSRAM a introduit la « Directive interne sur la sécurité de l'information au niveau Groupe » (Corporate Guideline on Information Security) afin d'assurer un niveau adéquat des mesures techniques et organisationnelles. Cette Directive interne est contraignante pour toutes les sociétés du groupe OSRAM et tous les collaborateurs (processus OSRAM IM3000). La version actuelle de la Directive interne est disponible sur intranet.

Un niveau adéquat de protection de données à caractère personnel est assuré par les mesures suivantes : contrôles d'accès aux locaux, aux systèmes et aux données, de même que des contrôles de transmission, de saisie, de traitements, de disponibilité et de ségrégation.

Il est impératif de protéger par mots de passe tous les postes de travail informatiques, y compris tous les dispositifs mobiles (tels les ordinateurs portables). L'intranet d'OSRAM est équipé d'un système de pare-feu afin de protéger les données du Groupe contre tout accès externe non autorisé. La transmission de données à caractère personnel au sein du réseau d'entreprise est généralement cryptée – dans la mesure nécessaire, compte tenu de la nature des données et de leurs finalités prévues.

2.9 Confidentialité du traitement de données

Seul un personnel autorisé et spécifiquement formé, en conformité avec les exigences de protection, est en droit de collecter, traiter et utiliser des données à caractère personnel. Les privilèges d'accès des collaborateurs individuels doivent être limités en fonction de la nature et de l'étendue de leur domaine d'activité correspondant. Il est interdit aux collaborateurs d'utiliser des données à caractère personnel à des fins privées, de même que de les transférer à des personnes non autorisées ou de les mettre à leur disposition. Tout autre collaborateur doit également être considéré comme « non autorisé » si – et dans la mesure où – il/elle n'a pas besoin d'avoir accès à des données à caractère personnel pour accomplir ses tâches. L'engagement de confidentialité reste en vigueur après la cessation du contrat de travail du collaborateur concerné.

2.10 Traitement en sous-traitance

Les sociétés participantes sont en droit de sous-traiter le traitement de données à caractère personnel en conformité avec les présentes BCR et dans le respect des exigences suivantes :

- le Responsable du traitement sélectionne les sous-traitants avec le plus grand soin ; le sous-traitant de données sélectionné est en mesure de mettre en œuvre les mesures techniques et organisationnelles de sécurité nécessaires afin de traiter des données à caractère personnel en conformité avec les règlements en matière de protection des données
- le Responsable du traitement est obligé d'assurer et de régulièrement vérifier que le sous-traitant de données se conforme aux mesures techniques et organisationnelles convenues

- la portée du traitement de données par le sous-traitant fait l'objet d'un contrat écrit ou autrement documenté, stipulant les droits et obligations du sous-traitant de données de manière juridiquement valable et sans équivoque
- le sous-traitant s'engage contractuellement à traiter les données reçues du Responsable du traitement exclusivement pour les fins faisant l'objet du contrat pertinent et conformément aux instructions données par le Responsable du traitement. Il est contractuellement interdit au sous-traitant de traiter des données pour ses propres fins ou pour les fins d'un tiers
- le Responsable du traitement demeure responsable pour la légitimité du traitement et, le cas échéant, demeure le seul interlocuteur de la personne concernée

2.11 Droits inaliénables de la personne concernée

Les personnes concernées disposent des droits inaliénables suivants à l'égard de leurs données à caractère personnel, traitées par une société participante, conformément aux présentes BCR :

