S

Binding Corporate Rules
BCR

pour les sociétés du groupe Siemens
et autres sociétés adhérentes
pour la protection des données personnelles

1. Introduction

Le principal objectif de ces règles d'entreprise contraignantes (BCR) est de garantir, pour toutes les sociétés du groupe Siemens et les sociétés adhérentes, une protection adaptée des informations à caractère personnel faisant l'objet d'un transfert dans le cadre des relations professionnelles liant une société participante établie dans un pays de l'Espace économique européen (pays de l'EEE), ou dans un pays où le niveau de protection des données est considéré comme suffisant par décision de la Commission européenne, à des sociétés du groupe Siemens et/ou d'autres sociétés adhérentes.

Dans ce but, il est essentiel d'établir des normes cohérentes quant à la sécurité et la confidentialité des données lors du traitement de ce type d'informations personnelles, conformément à la directive européenne sur la protection des données, et d'assurer ainsi un niveau de protection adapté pour ces données et des garanties suffisantes, conformément à la directive européenne concernant la protection du droit à la vie privée ainsi que des droits qui en découlent.

Ces BCR fournissent un cadre réglementaire général et universellement reconnu pour le traitement par les sociétés du groupe Siemens, ou d'autres sociétés adhérentes, de toutes les informations personnelles relatives aux employés, clients, fournisseurs, partenaires commerciaux actuels ou futurs, ainsi qu'aux autres personnes concernées

- dans la mesure où ces informations personnelles ont fait l'objet d'un transfert entre une société participante établie dans un pays de l'EEE ou dans un pays où le niveau de protection des données est considéré comme suffisant par décision de la Commission européenne et une société participante établie en dehors de l'EEE ; et
- dans le cadre du traitement des informations personnelles par des sociétés participantes établies dans un pays de l'EEE ou dans un pays où le niveau de protection des données est considéré comme suffisant par décision de la Commission européenne.

Les présentes BCR reflètent l'état des exigences actuelles en matière de protection des données au niveau international, telles qu'applicables au moment de l'entrée en vigueur des BCR, notamment les exigences liées à la directive européenne 95/46/CE sur la protection des données, aux documents de travail pertinents du groupe de travail Article 29, ainsi qu'aux principes émis lors de la Conférence internationale des commissaires à la protection des données et de la vie privée concernant les normes internationales sur la protection de la vie privée (ci-après désignée sous le terme de « Résolution de Madrid »), en date du 5 novembre 2009.

2. Champ d'application des BCR

Toutes les sociétés du groupe Siemens ainsi que toutes les autres sociétés adhérentes à l'échelle internationale entrent dans le champ d'application de ces BCR.

Les BCR s'appliquent au traitement de toutes les informations à caractère personnel faisant l'objet d'un transfert entre une société du groupe Siemens ou une autre société adhérente établie dans un pays de l'EEE ou dans un pays où le niveau de protection des données est considéré comme suffisant par décision de la Commission européenne, et une société du groupe Siemens ou une autre société adhérente établie en dehors de l'EEE. Elles s'appliquent également dans le cadre du traitement des informations à caractère personnel par des sociétés participantes établies dans un pays de l'EEE ou dans un pays où le niveau de protection des données est considéré comme suffisant par décision de la Commission européenne.

Les BCR assurent donc la protection de toutes les informations personnelles des employés, clients, fournisseurs, actionnaires et de tout autre tiers contractant ou partenaire commercial, actuel ou futur, d'une société du groupe Siemens ou d'une autre société adhérente établie dans un pays de l'EEE ou dans un pays où le niveau de protection des données est considéré comme suffisant par décision de la Commission européenne, y compris dans la mesure où de telles données font l'objet d'un transfert vers une société participante établie en dehors de l'EEE et y sont ensuite traitées par cette dernière.

3. Définitions

Les termes utilisés dans ces BCR sont définis comme suit :

- **BCR :** Binding Corporate Rules, c'est-à-dire les règles d'entreprise contraignantes présentées dans ce document, ainsi que les règlementations s'y rapportant.
- **CDPO :** Chief Data Privacy Officer, personne responsable de la confidentialité des données chez Siemens AG.
- **Consentement :** manifestation de volonté libre et éclairée par laquelle la personne concernée accepte que ses informations personnelles fassent l'objet d'un traitement spécifique[1].
- **Responsable du traitement :** société juridiquement indépendante qui détermine les finalités et les moyens de traitement des données. Les filiales dépendantes, les sites d'activité et les établissements permanents font partie intégrante du contrôleur.
- **Clients et fournisseurs :** personnes physiques et morales avec lesquelles une relation commerciale est établie ou prévue.
- **Personne concernée :** toute personne physique identifiée ou identifiable dont les données font l'objet d'un traitement. Par « identifiable », on entend une personne pouvant être directement ou indirectement identifiée, par exemple à l'aide d'un numéro d'identification ; certaines personnes morales peuvent être incluses dans le champ d'application des BCR, par l'établissement d'un accord en ce sens entre la société à l'origine du transfert des données et le destinataire de ces données.
- **DPO :** Data Privacy Officer, délégué à la protection des données nommé par la société participante, auquel il incombe de mettre en œuvre les BCR et de les faire respecter.
- **DPE :** Data Privacy Executive, directeur de la confidentialité des données. Le rôle de DPE d'une société du groupe Siemens est assuré par le PDG de ladite société du groupe Siemens.
- **Pays de l'EEE :** pays membres de l'Union européenne (UE) et autres pays signataires du traité sur l'Espace économique européen (EEE).
- **Société du groupe ou société du groupe Siemens :** société Siemens Aktiengesellschaft et toute société, basée en Allemagne ou à l'étranger, dans laquelle Siemens Aktiengesellschaft détient de façon directe ou indirecte une participation majoritaire, ou possède ou contrôle la majorité des droits de vote (« sociétés affiliées »).
- **LC CO DP / LC C DP :** unité en charge de la confidentialité générale des données au sein de Siemens AG.
- **Société participante :** société du groupe Siemens pour laquelle la mise en œuvre de ces BCR est obligatoire, ou autre entreprise associée à Siemens, en Allemagne ou à l'étranger, dans laquelle Siemens AG ou une société affiliée détient une participation minoritaire et qui, avec l'accord de Siemens AG, s'est engagée de son plein gré à se conformer aux

[1] Certaines législations nationales peuvent établir des critères spécifiques pour l'expression du consentement, lesquels peuvent avoir une incidence sur la validité de celui-ci.

réglementations des BCR en concluant un Accord d'adhésion (« autres sociétés adhérentes »).

