05/FR
WP108

Document de travail établissant une liste de contrôle type pour les demandes d'approbation des règles d'entreprise contraignantes

Adopté le 14 avril 2005

L'intervention des autorités chargées de la protection des données dans l'approbation des règles d'entreprise contraignantes est entièrement facultative[1] et peut être décidée au cas par cas. Aucune autorité n'est tenue de prendre part à une quelconque procédure visant à sanctionner de telles règles. La participation d'autorités non habilitées à permettre des transferts internationaux de données consistera à adresser un avis favorable, le cas échéant, à l'autorité nationale compétente pour autoriser de tels transferts.

Les éléments décrits dans le présent document sont, sans aucun doute, très importants; ils ne sont toutefois pas immuables, et le groupe de travail créé en vertu de l'article 29 est susceptible de réexaminer ledit document à la lumière de l'expérience acquise. Les entreprises sont invitées à utiliser la liste de contrôle figurant ci-après lorsqu'elles soumettent des règles d'entreprise contraignantes aux autorités nationales chargées de la protection des données. Elles devront également tenir compte du fait que les règles proposées pourront devoir être complétées afin de satisfaire aux exigences pertinentes des systèmes juridiques nationaux, notamment pour ce qui est des moyens envisagés afin que les personnes concernées puissent faire valoir leurs droits conformément à ces règles.

Les aspects qui ne sont pas couverts par la liste de contrôle type seront examinés et traités avec les autorités concernées à l'occasion des consultations courantes menées dans le cadre de la procédure de coopération. Cette liste est conçue de façon à couvrir toutes les exigences énoncées dans le document n° 74 du groupe de travail «Article 29»[2] («document WP74») et met l'accent sur les questions sur lesquelles les autorités de protection des données doivent se pencher lorsqu'elles examinent le caractère adéquat du niveau de protection offert à la lumière dudit document.

[1] Par «autorités chargées de la protection des données», il convient d'entendre les autorités chargées de la protection des données des États membres de l'UE et des pays de l'EEE

[2] Document de travail intitulé «Transferts de données personnelles vers des pays tiers: application de l'article 26, paragraphe 2, de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données», adopté le 3 juin 2003.

1. **À quoi sert cette liste de contrôle?**

2. La présente liste de contrôle vise à aider les groupes d'entreprises qui demandent l'approbation de leurs règles d'entreprise contraignantes et, en particulier, à fournir des précisions sur les exigences énoncées dans le document WP74[3].

3. **<u>À quelle autorité chargée de la protection des données devez-vous adresser votre demande?</u>**

   3.1. Si la société mère ou le siège d'exploitation de votre groupe relève du droit d'un État membre de l'UE, vous devez vous adresser à l'autorité chargée de la protection des données de cet État membre.

   3.2. Si le lieu d'implantation de la société mère ou du siège d'exploitation de votre groupe n'est pas clairement défini ou s'il est situé en dehors de l'UE, vous devez vous adresser à l'autorité chargée de la protection des données la plus appropriée au regard des critères définis ci-dessous.

   3.3. Au moment de déposer votre demande, vous devez expliquer en détail pourquoi l'autorité chargée de la protection des données à laquelle vous vous adressez est l'autorité la plus appropriée. Parmi les facteurs pris en considération pour déterminer si vous vous êtes adressé à l'autorité la plus appropriée figurent:

      3.3.1. le lieu d'implantation du siège européen de votre groupe;

      3.3.2. le lieu d'implantation de la société du groupe à laquelle les responsabilités en matière de protection des données ont été déléguées[4];

      3.3.3. le lieu d'implantation de la société qui est la mieux placée (en termes de fonction de gestion, de charge administrative, etc.) pour traiter la demande et mettre en œuvre les règles d'entreprise contraignantes au sein de votre groupe;

      3.3.4. le lieu où la plupart des décisions au regard des finalités et des moyens de traitement sont prises; et

      3.3.5. les États membres de l'UE d'où proviendront la majorité des transferts de données vers des pays en dehors de l'EEE.

   3.4. La priorité sera donnée au point 3.3.1. ci-dessus.

   3.5. Il ne s'agit pas de critères formels. L'autorité chargée de la protection des données à laquelle vous vous adressez aura toute discrétion pour décider si elle est, de fait, l'autorité la plus appropriée; en tout état de cause, les autorités chargées de la protection des données pourront décider entre elles de transmettre

[3] Le document WP74 définit les exigences relatives aux règles d'entreprise contraignantes.