- la personne concernée est en droit de **demander des informations** concernant ses données à caractère personnel sauvegardées, leur origine et les finalités de traitement. La personne concernée est en droit d'obtenir des informations sur l'identité du Responsable du traitement et, en cas de transfert de données à caractère personnel, elle est également en droit de demander des informations sur les destinataires ou catégories de destinataires. Le droit d'être informé s'applique également à la structure logique d'activités de traitement automatisé, pour autant que des décisions automatisées soient prises. Les informations susmentionnées doivent être fournies sous forme intelligible, c'est-à-dire que la personne concernée est en droit d'obtenir une copie de ses données à caractère personnel traitées, ou au moins des informations pertinentes, sous forme intelligible. Lorsque la législation locale en vigueur dans le pays de la société transférante prévoit toutefois une exemption, la personne concernée n'est PAS en droit d'obtenir des informations si l'exercice du droit d'être informé risque de compromettre les objectifs des affaires, en particulier du fait de la divulgation de secrets des affaires – à condition que l'intérêt de sauvegarder des secrets des affaires prévale sur l'intérêt de divulgation de la personne concernée. Des lois ou réglementations locales limitent le droit à l'information de la personne concernée si ce droit est exercé à maintes reprises pendant une courte période, à moins que la personne concernée ne puisse présenter une raison légitime. La société participante est en droit de facturer des raisonnables au demandeur, pour autant que la loi nationale l'y autorise
- la personne concernée peut demander la **rectification** des données à caractère personnel inexactes ou incomplètes
- lorsqu'il n'est pas possible de déterminer l'exactitude des données à caractère personnel, la personne concernée est en droit de demander leur **blocage**
- la personne concernée est en droit de demander **la suppression** des données à caractère personnel lorsqu'il s'avère que le traitement était illicite, ou l'est devenu entre-temps, ou lorsque le traitement n'est plus nécessaire pour les finalités prévues. Des demandes de suppression justifiées soumises par une personne concernée doivent être exécutées dans un délai raisonnable, à moins que des périodes de conservation légales ne doivent être respectées. Si des périodes de conservation sont prescrites par la loi, la personne concernée peut demander le blocage de ses données au lieu de leur suppression. Ceci s'applique également lorsqu'il s'avère que la suppression des données est impossible
- la personne concernée est en droit de **s'opposer** – gratuitement – au traitement de ses données à caractère personnel à des fins publicitaires, d'études de marché et/ou de sondages. La personne concernée doit être informée sur son droit d'opposition
- la personne concernée dispose d'un **droit d'opposition général** au traitement de ses données à caractère personnel si – compte tenu de sa situation personnelle spécifique – son intérêt prévaut sur l'intérêt du Responsable du traitement

Pour faire valoir les droits susmentionnés, la personne concernée peut s'adresser par écrit à la société participante, au DPC de la société participante ou au DDP de la société mère du groupe OSRAM. L'organisme contacté est tenu de répondre, dans un délai raisonnable, à une demande justifiée soumise par une personne concernée. La réponse doit être donnée sous forme écrite (un e-mail est suffisant).

2.12 Description du transfert de données

Le groupe OSRAM possède une structure complexe constituée d'un grand nombre de sociétés participantes qui échangent des données à caractère personnel à des finalités multiples. Des données sont échangées aussi bien entre des sociétés participantes situées dans un pays EEE qu'avec des sociétés participantes hors de l'EEE.

Il est nécessaire d'échanger les données à caractère personnel suivantes au sein du groupe OSRAM: données d'employés, de clients, de fournisseurs, d'actionnaires ainsi que d'autres partenaires commerciaux et parties contractantes. En fonction de la finalité du traitement, les données à caractère personnel suivantes sont échangées : nom, identifiant global, date de naissance, nationalité, état civil, sexe, coordonnées de contact, adresse, détails de compte, coordonnées bancaires, appartenance religieuse, ainsi que des informations sur l'éducation, les connaissances et compétences, la carrière, la date d'entrée dans l'entreprise, le niveau du poste de la personne concernée, etc.

Au sein du groupe OSRAM consolidé, toutes ces données sont traitées et transférées exclusivement dans le cadre de la gestion normale des affaires et à des fins d'administration interne. Les données sont transmises pour les finalités suivantes : recrutement, administration RH et développement des ressources humaines, conformité, exécution et implémentation de missions et projets pour des clients externes et internes, traitement de commandes et d'ordres de travail avec des fournisseurs et prestataires de service, accomplissement d'obligations de déclaration, règlement des comptes fournisseurs et comptes à recevoir, comptabilité, communication interne. Cela concerne également la consolidation et le regroupement de procédés informatiques dans certaines régions en vue de réaliser des réductions de coûts, tout comme la coopération et la coordination des sociétés du Groupe au niveau régional ou international dans le cadre de transactions d'affaires et de projets à l'échelle mondiale.

2.13 Aspects procéduraux

2.13.1 Nature contraignante des BCR

Les BCR sont, dans leur intégralité, juridiquement contraignantes.

2.13.1.1 Nature contraignante pour les sociétés du Groupe et les sociétés participantes

Les BCR ont été adoptées par les Responsables de la gouvernance du groupe OSRAM et mises en vigueur par la publication de la « Directive interne IM4000 » (« Règles d'entreprise contraignantes en matière de protection des données à caractère personnel »).