- **Données personnelles :** toute information liée à la personne concernée.
- **Traitement des données personnelles** ou **traitement des données :** toute opération ou ensemble d'opérations effectuées sur les informations à caractère personnel, de manière automatisée ou non, telles que collecte, stockage, conservation, adaptation, modification, lecture, récupération, utilisation, divulgation par transmission, blocage, suppression ou destruction.
- **Entité de traitement :** personne physique ou morale qui traite les données personnelles pour le compte d'un contrôleur.
- **Tiers :** toute personne physique ou morale ou autre entité distincte de la personne concernée, de l'entité de traitement ou du contrôleur.
- **Transfert de données personnelles** ou **transfert de données :** divulgation ou transmission des informations personnelles à des tiers, ou processus visant à divulguer ces données à des tiers, sous quelque forme que ce soit, à des fins d'examen ou de récupération.

4. Principes essentiels pour le traitement des informations à caractère personnel

Les principes énoncés ci-après sont tirés en particulier de la directive européenne 95/46/CE sur la protection des données et de la résolution de Madrid du 5 novembre 2009. Ils s'appliquent au traitement par les sociétés participantes des données à caractère personnel entrant dans le champ d'application de des présentes BCR :

4.1 Légitimité et légalité en matière de traitement des données

Le traitement des données à caractère personnel doit être effectué dans le respect de la loi, en conformité avec les dispositions légales applicables et en tenant pleinement compte des principes établis dans le cadre des présentes BCR.

Toute forme de traitement n'est tolérée que si au moins l'une des conditions préalables suivantes est satisfaite :

- La personne concernée a donné librement son accord exprès et sans équivoque ; ou
- Le traitement des données vise à établir une relation contractuelle ou une relation similaire de confiance avec la personne concernée ; ou
- Le traitement est nécessaire à la protection des intérêts légitimes du contrôleur et rien ne laisse supposer que le bien-fondé des intérêts de la personne concernée puisse prévaloir et empêcher le traitement des données ; ou
- Le traitement est stipulé ou autorisé par la législation et la réglementation nationales applicables au contrôleur ; ou
- Le traitement est nécessaire afin de respecter les obligations légales auxquelles le contrôleur est soumis ; ou
- Le traitement est requis, à titre exceptionnel, afin de protéger la vie, la santé ou la sécurité de la personne concernée.

Le contrôleur doit mettre en place des procédures simples, rapides et efficaces qui permettent à la personne concernée de retirer son accord à tout moment.

4.2 Objectif

Les données personnelles doivent être traitées uniquement dans les buts explicites et légitimes stipulés. En aucun cas elles ne doivent faire l'objet d'un traitement qui serait incompatible avec les

buts légitimes pour lesquels elles ont été collectées. Les sociétés participantes sont tenues de se conformer aux objectifs initiaux lorsqu'elles enregistrent et traitent ou utilisent les données qui leur sont transmises par une autre société participante; le but du traitement des données ne peut être modifié qu'avec l'accord de la personne concernée ou dans les limites autorisées par la loi applicable à la société participante transmettant les données.

4.3 Transparence

Toutes les sociétés participantes doivent traiter les données personnelles de manière transparente. Les personnes concernées dont les données personnelles font l'objet d'un traitement par une société participante doivent être informées par celle-ci des éléments suivants (en consultation avec la société transmettant les données, le cas échéant) :

- Identité du contrôleur et de la société transmettant les informations
- Catégories de destinataires ou identité de l'entité bénéficiaire
- Objectif du traitement
- Origine des données (sauf s'il s'agit de données personnelles collectées directement auprès de la personne concernée)
- Droit de s'opposer au traitement des données personnelles de la personne concernée à des fins publicitaires
- Autres informations dans les limites requises pour garantir l'équité, par exemple,
    - droit à l'information, à la rectification et à la suppression.

Dans la mesure où les données personnelles n'ont pas été collectées directement auprès de la personne concernée, de telles informations doivent être fournies, sauf, à titre exceptionnel, si leur non-divulgation est nécessaire à la protection de la personne concernée ou des droits de personnes tierces, si la personne concernée a déjà été informée ou si cela impliquerait des efforts disproportionnés.

4.4 Qualité des données et parcimonie

Les données personnelles doivent être exactes et, le cas échéant, tenues à jour. Les mesures appropriées doivent être prises afin de corriger ou de supprimer toute donnée inexacte ou incomplète.

Le principe qui préside au traitement des données est l'économie de données. L'objectif est de recueillir, traiter et utiliser uniquement les informations personnelles requises, c'est-à-dire une quantité de données aussi limitée que possible. En particulier, il est souhaitable d'exploiter des données anonymes ou utilisant des pseudonymes, si tant est que le coût et les efforts consentis pour ce faire soient proportionnels à l'objectif fixé. En effet, les études ou analyses statistiques basées sur des données anonymisées ou pseudonymisées ne sont pas concernées par les obligations de protection de la confidentialité des données, puisqu'elles ne peuvent pas permettre d'identifier la ou les personnes concernées.

Toutes les données personnelles qui ne sont plus nécessaires aux activités de l'entreprise pour lesquelles elles avaient initialement été recueillies et enregistrées doivent être effacées. Dans le cas où des durées obligatoires de conservation des informations sont prévues par la loi, il convient de bloquer l'accès aux données, et non de les effacer.

