Groupe de travail «Article 29» sur la protection des données

1271-00-01/08/FR
WP 154

Document de travail établissant un cadre pour la structure des règles d'entreprise contraignantes

Adopté le 24 juin 2008

INTRODUCTION

Le groupe de travail a déjà établi que les transferts internationaux de données à caractère personnel à partir de l'UE effectués entre filiales d'un même groupe peuvent avoir lieu sur la base des règles d'entreprise contraignantes (BCR) et a fourni des orientations quant aux éléments indispensables de ces règles dans les documents WP74[1] et WP108[2].

Pour continuer à aider les groupes d'entreprises et à les guider dans l'élaboration de règles d'entreprise contraignantes, le groupe de travail a élaboré le document ci-après qui laisse entrevoir ce à quoi ces règles pourraient ressembler si elles intégraient tous les éléments indispensables décrits dans les documents WP 74[3] et WP 108[4].

[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] 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.

[3] Cf. note de page 1.

[4] Cf. note de page 2.

Un cadre pour les règles d'entreprise contraignantes (BCR)

AVERTISSEMENT

Le présent cadre conçu pour les règles d'entreprise contraignantes n'est pas un modèle de BCR; il s'agit d'une simple proposition quant au contenu et à la façon dont les règles pourraient être structurées en un document unique qui peut être rendu contraignant pour le groupe d'entreprises.

Les règles d'entreprise contraignantes devraient être adaptées afin de prendre en compte la structure du groupe auquel elles s'appliquent, les opérations de traitement que les filiales effectuent et les politiques et procédures qu'elles mettent en œuvre pour protéger les données à caractère personnel. Par conséquent, veuillez noter que les autorités de protection des données n'accepteront aucun «copier – coller» du présent cadre.

Les règles d'entreprise contraignantes constitueront en effet pour votre groupe une politique de protection de la vie privée en ce qui concerne les transferts internationaux de données personnelles à partir de l'UE et pourraient s'appliquer à toutes les données personnelles traitées par les filiales du groupe dans le monde entier.

Introduction

- Obligation explicite faite à toutes les filiales du groupe et aux employés de respecter les règles d'entreprise contraignantes.
- Engagement pris par le conseil d'administration de l'entreprise en vue d'assurer le respect des règles décrites.
- Objectifs des règles d'entreprise contraignantes (fournir une protection adéquate pour les transferts et le traitement des données personnelles par le groupe).
- Référence aux textes applicables relatifs à la protection des données (directives européennes 95/46/CE et 2002/58/CE).

1 – Champ d'application

Description du champ d'application des règles d'entreprise contraignantes et, notamment:

- de leur applicabilité aux transferts et aux traitements au sein du groupe,
- de leur portée géographique (s'appliquent uniquement aux données traitées à l'intérieur de l'UE et transférées en dehors de l'UE ou à toutes les données),
- de leur champ d'application matériel (par exemple, type de traitement: automatique/manuel, nature des données: clients/RH/fournisseurs).

Description des flux des données et des finalités du traitement, y compris:

- de la nature des données transférées,
- des finalités du transfert/traitement,

- des importateurs/exportateurs des données dans l'UE et en dehors de l'UE[5].

2 – Définitions

Description des principaux termes et définitions:

- principales définitions (données à caractère personnel, données sensibles, personne concernée, responsable du traitement, sous-traitant, traitement, tiers, autorités de protection des données),
- d'autres définitions pertinentes pourraient être reprises dans un glossaire, telles que celles des termes suivants: exportateur de données, importateur de données, siège européen/filiale européenne responsable par délégation, filiales[6], délégué/instance chargé(e) de la protection des données,
- engagement à interpréter les termes figurant dans les règles d'entreprise contraignantes conformément aux directives européennes 95/46/CE et 2002/58/CE.

3 – Limitation des finalités

Description des finalités des traitements et des transferts de données et confirmation de ce que:

- les données personnelles seront transférées et traitées à des fins précises et légitimes,
- les données personnelles ne subiront pas de traitement ultérieur incompatible avec ces finalités,
- des garanties supplémentaires couvriront les données sensibles, comme le prévoit la directive européenne 95/46/CE.

4 – Qualité des données et proportionnalité

Engagements suivants:

- les données personnelles doivent être exactes et, au besoin, mises à jour,
- les données personnelles doivent être adéquates, pertinentes et leur volume ne doit pas être excessif au regard des finalités pour lesquelles elles sont transférées et traitées,
- le traitement des données personnelles ne sera pas appliqué plus longtemps que nécessaire au regard des finalités pour lesquelles elles sont collectées et traitées.