La Direction de chaque société participante est responsable de l'implémentation des BCR au sein de sa société, la mise en œuvre correcte et conforme restant placée sous la responsabilité individuelle dans le cadre du traitement de données à caractère personnel relevant de leurs attributions. En ce qui concerne les sociétés du groupe OSRAM, la responsabilité repose sur le CEO de la société dans ses attributions de DPE.

Les BCR sont contraignantes pour toutes les sociétés du groupe OSRAM et toutes les entreprises adoptantes et doivent être strictement respectées.

Dans le cas des sociétés du groupe, la Direction de la société est tenue de fournir une Déclaration d'engagement, explicite et écrite, afin de documenter l'acceptation et l'implémentation des BCR. En

fournissant cette déclaration, la Direction confirme que les BCR sont désormais contraignantes pour sa société. La Déclaration d'engagement doit être signée par la Direction de la société du groupe et renvoyée au DDP de la société mère OSRAM. Le document type de Déclaration d'engagement est joint en annexe des présentes BCR.

Toutes les sociétés du groupe OSRAM sont tenues de signer et d'implémenter les BCR – à moins qu'une société ne soit exemptée de l'implémentation des BCR pour des raisons valables (par ex. aucune activité commerciale, aucune main d'œuvre, aucun traitement de données à caractère personnel, liquidation ou cession imminente). Pour déposer une demande d'exemption, la société du groupe OSRAM peut envoyer un courriel au DDP qui décide s'il convient de faire droit à la demande. Le DDP informe la société du groupe de sa décision.

Les entreprises adoptantes – c.-à-d. des entreprises autres que des sociétés du groupe OSRAM dont la société mère du groupe OSRAM détient, directement ou indirectement, une participation – peuvent s'engager volontairement, mais de manière juridiquement contraignante, à se conformer aux BCR, si la société le souhaite et si le DDP consent à la participation. Il est à la discrétion du DDP d'accorder à des entreprises autres que des sociétés du groupe OSRAM la possibilité de participer volontairement au processus BCR.

Afin de documenter l'acceptation et l'implémentation des BCR par une entreprise adoptante, il est nécessaire de conclure un contrat d'adoption entre la société mère du groupe OSRAM et l'entreprise adoptante ; les BCR doivent être jointes en annexe au contrat d'adoption. Dès la conclusion d'un contrat d'adoption, les BCR deviennent contraignantes pour l'entreprise adoptante. Le contrat type d'adoption est joint en annexe des présentes BCR.

Sur l'intranet d'OSRAM, le DDP tient un registre électronique des sociétés participantes qui se sont engagées à se conformer aux BCR en signant une Déclaration d'engagement ou un contrat d'adoption. La version la plus récente du registre électronique est disponible sur intranet. Dans cet aperçu, toutes les sociétés du groupe qui sont exemptées de l'obligation de signer et d'implémenter les BCR pour des raisons valables sont mentionnées et clairement indiquées. Les sociétés du groupe n'ayant (pas encore) répondu à l'obligation d'accepter et d'implémenter les BCR figurent également et explicitement dans ledit registre.

Lorsqu'une société du groupe n'a pas (encore) fourni de Déclaration d'engagement aux BCR, il est indispensable de vérifier la légitimité du transfert de données à cette société du groupe selon le cas individuel. De plus, il est essentiel de mettre en œuvre des mesures spéciales, telles la signature des Clauses contractuelles types de la Commission européenne.

Aussi bien la société mère du groupe OSRAM que la société participante sont en droit de retirer, d'annuler ou de résilier l'engagement de conformité aux BCR. La perte du statut de « société du groupe » n'entraîne pas automatiquement la fin de toutes les obligations découlant des BCR. Dans ce cas, une résiliation des BCR par la société mère du groupe OSRAM ou l'ancienne société du groupe devient nécessaire. En cas de retrait/d'annulation de la Déclaration d'engagement ou de la Déclaration d'intention de conclure un contrat d'adoption, ou en cas de résiliation des BCR, les obligations découlant des BCR à l'égard des données à caractère personnel, traitées jusqu'au moment du retrait/de l'annulation/de la résiliation des BCR, restent en vigueur – jusqu'à ce que les données soient supprimées par la société en question en conformité avec les dispositions légales applicables en vigueur.

