GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

1271-04-02/08/FR
WP 155 rév. 04

Document de travail sur les questions fréquemment posées (FAQ) concernant les règles d'entreprise contraignantes

Adopté le 24 juin 2008
Révisé en dernier lieu et adopté le 8 avril 2009

FAQ sur les règles d'entreprise contraignantes (BCR)

Comme expliqué dans le document de travail 74 (WP 74)[1], le groupe de travail «Article 29» estime que les règles d'entreprise contraignantes sont une solution convenant aux sociétés multinationales et autres groupes semblables, qui leur permet de remplir leurs obligations légales et de garantir un niveau adéquat de protection des informations à caractère personnel lors du transfert de données à l'extérieur de l'Union européenne.

Le groupe de travail/les autorités de protection des données publient ces FAQ qui s'appuient sur leur expérience en matière de demandes d'approbation des règles d'entreprise contraignantes et de demandes d'information sur l'interprétation des documents WP 74[2] et WP 108[3]. Les FAQ ont pour but de clarifier certaines exigences particulières afin d'aider les demandeurs à obtenir l'approbation de leurs règles d'entreprise contraignantes.

Ces FAQ ne sont pas exhaustives et seront mises à jour le cas échéant.

1 – Les règles d'entreprise contraignantes doivent-elles s'appliquer à toutes les données à caractère personnel traitées par le groupe?

Non, les règles d'entreprise contraignantes sont un moyen juridique pour protéger adéquatement les données personnelles couvertes par la directive 95/46/CE et transférées en dehors de l'Union vers des pays dont on estime qu'ils n'offrent pas un niveau adéquat de protection. Les autres données personnelles traitées par le groupe et ne faisant l'objet d'aucun traitement à l'intérieur de l'UE ne doivent pas être soumises aux règles.

Toutefois, il est fortement recommandé que les groupes multinationaux appliquant des règles d'entreprise contraignantes adoptent un ensemble unique de politiques ou de règles globales pour protéger toutes les données à caractère personnel qu'ils traitent. L'existence d'un arsenal réglementaire unique donnera lieu à un système plus simple et plus efficace, que le personnel pourra plus aisément appliquer et que les personnes concernées comprendront plus facilement. Les entreprises inspireront certainement le respect si elles démontrent leur ferme volonté d'assurer un niveau élevé de protection de la vie privée à toutes les personnes concernées, indépendamment de leur lieu d'établissement et des exigences de juridictions particulières.

Il convient de noter que le groupe peut très bien disposer d'un arsenal réglementaire unique tout en limitant les droits de tiers bénéficiaires requis dans les règles d'entreprise contraignantes aux seules données personnelles transférées depuis l'Union européenne.

---

1 Document de travail WP 74: Transferts de données personnelles vers des pays tiers: Application de l'article 26 (2) de la directive de l'UE relative à la protection des donnés aux règles d'entreprise contraignantes applicables aux transferts internationaux de données, adopté le 3 juin 2003 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_fr.htm.

2 Cf. note de page 1.

3 Document de travail WP 108 établissant une liste de contrôle type pour les demandes d'approbation des règles d'entreprise contraignantes, adopté le 14 avril 2005 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_fr.htm.

2 – Les règles d'entreprise contraignantes doivent-elles s'appliquer aux sous-traitants qui ne font pas partie du groupe?

Non, seuls les sous-traitants qui font partie du groupe et qui traitent des données pour le compte d'autres filiales du groupe devront respecter les règles d'entreprise contraignantes en leur qualité de filiales du groupe. Les règles d'entreprise contraignantes peuvent contenir des règles particulières destinées aux filiales du groupe agissant en qualité de sous-traitants, de manière à remplir les exigences des articles 16 et 17 de la directive 95/46/CE.

Il n'est pas obligatoire que les sous-traitants qui ne sont pas des filiales du groupe et qui agissent pour le compte d'une filiale du groupe soient liés par les règles d'entreprise contraignantes. Toutefois, ces sous-traitants devront toujours agir selon les instructions du responsable du traitement et devront être liés par contrat ou par quelque autre acte juridique conformément aux dispositions des articles 16 et 17 de ladite directive.