[4] Conformément au document n° 74 du groupe de travail créé en vertu de l'article 29, si le siège du groupe n'est pas implanté dans l'UE/l'EEE, celui-ci doit déléguer à une filiale européenne les responsabilités en matière de protection des données, en la chargeant de veiller à ce que chacune de ses filiales étrangères adapte ses opérations de traitement en fonction des engagements qu'il a pris, collabore au besoin avec l'autorité chef de file et verse des indemnités en cas de dommages résultant d'une infraction aux règles d'entreprise contraignantes de la part de l'une quelconque de ses filiales

votre demande à une autorité chargée de la protection des données autre que celle à laquelle vous vous êtes adressé.

4. Quels renseignements devez-vous communiquer?

4.1. Vous devez fournir:

4.1.1. un document distinct indiquant:

4.1.1.1. les coordonnées des responsables au sein de votre entreprise auxquels des demandes peuvent être adressées, et

4.1.1.2. tous les renseignements pertinents de nature à justifier le choix de l'autorité chargée de la protection des données, notamment la structure fondamentale de votre groupe ainsi que la nature et la structure des opérations de traitement dans l'UE/l'EEE, eu égard en particulier au(x) lieu(x) où sont prises les décisions, la localisation des filiales dans l'UE, les moyens et finalités du traitement, les lieux à partir desquels les transferts à destination de pays tiers sont opérés, de même que les pays tiers à destination desquels les données sont transférées (renseignements que le «point d'entrée» communiquera aux autorités de protection des données concernées);

4.1.2. un document de référence exposant brièvement comment les critères énoncés dans le document WP74 (exposés ci-dessous) ont été respectés (ceci aidera les autorités chargées de la protection des données à définir les sections pertinentes des documents que vous fournissez);

4.1.3. tous les documents pertinents qui contiennent les «règles d'entreprise contraignantes» devant être adoptées par votre entreprise (par exemple, les politiques, codes, avis, procédures et contrats susceptibles d'avoir un rapport avec la demande). De même qu'une déclaration de principes générale, les autorités chargées de la protection des données doivent connaître les modalités effectives de traitement des données à caractère personnel au sein de votre groupe;

4.1.4. il convient de noter que, bien que les autorités de protection des données soient tenues, conformément à leur législation nationale, de ne pas divulguer sans autorisation légale des renseignements fournis par un responsable du traitement des données dans le cadre du processus d'autorisation, certaines d'entre elles sont également soumises à la législation sur la liberté d'information. En conséquence, si un document transmis à l'appui de votre demande d'autorisation contient des informations commerciales sensibles, vous devez le signaler de façon appropriée. Toutefois, la décision de divulguer ou non des informations sera prise par chaque autorité de protection des données concernée conformément à la législation de son pays relative à la liberté d'information. De même, les renseignements nécessaires pour permettre aux autres autorités de protection des données concernées de procéder à l'appréciation des règles d'entreprise contraignantes devront être diffusés.

5. **Preuves du caractère juridiquement contraignant des mesures:**

5.1. Les règles doivent avoir un caractère contraignant à la fois

5.1.1. au sein de l'entreprise, et

5.1.2. à l'extérieur de celle-ci, dans l'intérêt des individus.

5.2. Cette exigence peut être respectée de diverses façons, en fonction de la structure et de la taille de votre entreprise et des procédures adoptées concernant d'autres exigences réglementaires auxquelles votre entreprise est éventuellement soumise. Cela dépendra aussi de la législation nationale des États membres où est implantée votre entreprise.

5.3. **Caractère contraignant au sein de l'entreprise**

5.4. **De quelle façon les règles sont-elles contraignantes entre les différentes composantes de l'entreprise?**

5.5. Vous devez veiller à ce que les autres filiales du groupe respectent les règles d'entreprise contraignantes. Cet aspect est particulièrement important en l'absence de «siège» ou lorsque le siège est situé en dehors de l'EEE. La méthode dépendra de la structure de votre entreprise, mais également de la législation nationale des États membres dans lesquels votre entreprise est implantée.