2.13.1.2 Nature contraignante pour les collaborateurs des sociétés participantes

Les collaborateurs des sociétés participantes sont également tenus de se conformer aux BCR. Le CEO de chaque société participante est tenu d'assurer, par des moyens appropriés, que les collaborateurs s'engagent au respect des BCR d'une manière juridiquement contraignante.

Les BCR, ainsi que toute autre directive/réglementation en matière de protection des données à caractère personnel, sont à la disposition des collaborateurs des sociétés participantes à tout moment.

Les sociétés participantes sont tenues d'informer leurs collaborateurs que le non-respect des BCR peut donner lieu à des sanctions disciplinaires.

2.13.1.3 Nature contraignante vis-à-vis les personnes concernées

Certaines stipulations des BCR sont contraignantes vis-à-vis les personnes concernées en vertu de leurs droits de tiers bénéficiaires. Ces droits sont détaillés dans les paragraphes suivants : articles 1.2.1. – 1.2.10, 1.2.11, 1.2.13.1.3, 1.2.13.6, 1.2.13.9, 1.2.13.10 et 1.2.14.

Pour faire valoir des droits de tiers bénéficiaires susmentionnés vis-à-vis une société participante, les personnes concernées sont en droit de déposer une plainte devant l'autorité compétente chargée de la protection des données ou de déposer un recours devant les tribunaux compétents. De plus, les personnes concernées sont en droit de réclamer des dommages-intérêts.

À ce titre, les personnes concernées peuvent au choix porter plainte :

- devant la juridiction compétente pour le siège social de la société participante située dans un pays EEE et ayant transmis les données ; ou
- devant la juridiction compétence du siège social de la société mère du groupe OSRAM ; ou
- devant l'autorité de contrôle compétente chargée de la protection des données.

Cela signifie que les tribunaux et autorités de l'EEE sont également compétents lorsqu'une société participante située dans un pays hors de l'EEE contrevient aux BCR. Dans un tel cas, la personne concernée dispose des mêmes droits vis-à-vis la société mère du groupe OSRAM, comme si la violation avait été commise par la société mère du groupe OSRAM elle-même – et non par la société participante située dans un pays hors de l'EEE.

Les tribunaux et autorités au sein de l'EEE ne sont toutefois PAS compétents lorsque le destinataire des données a son siège social hors de l'EEE et que la législation de ce pays ne prévoit pas un niveau adéquat de protection des données (tel que constaté par une décision de la Commission européenne).

Afin d'assurer que les personnes concernées jouissent des mêmes droits de tiers bénéficiaires dans des pays où l'étendue des droits de tiers bénéficiaires ne correspond pas à celle stipulée dans les présentes BCR, OSRAM prépare – dans la mesure nécessaire – des ententes contractuelles supplémentaires avec les sociétés participantes concernées. Une clause stipulant les droits de tiers bénéficiaires à accorder aux personnes concernées est prévue dans la Déclaration d'engagement signée par les sociétés du groupe afin de confirmer l'acceptation et l'implémentation des BCR. Ceci s'applique également au contrat d'adoption que les entreprises adoptantes concluent avec la société mère du groupe OSRAM.

2.13.2 Accessibilité des BCR

Les BCR et la clause stipulant les droits de tiers bénéficiaires doivent être facilement accessibles aux personnes concernées. Les personnes concernées peuvent contacter le DPC compétent de la société participante ou, alternativement, s'adresser directement à la société mère du groupe OSRAM. OSRAM met les BCR à la disposition des personnes concernées de manière appropriée, notamment en publiant la version actuelle sur le site web d'OSRAM. Les documents afférents aux BCR applicables – notamment les annexes sui y sont référencées – sont mis à la disposition des personnes concernées sur demande à adresser au DDP.

2.13.3 Implémentation des BCR par les sociétés participantes

La Direction de chaque société participante – ou le CEO d'une société participante du fait de son rôle DPE – est responsable de l'implémentation correcte et de la conformité avec les BCR. La Direction de la société participante peut déléguer cette tâche au DPC. La responsabilité de l'exécution conforme de cette tâche incombe cependant à la Direction.

OSRAM a établi un réseau international de DPC. En signant la Déclaration d'engagement aux BCR ou en concluant le Contrat d'adoption des BCR, la société participante est tenue de désigner un DPC et d'envoyer ses coordonnées de contact au DDP. En outre, la société participante est tenue d'informer, dans les plus brefs délais, le DDP sur des changements relatifs à l'identité du DPC.