Si les sous-traitants ne font pas partie du groupe et sont établis en dehors de l'UE, les filiales du groupe devront également se conformer aux articles 25 et 26 de la directive 95/46/CE concernant les flux de données transfrontaliers et garantir un niveau adéquat de protection. Par exemple, l'entreprise peut prouver le caractère adéquat de ses procédures par des moyens contractuels, en utilisant par exemple les clauses contractuelles types adoptées par la Commission européenne pour les transferts aux sous-traitants en dehors de l'UE, ou en soumettant les sous-traitants aux dispositions des règles d'entreprise contraignantes pour ce qui concerne leurs données.

Les règles d'entreprise contraignantes devront traiter de ces situations.

3 – Si une violation des règles d'entreprise contraignantes est commise en dehors de l'UE, quelle filiale du groupe en est responsable?

Indépendamment de l'existence d'une responsabilité en vertu de la directive 95/46/CE incombant à l'entité qui exporte des données personnelles de l'Union, les règles d'entreprise contraignantes elles-mêmes doivent désigner une entité au sein de l'Union européenne qui accepte d'assumer la responsabilité de toute infraction aux règles commise par une filiale du groupe en dehors de l'UE. Il suffit que cette responsabilité porte sur les données transférées à partir de l'UE conformément aux règles.

Le document WP 74 considérait que, dans la majorité des cas, ce serait le siège du groupe, s'il est établi dans l'UE, qui endosserait la responsabilité en question. Si le siège du groupe est établi à l'extérieur de l'UE, le document WP 74 permet au groupe de désigner la filiale adéquate dans l'UE qui assumerait la responsabilité des infractions aux règles commises en dehors de l'UE. Cette responsabilité inclut, sans que cela soit exhaustif, le versement d'une indemnité pour réparer tout préjudice résultant d'une violation des règles d'entreprise contraignantes par une filiale du groupe établie en dehors de l'UE et liée par les règles.

Cependant, pour certains groupes dont la structure d'entreprise est particulière, il n'est pas toujours possible d'imposer à une entité précise d'assumer la totalité de la responsabilité d'éventuelles violations des règles d'entreprise contraignantes en dehors

de l'UE. Dans ces cas, le groupe de travail accepte que, lorsque le groupe peut démontrer en quoi il ne lui est pas possible de désigner une seule entité dans l'UE, celui-ci propose d'autres mécanismes de responsabilité mieux adaptés à son organisation.

Une possibilité consiste à instaurer un mécanisme de responsabilité solidaire entre les importateurs et les exportateurs de données, tel qu'il est prévu dans les clauses contractuelles types établies par la décision 2001/497/CE de la Commission du 15 juin 2001, ou à définir un autre régime de responsabilité reposant sur des obligations de diligence, tel qu'il est prévu dans les clauses contractuelles types visées dans la décision 2001/915/CE de la Commission du 27 décembre 2004. Une dernière possibilité, concernant en particulier les transferts effectués par des responsables du traitement vers des sous-traitants, consiste à appliquer le mécanisme de responsabilité prévu dans les clauses contractuelles types figurant dans la décision 2002/16/CE de la Commission du 27 décembre 2001.

Les autorités de protection des données peuvent accepter au cas par cas les solutions alternatives précitées en matière de responsabilité, dans la mesure où des garanties suffisantes et adéquates sont fournies par le demandeur. Lorsqu'un autre mécanisme est utilisé, il importe de prouver que les personnes concernées seront aidées dans l'exercice de leurs droits et ne seront aucunement défavorisées ou indûment empêchées de faire valoir leurs droits.

4 – Les règles d'entreprise contraignantes doivent-elles toujours conférer à la personne concernée le droit de déposer une plainte auprès de l'autorité de protection des données pour violation des règles d'entreprise contraignantes?

Oui, en dépit du fait que, dans certains cas, les règles ou en particulier les droits de tiers bénéficiaires peuvent avoir été limités aux données provenant de l'Union européenne et aux personnes disposant déjà, dans le cadre de leur législation nationale, du droit de porter plainte contre l'entité exportatrice auprès de l'autorité de protection des données, il est important de consacrer le droit de porter plainte en cas de violation des règles dans leur ensemble commise par une filiale du groupe.