4.5 Transmission des données

La transmission de données personnelles par une société participante (c'est-à-dire une société du groupe Siemens ou autre partie adhérente) à une société tierce (c'est-à-dire une société qui n'est pas tenue de respecter les BCR, par exemple une société à participation minoritaire n'ayant pas

conclu d'accord d'adhésion ou une société externe) en dehors de l'EEE n'est tolérée que dans les cas suivants :

- L'entité bénéficiaire assure un niveau de protection adéquat pour les données personnelles au sens de l'article 25 de la directive 95/46/CE de l'UE relative à la protection des données : elle doit, notamment, avoir conclu un contrat type conforme aux exigences de l'UE (décision 2010/87/UE relative aux clauses contractuelles types pour le transfert de données ou décisions 2001/497/CE ou 2004/915/CE) ou avoir adopté les accords contractuels adéquats entre elle et la société transmettant les informations ;
- Les données peuvent être transmises si elles entrent dans le cadre des exceptions définies à l'article 26 de la directive 95/46/CE de l'UE relative à la protection des données ;
- Si l'entité bénéficiaire est celle qui traitera les données, les conditions stipulées aux articles 16 et 17 de la directive 95/46/CE de l'UE relative à la protection des données doivent également être remplies.

4.6 Catégories spéciales de données à caractère personnel

En règle générale, les catégories spéciales de données personnelles, à savoir les informations concernant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance à un syndicat, la santé ou l'orientation sexuelle, ne doivent pas faire l'objet d'un quelconque traitement.

S'il s'avérait nécessaire de traiter des données appartenant à ces catégories spéciales de données personnelles, il faudrait obtenir le consentement exprès de la personne concernée, à moins que :

- la personne concernée ne soit pas en mesure de donner son accord (par exemple, en cas d'urgence médicale) et que le traitement de ces données soit nécessaire afin de protéger les intérêts vitaux de la personne concernée ou d'un tiers ; ou
- le traitement soit requis pour la pose d'un diagnostic médical, en vue d'un traitement médical préventif ou de l'administration de soins, ou aux fins de gestion des services de santé, et que le traitement des données soit réalisé par un membre du personnel médical soumis au secret professionnel ou par tout autre membre du personnel tenu au secret par une obligation similaire ; ou
- la personne concernée ait déjà rendu ces données publiques ; ou
- le traitement soit nécessaire afin d'établir, d'exercer ou de défendre des droits légaux dans le cadre de poursuites en justice, à condition que rien ne laisse supposer que le bien-fondé des intérêts de la personne concernée puisse prévaloir et empêcher le traitement de ces données ; ou
- le traitement soit expressément autorisé par la loi en vertu de la législation nationale applicable (par exemple, aux fins de l'inscription/la protection des minorités) et que des garanties supplémentaires au sens de la directive 95/46/CE de l'UE relative à la protection des données soient fournies pour le traitement des données, y compris des mesures de sécurité spécialement destinées aux données de ce type.

Le délégué à la protection des données ou DPO compétent au sein de la société participante doit être consulté avant de traiter les catégories spéciales de données à caractère personnel.

4.7 Décisions individuelles automatisées

Dans le cas où les données personnelles sont traitées en vue de décisions individuelles automatisées, les intérêts légitimes de la personne concernée doivent être garantis par l'intermédiaire de mesures appropriées. Les décisions ayant des conséquences juridiques négatives pour la personne concernée ou lui portant un préjudice important ne doivent pas être prises exclusivement sur la base d'une procédure individuelle automatisée destinée à évaluer les caractéristiques personnelles d'une personne. Autrement dit, les décisions ne devront pas être exclusivement basées sur l'utilisation de technologies de l'information. Une exception est possible uniquement si la décision :

- est prise dans le cadre de l'adoption ou de l'exécution d'un contrat à la demande de la partie concernée et à condition que cette demande ait été satisfaite ou qu'aient été prises

les mesures appropriées pour protéger les intérêts légitimes de la personne concernée, notamment en lui donnant la possibilité d'indiquer son point de vue ; ou

- est autorisée par une loi qui prévoit aussi des mesures permettant de protéger les intérêts légitimes de la personne concernée.

4.8 Sécurité des données

Les contrôleurs sont tenus de prendre les mesures techniques et organisationnelles adéquates afin d'assurer le niveau de sécurité requis pour protéger les données personnelles contre leur effacement, utilisation non autorisée ou altération involontaire ou illicite, leur perte ou leur destruction, ainsi que leur divulgation ou consultation non autorisée. Eu égard à l'état des techniques actuelles et au coût de leur mise en œuvre, de telles mesures doivent garantir un niveau de sécurité approprié par rapport aux risques induits par le traitement et la nature des données à protéger. Les catégories spéciales de données personnelles doivent faire l'objet de mesures de protection spécifiques.

Les mesures de sécurité à mettre en place concernent, en particulier, le matériel informatique (serveurs et ordinateurs de bureau), les réseaux, les lignes de communication et les applications.

Afin de s'assurer que les mesures techniques et organisationnelles prises en vue de protéger les données sont suffisantes, il est nécessaire de se référer le Guide de la sécurité des informations de l'entreprise, qui s'applique à l'ensemble du groupe Siemens en vertu de la circulaire CIT n° 4/2009. La version actuelle du Guide est disponible sur l'intranet.

Les mesures spécifiques mises en place afin de garantir un niveau de protection adéquat pour les données personnelles incluent les contrôles suivants : contrôle des admissions, contrôle des accès au système, contrôle des accès aux données, contrôle des transferts, contrôle des entrées, contrôle des postes, contrôle de la disponibilité et contrôle de la séparation des fonctions.

Tous les ordinateurs de bureau, y compris les périphériques mobiles (dont les ordinateurs portables), sont protégés par un mot de passe. L'intranet de Siemens dispose d'un pare-feu pour protéger le contenu interne à l'entreprise contre tout accès externe non autorisé. Les transferts de données personnelles au sein du réseau interne de l'entreprise sont généralement chiffrés, dans la mesure où la nature des données personnelles et leur utilisation prévue l'exigent.