Le DPC fait un rapport annuel à la Direction de la société participante. En outre, il informe régulièrement le CDPO (au moins une fois par an). Le DPC fait des rapports sur des sujets tels que le degré d'implémentation des BCR atteint par la société participante.

Le CDPO dirige le DDP, coordonne et guide tous les DPC des données des sociétés participantes. Le CDPO rend compte au CIO (Chief Information Officer, Directeur Informatique) de la société mère du groupe OSRAM ; le CIO rend compte au CFO. Le CDPO coordonne et fait avancer l'implémentation des BCR par les sociétés participantes. Il est notamment responsable d'obtenir les Déclarations d'engagement aux BCR et les Contrats d'adoption des BCR, de consulter et de guider les DPC concernant l'implémentation des BCR, ainsi que de la collecte et de l'évaluation des rapports à soumettre régulièrement par les DPC concernant la protection des données à caractère personnel et l'état d'implémentation des BCR. En outre, le CDPO est chargé de la rédaction de formations BCR appropriées et de leur mise à disposition aux sociétés participantes. Il est également responsable des mises à jour des BCR et de leur communication aux autorités de contrôle compétentes chargées de la protection des données. Le CDPO est soutenu dans ses tâches par le DDP.

Il fait un rapport annuel à la Direction de la société mère du groupe OSRAM. Ce rapport fournit notamment des informations sur le degré d'implémentation des BCR réalisé par les sociétés participantes.

2.13.4 Surveillance de la conformité avec les BCR

Le DPC désigné par la Direction de la société participante effectue des contrôles réguliers afin de veiller à ce que les BCR soient dûment respectées. La Direction de la Société participante soutient le DPC dans ses tâches et l'implique dans la procédure de traitement de plaintes de non-conformité avec les BCR déposées par des personnes concernées.

En cas de graves violations de données à caractère personnel et lors de problèmes d'importance fondamentale, le DPC est tenu de consulter le CDPO et de tenir compte de ses conseils et décisions en vue d'assurer un traitement conforme des violations et problèmes.

La société mère du groupe OSRAM est en droit d'effectuer des contrôles aléatoires afin de vérifier si le DPC remplit correctement son rôle d'assurer l'implémentation des BCR par la société participante et la conformité avec celles-ci. À cet effet, la société mère peut, soit demander au DPC de remplir un formulaire d'auto-évaluation (« Self-Assessment »), soit effectuer des audits. L'auditeur est tenu de documenter le contenu des audits.

Chaque société participante transférant des données est en droit de vérifier, dans des cas individuels, le traitement conforme des données par la société participante recevant les données. Ainsi, la société transférante exerce les droits incombant aux personnes concernées, et soutient les personnes concernées ayant subi des préjudices du fait du non-respect d'une obligation stipulée dans ces BCR dans l'exercice de leurs droits envers la société responsable.

2.13.5 Formation

L'information et la formation des collaborateurs constituent une condition essentielle à l'implémentation conforme des BCR. Il est indispensable que les collaborateurs soient informés que toute violation aux BCR est passible de poursuites en vertu de la loi pénale, de la loi sur la responsabilité civile ou de la loi du travail.

OSRAM offre des mesures spécifiques d'information et de formation visant à informer et former les collaborateurs des sociétés participantes sur la manipulation et la protection conforme des données à caractère personnel dans le cadre de l'implémentation des BCR. Ces mesures s'adressent notamment aux collaborateurs manipulant des données à caractère personnel, en permanence ou régulièrement, dans le cadre de leurs tâches. La participation aux séances de formation est obligatoire pour ces collaborateurs. Les formations BCR doivent être répétées à intervalles réguliers.

Les mesures d'information et de formation peuvent, entre autres, comprendre des séances en ligne (Web-Based Training, WBT), des présentations ainsi que du matériel d'auto-apprentissage, des séances « face à face » de même que des ateliers de formation adaptés aux besoins spécifiques des collaborateurs.

La participation réussie des collaborations aux parcours de formation doit être documentée.

Pour des informations détaillées, veuillez consulter le document « Concept de formation » (Training Concept).