5 – Base juridique du traitement des données à caractère personnel

Les données personnelles doivent être traitées sur la base des éléments suivants:

- la personne concernée a donné son accord explicite, ou
- le traitement est indispensable à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci, ou
- le traitement est nécessaire au respect d''une obligation légale à laquelle le responsable du traitement est soumis, ou

[5] Veuillez noter que certaines autorités de protection des données peuvent demander une description plus détaillée des transferts et du traitement.

[6] Une filiale peut agir en qualité de responsable du traitement, sous-traitant, exportateur de données ou importateur de données.

- le traitement est nécessaire pour la sauvegarde des intérêts vitaux de la personne concernée, ou
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées, ou
- le traitement est nécessaire aux fins d'un intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

6 – Base juridique du traitement des données sensibles

Le traitement des données sensibles est interdit, à l'exception des cas où:

- la personne concernée a donné son consentement explicite au traitement des données sensibles en question, sauf dans les cas où la législation l'interdit, ou
- le traitement est nécessaire aux fins du respect des obligations et droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates, ou
- le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée serait dans l'incapacité physique ou juridique de donner son consentement, ou
- le traitement est effectué par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale dans le cadre de leurs activités légitimes et avec des garanties appropriées, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers en rapport avec les objectifs poursuivis par celui-ci et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées, ou
- le traitement porte sur des données sensibles manifestement rendues publiques par la personne concernée, ou
- le traitement des données sensibles est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice, ou
- le traitement des données sensibles est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de la gestion de services de santé, dans la mesure où le traitement de ces données est effectué par un praticien de la santé soumis au secret professionnel en vertu du droit national ou de réglementations arrêtées par les autorités nationales compétentes, ou par une autre personne également soumise à une obligation de secret équivalente.

7 – Transparence et droit à l'information

Engagement à rendre les règles d'entreprise contraignantes aisément accessibles à toute personne concernée.

En outre, les règles d'entreprise contraignantes décrivent comment les personnes concernées sont informées du transfert et du traitement de leurs données personnelles.

Engagement à communiquer aux personnes concernées les informations ci-après préalablement au traitement de leurs données:

- identité du ou des responsables du traitement et, le cas échéant, de son représentant;

- finalités du traitement auquel les données seront soumises;
- toute information supplémentaire telle que:
  i) les destinataires ou les catégories de destinataires des données,
  ii) l'existence d'un droit d'accès des personnes concernées aux données les concernant et d'un droit de rectification de ces données,

dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations supplémentaires sont nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données.

Si les données n'ont pas été fournies par la personne concernée, l'obligation d'informer celle-ci ne s'applique pas si l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés, ou si la législation prévoit expressément l'enregistrement ou la communication des données.

8 – Droits d'accès, de rectification, d'effacement et de verrouillage des données:

Engagement selon lequel:

- toute personne a le droit d'obtenir une copie de toutes les données traitées la concernant, sans contrainte, à des intervalles raisonnables, et sans délais ou frais excessifs,
- toute personne concernée a le droit d'obtenir la rectification, l'effacement ou le verrouillage de données, notamment au motif que les données sont incomplètes ou inexactes,
- toute personne concernée a le droit de s'opposer à tout moment, pour des raisons pour des raisons impérieuses et légitimes tenant à sa situation particulière, à ce que des données le concernant fassent l'objet d'un traitement, sauf en cas de disposition contraire du droit national. Si l'opposition est justifiée, le traitement doit être interrompu,
- toute personne concernée a le droit de s'opposer, sur simple demande et sans frais, au traitement de données la concernant à des fins de démarchage direct.

Explication sur la façon dont les personnes concernées peuvent avoir accès à leurs données personnelles.

9 – Décisions individuelles automatisées

Engagement selon lequel aucune évaluation ou décision en rapport avec la personne concernée et de nature à l'affecter de manière significative ne sera fondée uniquement sur le traitement automatisé de ses données, sauf si la décision en question:

- est prise en vue de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion ou d'exécution du contrat, introduite par la personne concernée, ait été satisfaite, ou que des mesures appropriées, telles que la possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime, ou
- est autorisée par une loi qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée.

10 – Sécurité et confidentialité

Engagement selon lequel les mesures d'ordre technique et organisationnel appropriées seront prises pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données via un réseau, ainsi que contre toute autre forme de traitement illicite.