4.9 Confidentialité du traitement des données

Seuls les membres autorisés du personnel qui ont été spécifiquement formés en conformité avec les exigences de protection de la confidentialité des données peuvent recueillir, traiter ou exploiter des données à caractère personnel. Les autorisations d'accès accordées à chaque employé dépendent de la nature de leurs attributions spécifiques et de leur champ d'action. Il est interdit aux employés d'utiliser les données personnelles à des fins privées, de les transmettre ou de les rendre disponibles par tout autre moyen à des personnes non autorisées. Dans ce contexte, on entend par « personnes non autorisées » notamment les autres employés, dès lors qu'ils n'ont pas besoin des données personnelles pour mener à bien leurs propres activités. L'obligation de confidentialité s'étend au-delà de la fin de la relation de travail de l'employé concerné.

4.10 Traitement externalisé des données

Dans le cas où les sociétés participantes chargent une autre entreprise de traiter les données à caractère personnel d'après les modalités des présentes BCR, les exigences suivantes doivent être respectées :

- L'entreprise en charge du traitement doit être soigneusement sélectionnée par le contrôleur : l'entité de traitement sélectionnée doit pouvoir garantir l'application des mesures de sécurité techniques et organisationnelles requises pour exécuter le traitement des données en accord avec la réglementation en matière de protection de la confidentialité des données ;
- Le contrôleur doit s'assurer, par le biais de vérifications régulières, que l'entité de traitement est toujours en totale conformité avec les mesures de sécurité techniques et organisationnelles convenues ;

- Dans le cadre du mandat de traitement des données, les performances doivent être établies par le biais d'un contrat écrit ou autrement documenté, dans lequel les droits et obligations de l'entité de traitement sont clairement définis ;
- L'entité de traitement doit s'engager par contrat à traiter les données transmises par le contrôleur uniquement dans le cadre contractuel stipulé et selon les instructions fournies par le contrôleur. Le traitement des données aux fins propres de l'entité de traitement ou pour le compte d'un tiers doit être interdit par les dispositions contractuelles ;
- Le contrôleur conserve la responsabilité de la légitimité du traitement et reste l'interlocuteur de la personne concernée par les données à caractère personnel.

5. Droits fondamentaux de la personne concernée

Les personnes concernées possèdent les droits inaliénables répertoriés ci-après, eu égard à leurs données à caractère personnel qui sont traitées par la société participante dans le cadre des présentes BCR.

- La personne concernée peut demander à ce que lui soient communiquées, sous une forme intelligible, les données personnelles traitées la concernant, ou toute information disponible concernant leur origine et l'objectif du traitement. La personne concernée a également le droit d'être informée de l'identité du contrôleur et, dans le cas où ses données personnelles sont transmises à d'autres personnes, de celle des destinataires ou des catégories de destinataires. Le droit à l'information s'applique également à la structure logique des opérations de traitement automatisées, dans le cas où des décisions automatisées sont concernées. Dans les cas prévus par la législation locale applicable, la personne concernée ne dispose pas de droit à l'information si cela nuit considérablement à l'activité de l'entreprise, en particulier si la divulgation de secrets commerciaux et l'intérêt de protéger ces secrets l'emportent sur l'intérêt de la personne concernée. Les réglementations locales peuvent restreindre le droit à l'information de la personne concernée si ce droit est exercé de manière répétée sur une courte période, à moins que la personne concernée ne puisse y apporter une justification légitime. La société participante peut facturer des frais d'un montant raisonnable à la personne concernée en contrepartie de ces informations, dans la mesure où la législation nationale applicable le permet.
- La personne concernée peut demander la rectification de ses données à caractère personnel si celles-ci sont incorrectes ou incomplètes.
- La personne concernée a le droit de demander à ce que ses données personnelles soient rendues inaccessibles s'il n'est pas possible d'établir leur exactitude.
- La personne concernée a le droit de demander à ce que ses informations personnelles soient effacées si leur traitement était illégal ou l'est devenu entre temps, ou dès qu'elles ne sont plus requises à des fins de traitement. Toute demande justifiée de suppression émanant de la personne concernée doit être prise en compte dans un délai raisonnable, sauf si cela contrevient aux périodes légales de conservation des informations ou aux obligations contractuelles. S'il existe une durée légale de conservation, la personne concernée peut demander que l'accès à ses données soit bloqué plutôt que les données effacées. Il en va de même s'il s'avère impossible d'effacer les données.
- La personne concernée a le droit de s'opposer au traitement de ses données personnelles à des fins publicitaires ou pour les besoins d'une étude de marché et/ou d'une enquête d'opinion. La personne concernée doit être informée gratuitement de son droit d'opposition.
- La personne concernée dispose également d'un droit général d'objection au traitement de ses données personnelles dès lors que, de par sa situation personnelle, son intérêt légitime est supérieur à celui du contrôleur, eu égard au traitement des données personnelles.

La personne concernée peut faire valoir les droits cités ci-dessus par écrit auprès de la société participante, du DPO compétent au sein de la société participante ou du LC CO DP. Suite à toute requête justifiée de la personne concernée, l'entité contactée doit fournir une réponse dans un délai raisonnable. Cette réponse doit être fournie sous forme écrite (un e-mail est accepté).

6. Description du transfert des données

L'entreprise Siemens est organisée selon une structure complexe, réunissant un grand nombre de sociétés du groupe et de sociétés participantes entre lesquelles des données à caractère personnel sont échangées à des fins diverses. L'échange de données s'effectue entre sociétés participantes situées dans des pays de l'EEE, mais aussi avec des sociétés participantes établies en dehors de l'EEE.

La nécessité de tels échanges de données au sein de l'ensemble du groupe Siemens concerne les données personnelles des employés, des clients, des fournisseurs, des actionnaires et d'autres partenaires commerciaux et parties contractantes. Il peut s'agir, selon l'objectif prévu, du nom, de l'identificateur universel, de la date de naissance, de la nationalité, du statut marital, du sexe, des coordonnées de contact et de livraison, des informations de compte, des coordonnées bancaires, de l'appartenance religieuse, du cursus de formation, des connaissances et compétences, de la carrière, de la date d'embauche, du niveau hiérarchique, etc.