2.13.6 Processus interne de traitement des plaintes

Afin de déposer une plainte concernant une violation aux BCR commise par une société participante, ou en cas de questions, les personnes concernées peuvent s'adresser à tout moment à l'organisme interne des plaintes (DDP ; pour les coordonnées de contacts, voir Chapitre Contact 2.15) ou à l'interlocuteur local en matière de protection des données de la société participante (en règle générale, le DPC). Il est essentiel que l'organisme contacté envoie un accusé de réception de la plainte à la personne concernée dans les plus brefs délais. La réponse à la plainte doit parvenir à la personne concernée dans un délai raisonnable – au minimum dans les trois (3) mois suivant la réception de la plainte. L'accusé de réception doit également comprendre des informations relatives à l'organisme chargé du traitement de la plainte – c'est-à-dire le DDP ou le DPC.

Les collaborateurs chargés du traitement de la plainte au sein du département compétent jouissent de l'indépendance nécessaire à l'exercice de leurs missions.

Lors d'enquêtes, la société participante et le CDPO sont tenues de coopérer avec les autorités de contrôle compétentes chargées de la protection des données dans le pays correspondant et de respecter leur décision.

Pour plus de détails (forme de plainte, délais de traitement, démarches en cas d'acception et/ou de rejet de la plainte, voies de recours complémentaires), veuillez-vous reporter au document séparé « Concept de gestion des plaintes » (Complaint Management Concept).

2.13.7 Audit de conformité aux BCR

OSRAM a étendu son système d'audit et de contrôle interne existant par un programme d'audit BCR. Dans le cadre de ce programme, les sociétés participantes sont tenues d'effectuer des contrôles réguliers afin d'assurer un niveau de protection des données en conformité avec les BCR.

La responsabilité principale de la réalisation d'audits à base de documents, ainsi que d'audits BCR réguliers sur site et d'audits ad-hoc, revient au département d'audit d'OSRAM. Alternativement et si nécessaire, il est possible de mandater un auditeur externe pour la réalisation d'un audit BCR.

Il revient au département d'audit d'OSRAM de définir des intervalles d'audits BCR réguliers en accord avec le calendrier d'audit général.

Une fois par an, les sociétés participantes sont tenues de réaliser des audits BCR réguliers sur la base de documents papier. À cet effet, elles sont obligées de remplir un questionnaire d'auto-évaluation. Les résultats des auto-évaluations régulières doivent être soumis au CDPO. Le département d'audit d'OSRAM doit être informé des résultats.

En cas de circonstances particulières (liées par ex. à des incidents de violation de données, à des plaintes déposées par des personnes concernées ou à des défaillances détectées lors des auto-évaluations), le CDPO ou le Département de la sécurité informatique d'OSRAM (IT DIS) peut demander des audits BCR ad-hoc supplémentaires en dehors du calendrier d'audits BCR régulier.

L'audit BCR couvre tous les aspects des BCR. Lorsqu'il ressort d'un audit BCR qu'il est nécessaire de prendre des mesures correctives afin de remédier à une infraction aux BCR, l'implémentation des mesures correctives doit également être assurée dans le cadre de l'audit BCR.

La version complète du rapport d'audit est envoyée au CDPO, au Directeur responsable de la société mère du groupe OSRAM ainsi qu'à la Direction de la société participante auditée. Les résultats de l'audit BCR sont mis à la disposition de l'autorité de contrôle compétente chargée de la protection des données sur demande. OSRAM peut rendre certaines données d'audit non reconnaissables en vue de protéger des informations confidentielles de l'entreprise.

L'autorité de contrôle compétente chargée de la protection des données est, de son côté, également en droit de soumettre la société participante à un audit BCR. Dans un tel cas, l'autorité de contrôle compétente peut faire réaliser l'audit BCR par son propre personnel ou mandater un auditeur accrédité indépendant. Tout audit BCR réalisé par une autorité de contrôle compétente doit être limité de façon à vérifier uniquement la conformité aux BCR par la société participante. Des restrictions découlant d'engagements de confidentialité ou de secrets des affaires et industriels sont à respecter.

Pour plus de détails concernant l'audit BCR, veuillez-vous reporter au document séparé « Concept d'audit BCR » (BCR Audit Concept).

2.13.8 Mise à jour des BCR et gestion des changements

OSRAM se réserve le droit de changer et/ou mettre à jour les présentes BCR à tout moment. Notamment, une mise à jour peut devenir nécessaire afin d'adapter les BCR à des dispositions légales modifiées, à des modifications de la structure du groupe OSRAM ou à des conditions imposées par les autorités de contrôle compétentes chargées de la protection des données.