Compte tenu des technologies de pointe et des coûts liés à la mise en œuvre de ces mesures, celles-ci doivent assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.

À cet égard, des mesures de sécurité accrues doivent être appliquées lors du traitement de données sensibles.

11 – Relations avec les sous-traitants qui sont des filiales du groupe

Explications sur la façon dont les données personnelles sont protégées lorsqu'il est fait appel à un sous-traitant qui est une filiale du groupe. Il s'agit notamment d'exiger que:

- le responsable du traitement choisisse un sous-traitant fournissant des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer et veille au respect de ces mesures;
- le responsable du traitement fournisse au sous-traitant des instructions par contrat conforme à la législation applicable, ce contrat stipulant notamment:
  i) que le sous-traitant n'agit que sur seule instruction du responsable du traitement,
  ii) que les obligations en matière de sécurité et de confidentialité incombent au sous-traitant.

12 – Restrictions aux transferts et aux transferts ultérieurs à des responsables du traitement et à des sous-traitants externes (qui ne sont pas des filiales du groupe)

Description des mesures mises en œuvre pour restreindre les transferts ou les transferts ultérieurs à l'extérieur du groupe et engagement selon lequel:

- les sous-traitants externes établis dans l'UE ou dans un pays reconnu par la Commission européenne comme garantissant un niveau adéquat de protection seront liés par contrat écrit stipulant que le sous-traitant n'agit que sur seule instruction du responsable du traitement et est responsable de la mise en œuvre des mesures de sécurité et de confidentialité adéquates;
- tous les transferts de données à des responsables de traitement externes établis à l'extérieur de l'UE doivent être conformes aux règles communautaires relatives aux flux de données transfrontaliers (articles 25-26 de la directive 95/46/CE: en utilisant, par exemple, les clauses contractuelles types de l'UE approuvées par les décisions 2001/497/CE ou 2004/915/CE de la Commission ou d'autres moyens contractuels adéquats conformément aux articles 25 et 26 de la directive européenne);
- tous les transferts de données à des sous-traitants externes établis à l'extérieur de l'UE doivent respecter les règles relatives aux sous-traitants (articles 16-17 de la directive 95/45/CE), outre les règles concernant les flux transfrontaliers de données (articles 25-26 de la directive 95/46/CE).

13 – Programme de formation

Engagement à dispenser une formation adéquate en matière de règles d'entreprise contraignantes au personnel ayant un accès permanent ou régulier aux données personnelles, et associé à la collecte des données personnelles ou au développement d'outils servant au traitement des données personnelles.

14 – Programme d'audit

Engagement à effectuer des audits concernant le respect des règles d'entreprise contraignantes au sein du groupe, et notamment sur les points suivants:

- le programme d'audit couvre tous les aspects des règles d'entreprise contraignantes, y compris les méthodes visant à garantir que des mesures correctives seront mises en œuvre;
- ces audits sont menés régulièrement (préciser la fréquence) par des contrôleurs internes ou externes agréés ou à la demande expresse d'un délégué à la protection des données/d'une instance de protection de la vie privée (ou de toute autre instance au sein du groupe);
- les résultats de tous les audits sont communiqués au délégué à la protection des données/à l'instance de protection de la vie privée (ou toute autre instance compétente au sein du groupe) et au conseil d'administration;
- les autorités de protection des données peuvent recevoir une copie de ces audits, sur demande;
- le plan d'audit doit permettre aux autorités de protection des données de réaliser elles-mêmes des audits sur la protection des données, si besoin est;
- chacune des filiales du groupe consent à se soumettre aux audits réalisés par les autorités de protection des données et s'engage à suivre les conseils des autorités en question sur tout ce qui touche à ces règles.

15 – Respect des règles et contrôle de leur application

Engagement à désigner le personnel nécessaire (tel qu'un réseau de responsables de la protection des données), assisté par la direction, afin de surveiller et de garantir le respect des règles.

Une brève description de la structure interne, du rôle et des compétences du réseau, des responsables de la protection des données, ou de la fonction similaire créée en vue de garantir le respect des règles. Il peut être par exemple prévu que le haut responsable de la protection des données remplit une fonction de conseil auprès de l'organe de direction, traite les demandes des autorités de protection des données, établit des rapports annuels sur le respect des règles, garantit le respect des règles au niveau global, et que les délégués à la protection des données soient chargés de traiter des réclamations émanant des personnes concernées, de soumettre des rapports sur des questions importantes liées à la protection des données au haut responsable de la protection des données, et de garantir le respect des règles au niveau local.