5 – Les informations sur les droits de tiers bénéficiaires doivent-elles être facilement accessibles aux personnes concernées qui en bénéficient?

Oui, le document WP 74 exige que les règles d'entreprise contraignantes ainsi que les voies de réclamation et de réparation en cas d'infraction aux règles soient facilement accessibles aux personnes concernées. L'existence de droits de tiers bénéficiaires et le contenu de ces droits représentent une option importante pour toute personne concernée étudiant les voies de recours qui s'offrent à elle. Certaines entreprises ont décidé, pour des raisons légitimes, de ne pas inclure de clause relative aux droits de tiers bénéficiaires dans le texte des règles d'entreprise contraignantes, mais de présenter ces droits dans un document séparé. Lorsque ces droits figurent dans un document distinct, ils doivent être énoncés d'une manière transparente et être facilement accessibles à toute personne concernée qui en bénéficie.

6 – Les règles d'entreprise contraignantes doivent-elles décrire les traitements et les transferts de données à caractère personnel effectués au sein du groupe, et jusqu'à quel niveau de détail?

Oui, il y a lieu de faire figurer dans les règles d'entreprise contraignantes une description générale des principales finalités du traitement des données et des types de transferts.

Le groupe peut, par exemple, expliquer dans ses règles d'entreprise contraignantes que les transferts sont effectués vers toutes ses entités pour des raisons liées à la mobilité du personnel, que les données relatives aux ressources humaines sont envoyées aux principaux centres de données du groupe en Allemagne, aux États-Unis et à Singapour en vue de leur conservation et de leur archivage, que les données relatives aux ressources humaines sont communiquées au siège aux fins de la définition d'une stratégie de rémunération globale et de la planification des prestations pour le groupe.

Cependant, s'agissant des autorisations et permis nationaux, certains États membres pourraient imposer aux demandeurs d'inscrire dans des fichiers nationaux tous les transferts qui seront effectués entre leur territoire et des pays tiers.

7 – Les règles d'entreprise contraignantes doivent-elles être exposées dans un document unique qui consacre l'ensemble des obligations du groupe et des droits des individus?

Les autorités de protection des données pourraient beaucoup plus facilement examiner les règles d'entreprise contraignantes - lesquelles seraient aussi plus transparentes pour les personnes concernées - s'il existait un document exposant clairement l'ensemble des obligations et des droits. Ce document devrait, si nécessaire, être accompagné d'une documentation complémentaire et pertinente (par exemple, concernant les politiques, les orientations, les programmes d'audit et de formation). Cette structure est proposée à titre d'exemple dans le document WP 154 adopté le 24 juin 2008 qui établit un cadre pour les règles d'entreprise contraignantes. Il n'est cependant pas obligatoire de faire figurer celles-ci dans un document unique.

8 – Quelle terminologie les demandeurs doivent-ils utiliser pour rédiger leurs règles d'entreprise contraignantes?

Les règles d'entreprise contraignantes étant un instrument qui produit des effets juridiques internes et externes, censé assurer un niveau de protection des données adéquat au regard de la directive 95/46/CE, il convient que les formulations et les définitions utilisées dans leurs principes de base (énoncés dans les documents WP 74, WP 108, WP 153 et WP 154) soient conformes aux formulations et définitions figurant dans ladite directive.
Toute mauvaise interprétation des règles d'entreprise contraignantes sera ainsi évitée et leur compréhension aisée aidera le demandeur à obtenir une autorisation auprès de l'autorité de protection des données.
Cela n'empêche pas les entreprises d'utiliser d'autres formulations – ayant toutefois la même signification – si elles sont plus facilement compréhensibles par leur personnel et leurs clients chargés de transposer ces règles d'entreprise contraignantes dans le cadre de politiques du groupe ou de directives internes.

9 – Quels droits doivent être conférés aux personnes en vertu de la clause relative aux droits de tiers bénéficiaires?