Selon les circonstances, des modifications majeures peuvent nécessiter un renouvellement de l'autorisation par les autorités de contrôle compétentes chargées de la protection des données. Un renouvellement de l'autorisation n'est cependant pas nécessaire pour toute autre modification des BCR.

Le DDP tient une liste des modifications/mises à jour des BCR effectuées depuis leur entrée en vigueur. De plus, le DDP tient un registre régulièrement mis à jour de toutes les sociétés participantes s'étant engagées, de manière juridiquement contraignante, au respect des BCR.

Le CDPO est tenu d'informer les autorités de contrôle compétentes, au moins une fois par an, sur des modifications apportées aux BCR ainsi que, sur demande, sur des modifications du registre. Ces notifications doivent comprendre une brève explication des motifs justifiant des modifications.

2.13.9 Coopération mutuelle et coopération avec les autorités de contrôle compétentes chargées de la protection des données

Toutes les sociétés participantes s'engagent à coopérer en toute confiance et à se soutenir les unes les autres dans le traitement de demandes et de plaintes reçues de personnes concernées relatives à des violations des BCR.

En outre, les sociétés participantes s'engagent à coopérer activement avec les autorités de contrôle compétentes chargées de la protection des données en vue d'assurer l'implémentation conforme des BCR. Notamment, elles sont tenues de répondre à des questions concernant les BCR dans un délai raisonnable et de manière appropriée et de tenir compte des conseils et décisions donnés par les autorités de contrôle compétentes chargées de la protection des données en vue d'assurer une implémentation conforme des BCR.

2.13.10 Rapport entre les BCR et les dispositions locales en vigueur

La législation locale applicable, à laquelle la société participante ayant transféré les données est soumise, constitue la base légitime pour le traitement de données à caractère personnel. Lorsque les lois locales applicables prévoient un niveau plus strict de protection de données à caractère personnel que stipulé par ces BCR, les lois locales plus strictes feront foi. Chaque société participante est tenue de vérifier (par ex. par l'intermédiaire du Délégué à la protection des données, du DPC ou de son service juridique) s'il existe des dispositions locales applicables (par ex. lois sur la protection des données à caractère personnel) et, le cas échéant, de se conformer à celles-ci. Lorsque la législation locale applicable prévoit un niveau de protection des données à caractère personnel moins élevé que les BCR, les présentes BCR feront foi.

En cas de divergence entre les obligations découlant de la législation locale applicable et les BCR, la société participante est obligée d'informer le CDPO dans les plus brefs délais. Il/elle doit enregistrer le conflit déclaré dans le registre.

Ensuite, le DDP informe toutes les sociétés participantes, ayant transmis des données à la société participante concernée, de l'existence d'un conflit entre les BCR et la législation locale. En outre, le DDP est tenu d'informer l'autorité de contrôle compétente chargée de la protection des données sur le conflit juridique. En coopération avec l'autorité de contrôle compétente et la société participante, il est tenu de chercher une solution viable qui correspond le mieux aux principes de la Directive européenne sur la protection des données.

2.14 Responsabilité

Chaque société participante est tenue responsable de tout préjudice causé par une violation des BCR commise par elle-même.

En outre, la société mère du groupe OSRAM assume la responsabilité pour toute violation des BCR commise par des sociétés participantes situées dans un pays hors de l'EEE – à l'inclusion des dommages-intérêts à payer en cas de violation des BCR et également en cas de violation des droits de la personne concernée en raison d'un tel incident de non-conformité commis par une société participante hors de l'EEE. La société mère du groupe OSRAM s'engage à prendre toutes les mesures nécessaires afin de remédier aux violations des BCR commises par des sociétés participantes situées dans un pays hors de l'EEE.

La charge de la preuve incombe à la société mère du groupe OSRAM. Notamment, il lui incombe de prouver qu'aucune violation des BCR ne s'est produite ou que la société participante située dans un pays hors de l'EEE n'est pas responsable de la violation des BCR pour laquelle la personne concernée réclame des dommages et intérêts.

Si la société mère du groupe OSRAM peut fournir la preuve que la société participante située hors de l'EEE n'est pas responsable de la violation des BCR, la société mère peut chercher elle-même à se dégager de la responsabilité.

2.15 Contact

En cas d'inquiétudes concernant la protection de données, les personnes concernées sont invitées à contacter le DPC de la société participante ou le CDPO :

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