Ces données font l'objet de traitements et de transferts au sein du groupe Siemens exclusivement, dans le cadre de ses activités normales et aux fins de son administration interne. Les transferts de données sont ainsi réalisés aux fins du recrutement, de la gestion des RH et du développement des compétences du personnel, aux fins de la conformité, afin d'exécuter et de réaliser les missions et projets pour des clients internes et externes, afin de traiter les bons de commande et les ordres de travail passés auprès des fournisseurs et des prestataires de services, afin de répondre à l'obligation de génération de rapports, afin d'honorer les dettes d'exploitation ou de collecter les créances clients, à des fins comptables, à des fins de communication interne, dans le but de consolider ou de regrouper des processus informatiques au sein de certaines régions afin de réduire les coûts, mais aussi pour faciliter la coopération et la coordination des sociétés du groupe aux niveaux des divisions et des régions, ainsi que de manière globale, dans le cadre de projets et transactions commerciales à l'échelle internationale.

7. Questions de procédure

7.1 Nature contraignante des BCR

Les BCR sont contraignantes dans leur intégralité.

7.1.1 Nature contraignante pour les sociétés du groupe Siemens et autres sociétés adhérentes

Les BCR ont été adoptées par Siemens Aktiengesellschaft (Siemens AG) et sont entrées en vigueur suite à la publication d'une Circulaire d'entreprise Siemens.

C'est à la direction générale de chaque société participante qu'incombe la responsabilité de vérifier la bonne mise en œuvre de ces BCR au sein de son organisation ; quant à l'exécution des règles au cas par cas, elle relève de la responsabilité de l'entité qui, au sein de cette société, est chargée de traiter les données personnelles. Dans chaque société du groupe Siemens, la responsabilité incombe au Directeur général en sa qualité de DPE (Data Privacy Executive, directeur de la confidentialité des données).

De nature contraignante, les BCR doivent être appliquées et respectées par toutes les sociétés du groupe Siemens, ainsi que par les autres sociétés adhérentes.

Dans le cas des sociétés du groupe, afin de consigner l'acceptation et la mise en œuvre des BCR, la direction générale de la société concernée doit émettre, par écrit et de manière explicite, une Déclaration d'engagement en faveur des dispositions des BCR. La publication de cette Déclaration d'engagement écrite rend les dispositions des BCR individuellement contraignantes pour la société du groupe. Le document doit être signé par la direction générale de la société puis renvoyé au LC C DP. La Déclaration d'engagement est jointe à l'Annexe 1 des BCR.

En principe, chaque société du groupe Siemens doit signer la Déclaration d'engagement et appliquer les BCR dans un délai de deux ans maximum à compter de la date de publication de la Circulaire d'entreprise Siemens qui la concerne (étant entendu que, pendant la période de

transition, la société s'efforcera de s'y conformer dans la mesure du possible). Cette exigence s'applique sauf si une société du groupe Siemens bénéficie d'une dérogation qui la dispense de mettre en œuvre les BCR pour une raison valable (par exemple, une loi ou réglementation financière/bancaire obligatoire, l'absence d'activité commerciale, l'absence d'employés, l'absence de traitement de données personnelles ou encore une cession ou un dépôt de bilan imminent). La demande de dérogation doit être envoyée par e-mail à Siemens AG (LC C DP) par la société du groupe Siemens, en précisant le motif. Le LC C DP détermine alors si la demande est justifiée et informe la société de sa décision.

Les sociétés ne faisant pas partie du groupe Siemens, dans lesquelles Siemens AG détient des parts directes ou indirectes, peuvent d'elles-mêmes prendre un engagement juridiquement contraignant de manière à se conformer aux dispositions des BCR, si elles le souhaitent et si Siemens AG (LC C DP) accepte une telle participation (les « autres sociétés adhérentes »). Seule Siemens AG peut décider, à son entière discrétion, d'accorder ou non la possibilité aux sociétés externes au groupe Siemens de participer volontairement au processus BCR.

Afin de consigner l'acceptation et la mise en œuvre des BCR par ces autres sociétés adhérentes, un Accord d'adhésion est conclu entre Siemens AG (LC C DP) et chaque société participante ; les BCR sont incluses en annexe de l'Accord d'adhésion. Une fois l'Accord d'adhésion conclu, les dispositions des BCR deviennent individuellement contraignantes pour la société participante. Ainsi, ces autres sociétés adhérentes disposent d'une période de transition au cours de laquelle elles devront mettre en œuvre tous les moyens nécessaires pour respecter les BCR, période qui ne saurait excéder deux ans à compter de la date d'entrée en vigueur de l'Accord d'adhésion (étant entendu que, pendant cette période de transition, la société s'efforcera de se conformer aux règles dans la mesure du possible). Le texte de l'Accord d'adhésion est joint en annexe des BCR.

Sur l'intranet Siemens, le LC C DP tient à jour un registre électronique des sociétés participantes qui ont choisi de se conformer aux dispositions des BCR en signant une Déclaration d'engagement ou un Accord d'adhésion. La dernière version du registre électronique (vue d'ensemble de l'état) est consultable à tout moment sur l'intranet du LC CO DP. Cette vue d'ensemble présente également les sociétés du groupe qui ont bénéficié d'une dérogation à titre exceptionnel les dispensant de signer et d'appliquer les BCR pour un motif valable. Enfin, elle consigne et présente les sociétés du groupe qui n'ont pas (encore) satisfait à leur obligation d'accepter et d'appliquer les BCR.

Si une société du groupe n'a pas (encore) signé de Déclaration d'engagement en faveur des BCR, il convient de vérifier au cas par cas que chaque transfert de données vers cette société est légitime et réalisé par le biais de mesures spéciales adaptées, conformément aux exigences des articles 25 et 26 de la directive 95/46/CE. Cela s'applique également aux autres sociétés adhérentes tant qu'elles n'ont pas encore conclu d'Accord d'adhésion.