16 – Actions dans le cas où la législation nationale entrave le respect des règles d'entreprise contraignantes

Engagement clair selon lequel, lorsqu'une filiale du groupe a des raisons de croire que la législation qui lui est applicable risque de l'empêcher de remplir ses obligations en vertu des règles d'entreprise contraignantes et d'avoir un impact négatif sur les garanties fournies, ladite filiale en informera immédiatement le siège européen du groupe ou la filiale européenne responsable par délégation de la protection des données ou tout autre délégué/instance chargé(e) de la confidentialité des données (à moins que cela ne soit interdit par une autorité chargée d'assurer le respect de la loi, comme, par exemple, une interdiction prévue par le code pénal pour préserver le secret de l'instruction).

En outre, un engagement doit être prévu, selon lequel, en cas de conflit entre la législation nationale et les engagements en vertu des règles, le siège européen, la filiale européenne responsable par délégation de la protection des données, ou un autre délégué/instance chargé(e) de la confidentialité prendra une décision responsable sur l'action à entreprendre et, en cas de doute, consultera les autorités compétentes en matière de protection des données.

17 – Mécanismes internes de réclamation

Engagement à instaurer un système interne de traitement des plaintes dans le cadre duquel:

- toute personne concernée doit pouvoir introduire une plainte indiquant qu'une filiale du groupe ne respecte pas les règles;
- les plaintes doivent être traitées par un département ou une personne clairement identifié(e) disposant d'un degré approprié d'indépendance dans l'exercice de ses fonctions.

18 – Droits de tiers bénéficiaires

Déclaration claire selon laquelle les règles d'entreprise contraignantes accordent aux personnes concernées des droits en matière d'application des règles en tant que tiers bénéficiaires. Parmi ces droits doivent figurer un droit de recours en cas de violation des droits garantis et un droit à réparation (cf. articles 22 et 23 de la directive européenne).

Déclaration selon laquelle la personne concernée peut choisir d'introduire une plainte auprès:

- de la juridiction de l'exportateur des données établi dans l'UE, ou
- de la juridiction du siège européen/de la filiale européenne responsable par délégation, ou
- des autorités compétentes en matière de protection des données.

Engagement prévoyant que toutes les personnes concernées bénéficiant de droits de tiers bénéficiaires devraient également avoir facilement accès à cette clause.

19 - Responsabilité

Engagement selon lequel:

- le siège européen ou la filiale européenne responsable[7] par délégation de la protection des données accepte d'endosser la responsabilité et de prendre les mesures nécessaires pour réparer les actes commis par d'autres filiales du groupe établies en dehors de l'UE et de verser une indemnité pour tout préjudice résultant de la violation des règles d'entreprise contraignantes par les filiales;
- c'est au siège européen ou à la filiale européenne responsable par délégation de la protection des données que revient la charge de prouver que la filiale établie en dehors de l'UE n'est pas responsable de la violation ayant abouti à la demande de réparation.

Si le siège européen ou la filiale européenne responsable par délégation de la protection des données est en mesure de prouver que la filiale en dehors de l'UE n'est pas responsable de la violation, il (elle) pourra être dégagé(e) de toute responsabilité.

20 – Entraide et coopération avec les autorités de protection des données

Engagement selon lequel:

- les filiales coopèrent et s'entraident pour la gestion des demandes ou des plaintes de particuliers, ou des enquêtes ou demandes d'informations émanant d'autorités de protection des données;
- les entités appliquent les conseils des autorités de protection des données portant sur l'interprétation des règles d'entreprise contraignantes.

21 – Mises à jour des règles

Engagement à communiquer à toutes les filiales du groupe et aux autorités de protection des données toute modification significative apportée aux règles d'entreprise contraignantes ou à la liste des filiales, visant à prendre en compte les modifications de l'environnement réglementaire et de la structure d'entreprise et, stipulant plus exactement que:

- certaines modifications peuvent exiger la délivrance d'une nouvelle autorisation par les autorités de protection des données;
- les mises à jour des règles d'entreprise contraignantes ou de la liste des filiales soumises aux règles d'entreprise contraignantes sont possibles sans qu'il soit nécessaire d'introduire une nouvelle demande d'autorisation, moyennant le respect des conditions suivantes:

[7] S'il n'est pas possible pour certains groupes, dont la structure d'entreprise est particulière, d'imposer à une entité d'assumer la totalité de la responsabilité des violations des BCR en dehors de l'UE, les autorités de protection des données peuvent accepter d'autres mécanismes de responsabilité, définis au cas par cas, s'ils permettent de s'assurer de façon satisfaisante que les personnes concernées pourront faire valoir leurs droits et qu'elles ne seront pas désavantagées dans ce processus. Parmi les régimes possibles de responsabilité figurent le mécanisme de responsabilité solidaire entre les importateurs de données et les importateurs de données, prévu dans les clauses contractuelles types de établies dans la décision 2001/497/CE de la Commission du 15 juin2001, ou le régime de responsabilité reposant sur des obligations de diligence telles que fixées dans les clauses contractuelles types visées dans la décision 2004/915/CE de la Commission du 27 décembre 2004. Une dernière possibilité, concernant en particulier les transferts effectués par des responsables de traitement vers des sous-traitants, consiste à appliquer le mécanisme de responsabilité prévu dans les clauses contractuelles types visées dans la décision 2002/16/CE de la Commission du 27 décembre 2001.

i) une personne désignée actualise la liste des filiales soumises aux règles d'entreprise contraignantes, enregistre et consigne toute mise à jour des règles, et fournit les informations requises aux personnes concernées ou aux autorités de protection des données, à leur demande;
ii) aucun transfert n'est effectué vers une nouvelle filiale tant que celle-ci n'est pas véritablement liée par les règles contraignantes et tant qu'elle n'est pas en mesure de garantir leur respect;
iii) toute modification des règles ou de la liste des filiales, assortie d'un bref exposé des motifs justifiant cette mise à jour, doit être notifiée une fois par an aux autorités de protection des données délivrant les autorisations.

Engagement selon lequel toute modification substantielle des règles sera également communiquée aux personnes concernées.

22 - Liens entre la législation nationale et les règles d'entreprise contraignantes

Explication selon laquelle:
- si la législation locale - par exemple, la législation communautaire - exige un degré supérieur de protection des données personnelles, celle-ci prime sur les règles d'entreprise contraignantes;
- dans tous les cas, les données seront traitées conformément au droit applicable visé à l'article 4 de la directive 95/46/CE, ainsi qu'à la législation locale pertinente.

23 – Dispositions finales

- Date d'entrée en vigueur
- Période de transition

Documentation à fournir aux autorités de protection des données

1 - Le formulaire de demande établi dans le document WP133.
2 - Toute documentation permettant de démontrer que les engagements figurant dans les règles d'entreprise contraignantes sont respectés, par exemple:

- politiques en matière de protection de la vie privée par type de traitement (par exemple., politique de protection de la vie privée des clients, des RH) destinées à informer les personnes concernées (par exemple, les clients, les employés) sur les mesures prises par l'entreprise pour protéger leurs données à caractère personnel;
- lignes directrices destinées aux employés ayant accès aux données à caractère personnel et leur facilitant la compréhension et l'application des règles d'entreprise contraignantes (par exemple, lignes directrices sur la manière de répondre aux réclamations des personnes concernées, sur la transmission d'informations aux personnes concernées, sur les mesures à observer en matière de sécurité/confidentialité);
- un plan et un programme d'audit de la protection des données personnelles indiquant les personnes compétentes (contrôleurs internes/externes agréés de l'entreprise);
- exemples et/ou explication concernant le programme de formation;

- documentation prouvant que la filiale qui est à l'origine du transfert de données à l'extérieur de l'UE, ainsi que le siège européen ou la filiale européenne responsable par délégation de la protection des données disposent de ressources financières en suffisance pour couvrir le versement d'une indemnité en cas de violation des règles d'entreprise contraignantes;
- description du système interne de réclamation;
- liste des entités liées par les règles d'entreprise contraignantes;
- politique de sécurité applicable aux systèmes informatiques de traitement des données personnelles au sein de l'UE;
- processus de certification permettant de garantir que toutes les nouvelles applications logicielles de traitement de données communautaires sont conformes aux règles d'entreprise contraignantes;
- tout contrat type à utiliser dans les relations avec les sous-traitants (filiales ou non filiales du groupe) assurant le traitement de données communautaires;
- description du poste de délégué à la protection des donnés ou des autres personnes chargées de la protection des données au sein de l'entreprise.

Fait à Bruxelles, le 24.6.2008

Pour le groupe de travail
Le Président
Alex TÜRK