Toute personne dont les données à caractère personnel font l'objet d'un traitement dans le cadre des règles d'entreprise contraignantes peut faire valoir les principes suivants - établis par ces règles et qui ont valeur de droits - devant l'autorité de protection des données ou la juridiction compétente conformément aux règles définies dans les documents WP 74, WP 108 et WP 153, afin de former un recours et d'obtenir réparation si un membre du groupe a manqué à ses obligations et ne respecte pas ces principes.

Concrètement, les principes dont on peut se prévaloir au titre des droits de tiers bénéficiaires sont les suivants:

- limitation des finalités (WP 153 point 6.1, WP 154 point 3),
- qualité des données et proportionnalité (WP 153 point 6.1, WP 154 point 4),
- critères de légitimation du processus (WP 154 points 5 et 6),
- transparence et accessibilité des règles d'entreprise contraignantes (WP 153 points 6.1 et 1.7, WP 154 point 7),
- droits d'accès, de rectification, d'effacement et de verrouillage des données, et objet du traitement (WP 153 point 6.1, WP 154 point 8),
- droits en cas de décisions individuelles automatisées (WP 154 point 9),
- sécurité et confidentialité (WP 153 point 6.1, WP 154 points 10 et 11),
- restrictions aux transferts ultérieurs en dehors du groupe (WP 153 point 6.1, WP 154 point 12),
- législation nationale empêchant le respect des règles d'entreprise contraignantes (WP 153 point 6.3, WP 154 point 16),
- droit de porter plainte par l'intermédiaire du mécanisme interne de réclamation des entreprises (WP 153 point 2.2, WP 154 point 17),
- devoir de coopération avec l'autorité de protection des données (WP 153 point 3.1, WP 154 point 20),
- responsabilité et voies de recours (WP 153 points 1.3 et 1.4, WP 154 points 18 et 19).

Les entreprises doivent veiller à ce que l'ensemble de ces droits soient inclus dans la clause relative aux droits de tiers bénéficiaires qui figure dans leurs règles d'entreprise contraignantes, par exemple en faisant référence aux clauses/sections/parties desdites règles qui consacrent ces droits ou en les énonçant tous dans ladite clause.

Ces droits ne s'étendent pas aux éléments des règles d'entreprise contraignantes qui relèvent de mécanismes internes appliqués au sein d'entités, tels que le détail des actions de formation, les programmes d'audit, le réseau pour le contrôle du respect des règles et le mécanisme de mise à jour des règles [WP 153 points 2.1, 2.3, 2.4 et 5.1, WP 154 points 13 à 15 et point 21].

10 – Quelle relation y a-t-il entre les législations relatives à la protection des données en vigueur dans l'EEE et les règles d'entreprise contraignantes?

Les règles d'entreprise contraignantes ne remplacent pas les législations relatives à la protection des données qui s'appliquent au traitement de données à caractère personnel dans les États membres de l'EEE. Bien que ces règles fournissent des garanties adéquates pour les transferts de données à caractère personnel, il n'y a pas lieu de les considérer comme un instrument qui remplace lesdites législations. En effet, toute autorisation donnée par un État membre de l'EEE en vertu de l'article 26, paragraphe 2, de la directive 95/46/CE porte exclusivement sur des transferts internationaux effectués par un État membre de l'EEE vers un ou plusieurs pays tiers et n'atteste donc pas que des activités de traitement qui se déroulent au sein de l'EEE sont conformes aux législations en vigueur dans l'EEE en matière de protection des données.

11 – Que signifie le renversement de la charge de la preuve en pratique?

Si une personne concernée peut démontrer avoir subi un préjudice et établir les faits prouvant que ce préjudice est très probablement le résultat d'une violation des règles d'entreprise contraignantes, il appartient au membre européen du groupe qui a accepté d'assumer la responsabilité en la matière de prouver que le membre non européen du groupe n'est pas responsable de la violation qui est à l'origine du préjudice, ou qu'aucune violation n'a été commise.

Fait à Bruxelles, le 24.6.2008

Pour le groupe de travail
Le président
Alex TÜRK

Révisé en dernier lieu et adopté le 8.4.2009

Pour le groupe de travail
Le président
Alex TÜRK