Siemens AG ou chaque société participante peut mettre fin à l'engagement à se conformer aux BCR par un retrait, une annulation ou une dénonciation. La perte du statut de société du groupe ne signifie par forcément la fin des obligations découlant des BCR. Dans ce cas, la dénonciation des BCR par Siemens AG ou par la société faisant (anciennement) partie du groupe est nécessaire. Par ailleurs, en cas de retrait ou d'annulation de la Déclaration d'engagement ou de la décision de signer un Accord d'adhésion, ou en cas de dénonciation des BCR, les obligations en découlant concernant les données personnelles traitées jusque là restent valables tant que lesdites données n'ont pas été effacées par la société concernée, conformément aux dispositions réglementaires.

7.1.2 Nature contraignante vis-à-vis des employés des sociétés participantes

Les employés des sociétés participantes sont également tenus de respecter les dispositions des BCR. Le directeur général de chaque société participante est dans l'obligation de s'assurer, par le biais de moyens adéquats, que les BCR ont un effet juridiquement contraignant pour ses employés. Dans cette optique, dès lors que les BCR sont publiées dans le cadre d'une Circulaire d'entreprise Siemens, elles deviennent contraignantes pour tous les employés de la même manière (avec d'éventuelles variations d'un pays à l'autre) que toutes les autres Circulaires d'entreprise Siemens, notamment en vertu du Code d'éthique Siemens qui exige que les employés se conforment à toutes les circulaires et politiques Siemens applicables.

Les dispositions des BCR et toutes les autres réglementations relatives à la protection de la confidentialité des données sont à la disposition permanente des employés des sociétés participantes.

Les sociétés participantes s'engagent à informer leur personnel que le non-respect des dispositions des BCR peut entraîner des sanctions disciplinaires ou des mesures en vertu du droit du travail (avertissement officiel, licenciement) à l'encontre des employés.

7.1.3 Nature contraignante vis-à-vis des personnes concernées

Certaines dispositions des BCR sont également contraignantes pour les personnes concernées, en vertu des droits des tiers bénéficiaires. Les dispositions des sections suivantes confèrent des avantages aux tiers : Sections 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 5, 7.1.3, 7.6, 7.9, 7.10 et 8.

Les personnes concernées peuvent choisir de déposer une plainte pour non-respect des dispositions applicables des BCR par une société participante, soit à l'encontre de ladite société, soit à l'encontre de Siemens AG (LC CO DP). Des informations complémentaires sur les voies de recours et sur la procédure interne de dépôt de plainte sont disponibles à la Section 7.6 des BCR, ainsi que dans un document distinct traitant de la procédure à suivre en cas de dépôt de plainte (Concept de gestion des plaintes).

En outre, les personnes concernées sont habilitées à faire respecter tous les droits de tiers bénéficiaires mentionnés ci-dessus par une société participante, en déposant une plainte auprès de l'autorité compétente de protection des données ou par le biais d'autres recours juridiques devant les tribunaux compétents. Elles peuvent réclamer une indemnisation en cas de dommages.

Les personnes concernées ont la possibilité de déposer une plainte :

- auprès de la juridiction de la société participante ayant transmis les données ;
- auprès de la juridiction dont dépend le siège social de Siemens AG ;
- auprès de l'autorité compétente de protection des données.

Cela signifie qu'en cas d'infraction aux dispositions des BCR par une société participante établie en dehors de l'Espace économique européen (EEE), les tribunaux et autorités de l'EEE restent compétents. La personne concernée détient les mêmes droits vis-à-vis de la société participante qui a accepté la responsabilité que si l'infraction avait été commise par une société basée dans un pays de l'EEE.

En revanche, la compétence des tribunaux et des autorités de l'EEE telle qu'elle est décrite ci-dessus ne s'applique pas si le destinataire des données est établi dans un pays extérieur à l'EEE mais dont le niveau de protection des données a été reconnu comme suffisant par décision de la Commission européenne.

Afin de s'assurer que les personnes concernées bénéficient également des droits de tiers bénéficiaires légalement exécutoires dans les pays où l'octroi de tels droits par le document des BCR s'avérerait insuffisant, Siemens AG s'engage, dans la mesure où cela est nécessaire, à rédiger des accords contractuels additionnels avec le concours des sociétés participantes qui l'autorisent. Une clause de tiers bénéficiaire accordant les droits nécessaires aux personnes concernées est incluse dans la Déclaration d'engagement que les sociétés du groupe signent pour indiquer qu'elles acceptent et appliquent les BCR. Il en va de même pour l'Accord d'adhésion conclu par les autres sociétés adhérentes avec Siemens AG.

7.2 Caractère public des BCR

Les personnes concernées doivent pouvoir accéder aux BCR et à la clause relative aux tiers bénéficiaires facilement et de manière permanente. Elles peuvent contacter le délégué à la protection des données (DPO) de la société participante ou, éventuellement, contacter directement Siemens AG. Siemens AG s'engage à mettre les BCR à la disposition des personnes concernées de manière appropriée et permanente, en particulier en publiant la version à jour de ces BCR sur son site Internet, à l'adresse http://www.siemens.com.

7.3 Mise en œuvre des BCR au sein des sociétés participantes

La direction générale de la société participante, ou le PDG de la société du groupe participante agissant en qualité de DPE, est responsable de la mise en œuvre des BCR et de leur respect. La direction générale de la société participante peut déléguer cette tâche, mais non sa responsabilité, au DPO.

Siemens a établi un réseau mondial de DPO. Lors de la publication de la Déclaration d'engagement en faveur des BCR ou de l'adoption d'un Accord d'adhésion aux BCR, chaque société participante indique le DPO compétent et transmet les coordonnées de celui-ci au LC C DP. La société participante doit informer le LC C DP sans tarder de tout remplacement au poste de DPO.

Le DPO soumet, au moins une fois par an, un rapport à la direction générale de la société participante concernée et rend compte régulièrement (au moins une fois par an) au CDPO de Siemens AG. Le DPO communique, en particulier, sur le degré de mise en œuvre des BCR au sein de la société participante.

Le CDPO de Siemens AG, quant à lui, rend compte une fois par an devant le Conseil d'administration de Siemens AG. Son rapport concerne, en particulier, le degré de mise en œuvre des BCR au sein des différentes sociétés participantes.

Le CDPO (Chief Data Privacy Officer) est le responsable de la confidentialité des données au niveau de Siemens AG. En tant que tel, il a été nommé à cette fonction par une annonce du Conseil signée par le PDG et le conseiller général de Siemens AG. Le CDPO est à la tête de l'unité LC CO DP, laquelle a la responsabilité opérationnelle du programme de confidentialité des données de Siemens et de l'instauration des exigences de confidentialité des données, en particulier à travers des initiatives de formation et de contrôle (notamment, gestion des incidents et évaluation des risques). Dans ses fonctions à la tête de cette unité, le CDPO est aidé par d'autres employés de cette même unité qu'il a lui même recrutés et qui doivent lui rendre compte.

7.4 Contrôle de la conformité aux BCR

La conformité des sociétés participantes aux BCR fait l'objet d'évaluations régulières, principalement par le DPO nommé par la direction générale de chaque société participante. La direction générale de la société participante concernée soutient le DPO dans l'exercice de ses fonctions et l'implique dans le cas où des personnes concernées par les données personnelles portent plainte pour non-respect des BCR.

En cas de non-respect significatif de la confidentialité des données ou de problèmes cruciaux, le DPO consulte le CDPO de Siemens AG et tient compte de ses avis et décisions pour y remédier.

Le LC CO DP est habilité à réaliser des contrôles aléatoires sur le travail du DPO en rapport avec la mise en œuvre des BCR et leur respect au sein de la société participante. Pour cela, il peut demander au DPO de réaliser une auto-évaluation écrite ou organiser des entretiens. La teneur de ces entretiens doit être documentée par le LC CO DP.

Toute société participante qui transfère des données a le droit d'évaluer, au cas pas cas, le traitement qui en est fait par l'entité destinataire. Ce faisant, la société transférant les données exerce les droits établis en faveur des personnes concernées et leur apporte son soutien dans leurs revendications à l'encontre de la société responsable de la violation des obligations imposées par les présentes BCR.

7.5 Formation

Un élément clé pour la mise en œuvre réussie des BCR consiste à communiquer aux employés les informations et instructions adéquates. Les employés doivent notamment être informés que toute violation des BCR peut avoir des répercussions pour eux en termes de responsabilité civile, de droit pénal ou de droit du travail.

Siemens AG fournit des informations spécifiques et met en place des initiatives de formation spéciales afin que les employés des sociétés participantes soient en mesure d'assurer de manière adéquate le traitement et la protection des données personnelles dans le cadre de la mise en

œuvre des BCR. Les initiatives de formation sont destinées, en particulier, aux employés amenés à traiter les données à caractère personnel de manière permanente ou régulière. Pour ces employés, la participation aux cours de formation est obligatoire. Les cours de formation sur les BCR doivent être suivis à intervalles réguliers.

Les initiatives de formation et d'information peuvent par exemple se présenter sous la forme de formations en ligne, de présentations et de documents d'auto-formation, de programmes de formation théoriques en groupe et d'ateliers conçus spécifiquement pour les employés.

Les progrès des employés dans le cadre de ces programmes de formation doivent être documentés.

Des informations supplémentaires sont disponibles dans un document détaillant les concepts de formation.

7.6 Traitement des plaintes

Les personnes concernées par les données personnelles peuvent contacter le service compétent de gestion des plaintes chez Siemens AG (LC CO DP ; pour connaître les coordonnées, reportez-vous à la section 9) ou le DPO compétent au sein de la société participante et ce, à tout moment, que ce soit pour adresser des plaintes par rapport à la violation des BCR par une société participante ou pour poser des questions. La personne concernée devra être rapidement notifiée de la réception de sa plainte par l'entité contactée, et cette plainte devra être traitée dans les trois (3) mois à compter de sa réception. Ce délai peut être prolongé dans les limites du raisonnable en cas de retard non imputable à la société du groupe Siemens ou l'autre société adhérente, par exemple si la personne concernée n'a pas fourni les informations considérées comme nécessaires dans les temps.

Les employés chargés de traiter la plainte au sein du service compétent de gestion des plaintes jouissent du niveau adéquat d'indépendance dans l'exercice de leurs fonctions.

Dans le cadre d'une enquête, la société participante et le LC CO DP doivent coopérer avec les autorités du pays en matière de protection des données et respecter leurs opinions.

Plus d'informations sont disponibles dans un document distinct relatif au concept de gestion des plaintes, lequel figure en annexe des BCR. Il détaille notamment les formes de plainte, les temps de réponse, la procédure découlant de l'acceptation/du rejet de la plainte, les autres recours légaux, etc.

7.7 Audit et BCR

En complément des autres systèmes de contrôle et d'audit interne existant au sein du groupe d'entreprises Siemens, Siemens a mis en place un programme distinct d'audit pour les BCR afin de s'assurer qu'est réalisée une évaluation régulière du niveau de protection des données au sein des sociétés participantes, comme exigé par les dispositions des BCR. Ces audits BCR doivent être effectués de manière régulière ou à la demande du CDPO de Siemens AG ; ils seront réalisés par l'organisme d'audit de Siemens (F A) avec l'aide de l'organisme de protection des données Siemens (des experts en protection des données, par exemple) ou par un auditeur externe. Si nécessaire, un audit BCR peut aussi être demandé par le service d'audit interne de Siemens (F A), par le Comité d'audit de Siemens AG, par la direction générale ou le Comité d'audit de la société participante, ou encore par le service chargé de la sécurité des informations (GS IT ISEC).

L'audit BCR couvre tous les aspects des BCR. Si un audit BCR conclut qu'il est nécessaire de prendre des actions correctives pour remédier à une violation des BCR, le CDPO est chargé d'en surveiller la mise en œuvre.

Le CDPO de Siemens AG, le responsable en la matière au sein du Conseil d'administration de Siemens AG et la direction générale de la société participante auditée reçoivent le rapport d'audit BCR complet. Les résultats de l'audit BCR sont également mis à la disposition de toute autorité compétente en matière de protection des données qui en fait la demande (c'est-à-dire les autorités des pays de l'EEE à partir desquels des données personnelles ont été transmises à la société auditée).

L'autorité compétente en matière de protection des données a le droit de mener son propre audit BCR de la société participante. Elle peut soit réaliser l'audit elle-même, soit mandater un auditeur indépendant accrédité. Dans le cas d'un audit BCR officiel de ce type, seule la conformité aux BCR au niveau de la société participante est prise en compte. Il doit être tenu pleinement compte des restrictions résultant d'accords de confidentialité ou de secrets commerciaux ou industriels.

Les détails de l'audit BCR sont présentés dans un document distinct relatif au concept d'audit BCR.

7.8 Mise à jour des BCR et gestion du changement

Siemens se réserve le droit de modifier et/ou de mettre à jour les présentes BCR à tout moment. Une telle mise à jour des BCR peut notamment s'avérer nécessaire suite à une modification des obligations légales, à des changements structurels significatifs au niveau du groupe Siemens ou à certaines exigences officielles imposées par les autorités compétentes en matière de protection des données.

En cas de modifications importantes des BCR, l'octroi d'une nouvelle approbation peut être exigé dans certains cas. Toute autre modification peut être apportée aux BCR sans nouvelle approbation de la part des autorités compétentes en matière de protection des données.

Le LC C DP tient à jour la liste de toutes les modifications/mises à jour des BCR depuis leur entrée en vigueur. Il tient également à jour la liste régulièrement actualisée de toutes les sociétés participantes qui sont effectivement liées par les BCR (vue d'ensemble des états, se reporter à la section 7.1.1). Le transfert de données personnelles à une nouvelle société participante n'est autorisé qu'à partir du moment où celle-ci se conforme aux BCR et a publié une déclaration effective d'engagement en faveur des BCR ou a conclu un Accord d'adhésion aux BCR et renvoyé cet accord dûment signé au LC C DP.

Le LC C DP informe l'autorité en charge de la protection des données des modifications apportées aux BCR ainsi qu'à la vue d'ensemble des états, sur demande mais au minimum une fois par an. Ces notifications doivent comporter une brève explication justifiant les modifications apportées.

7.9 Assistance mutuelle et coopération avec les autorités en charge de la protection des données

Siemens AG et les sociétés participantes devront coopérer en toute confiance et se soutenir mutuellement en cas de demandes ou de plaintes exprimées par les personnes concernées par rapport à une éventuelle non-conformité avec les BCR.

Siemens AG et les sociétés participantes s'engagent en outre à coopérer en toute confiance avec les autorités compétentes en matière de protection des données dans le cadre de la mise en œuvre des BCR. Elles devront répondre aux demandes concernant les BCR formulées par l'autorité en charge de la protection des données, de façon appropriée et dans un délai raisonnable, et également suivre les conseils et les décisions prises par les autorités compétentes en matière de protection des données en ce qui concerne la mise œuvre des BCR.

7.10 Relations entre BCR et dispositions réglementaires locales

L'évaluation de la légitimité du traitement des données personnelles dépend de la législation locale applicable. Si la législation locale applicable stipule un niveau de protection des informations personnelles plus élevé que celui défini par les BCR, le traitement des données devra respecter la législation applicable. Chacune des sociétés participantes est tenue de vérifier (par exemple par l'intermédiaire du DPO ou du service juridique) l'existence de telles dispositions réglementaires locales (par exemple, une législation relative à la confidentialité des données) et d'en garantir le respect. Si la législation locale applicable indique un niveau de protection des informations personnelles moins élevé que celui défini par les BCR, les présentes BCR seront appliquées.

Dans l'hypothèse où les obligations découlant de la législation locale applicable entrent en conflit avec les BCR, la société participante en informera le LC C DP dans les plus brefs délais. Le LC C DP consignera le conflit signalé dans la vue d'ensemble des états (se reporter à la section 7.1.1).

Le conflit signalé entre les BCR et la législation locale sera notifié par le LC C DP à toutes les sociétés participantes ayant déjà transféré des données à la société participante en question. Le LC C DP informera également l'autorité compétente en matière de protection des données de ce conflit de réglementations et recherchera, conjointement avec cette autorité et la société participante, une solution concrète afin de résoudre ce problème en respectant au mieux les principes énoncés dans la directive 95/46/CE de l'UE relative à la protection des données.

8. Responsabilité

Siemens AG assume toute responsabilité en cas de non-respect des BCR par les sociétés participantes basées en dehors de l'EEE. Siemens AG s'engage à vérifier que les sociétés participantes basées en dehors de l'EEE respectent les BCR et que, dans le cas contraire, ces sociétés prennent les mesures correctives nécessaires pour se mettre en conformité avec les BCR.

Siemens AG s'engage également à verser des indemnités pour les dommages causés dans le cas où une infraction aux BCR serait établie et entraînerait une violation des droits de la personne concernée.

La charge de la preuve incombe à Siemens AG. Siemens AG doit démontrer qu'aucune infraction aux BCR n'a été commise ou que la société participante basée en dehors de l'EEE n'est pas responsable de l'infraction aux BCR sur la base de laquelle la personne concernée demande à être indemnisée.

9. Contact

Les personnes concernées peuvent faire part de leurs problèmes et questions au DPO de la société participante concernée ou à l'entité en charge de la confidentialité générale des données chez Siemens AG à l'adresse suivante :

Siemens AG

LC CO DP

St.-Martin-Str. 76

D-81541 Munich

E-mail : datenschutz@siemens.com

Site intranet de Siemens : https://intranet.privacy.siemens.com

Internet : http://www.siemens.com

10. Annexes

Annexe 1 : Déclaration d'engagement pour les sociétés du groupe

Annexe 2 : Accord d'adhésion pour les autres sociétés adhérentes

Annexe 3 : Liste des sociétés participantes

Annexe 4 : Gestion des plaintes liées aux BCR