5.6. Les éléments suivants sont des suggestions quant à la façon dont un ensemble de règles d'entreprise peuvent être rendues contraignantes pour une entreprise; il se peut toutefois qu'il existe d'autres moyens mieux adaptés aux dispositions envisagées:

5.6.1. règles d'entreprise contraignantes ou règles contractuelles pouvant être imposées aux autres filiales du groupe;

5.6.2. déclarations ou engagements unilatéraux pris ou donnés par la société mère qui sont contraignants pour les autres filiales du groupe;

5.6.3. incorporation d'autres mesures réglementaires, telles que des obligations figurant dans des codes légaux dans un cadre juridique défini; ou encore

5.6.4. incorporation des règles à l'intérieur des principes généraux d'activité d'une entreprise, avec à l'appui des politiques, audits et sanctions appropriés.

5.7. Toutes les suggestions qui précèdent peuvent ne pas avoir le même effet dans chaque État membre. Par exemple, de simples déclarations unilatérales ne sont pas considérées comme contraignantes dans certains États membres. Vous devrez donc vous faire conseiller au niveau local si vous avez l'intention de fonder votre action sur de telles déclarations.

Veuillez expliquer de quelle façon les règles sont contraignantes pour les filiales du groupe.

5.8. **Comment les règles sont-elles rendues contraignantes pour les salariés?**

5.9. Les salariés doivent être tenus au respect des règles, par exemple par le biais d'obligations spécifiques figurant dans un contrat de travail ou de la subordination du respect des règles à des procédures disciplinaires. Il convient en outre d'élaborer des programmes de formation adéquats et d'impliquer le personnel d'encadrement. Le titre de la personne responsable en dernier recours du respect des règles devra également être indiqué.

Veuillez expliquer comment les règles sont contraignantes pour les salariés au sein de votre entreprise, ainsi que les sanctions prévues en cas de non-respect desdites règles.

5.10. **Comment les règles sont-elles rendues contraignantes pour les sous-traitants chargés du traitement des données?**

5.11. Vous devez indiquer comment vos règles d'entreprise contraignantes sont rendues contraignantes pour les sous-traitants. Veuillez fournir des preuves du type de conditions contractuelles imposées aux sous-traitants et expliquer ce que prévoient les contrats en cas de non-respect desdites règles.

Veuillez préciser de quelle façon les règles sont contraignantes pour les sous-traitants et les sanctions appliquées en cas de non-respect desdites règles.

5.12. **Comment les règles sont-elles contraignantes à l'extérieur dans l'intérêt des individus?**

5.13. Les personnes entrant dans le champ d'application des règles d'entreprise contraignantes doivent être en mesure de faire respecter ces règles à la fois par les autorités chargées de la protection des données et par les tribunaux.

5.14. Ces personnes doivent être en mesure de déposer des réclamations auprès de la juridiction compétente dont relève:

5.14.1. la filiale du groupe à l'origine du transfert, ou

5.14.2. le siège dans l'UE ou la filiale européenne du groupe compétente en matière de protection des données.

5.15. Veuillez indiquer dans votre demande les démarches pratiques qu'une personne concernée peut entreprendre pour obtenir un recours auprès de votre entreprise, notamment en ce qui concerne le traitement des réclamations.

5.16. Par exemple, si votre siège et l'autorité chef de file se trouvent en Belgique et que l'une des sociétés de votre groupe en Italie enfreint vos règles d'entreprise, la personne concernée doit savoir qu'elle peut déposer une réclamation contre l'entreprise en infraction en Italie et/ou contre le siège en Belgique.

5.17. Votre demande doit contenir une confirmation du fait que le siège européen de l'entreprise ou la partie de l'entreprise compétente en matière de protection des données dans l'UE possède des actifs suffisants ou a pris des dispositions appropriées pour permettre le versement d'une indemnité pour tout dommage résultant de la violation, par toute partie de l'entreprise, des règles d'entreprise contraignantes.

5.18. Vous devez indiquer la partie de l'entreprise responsable du traitement des réclamations, ainsi que les modalités de l'accès au processus de traitement des réclamations dont bénéficie la personne concernée.

5.19. Il doit être précisé dans votre demande que la charge de la preuve concernant l'infraction présumée incombe à la filiale du groupe à l'origine du transfert, au siège européen ou à la partie de l'entreprise compétente en matière de protection des données, indépendamment de l'endroit d'où provient la réclamation.

5.20. Votre demande doit prendre acte du fait qu'une personne concernée bénéficiera des droits accordés par la directive 95/46/CE.

5.21. Votre demande doit aussi comporter une confirmation du fait que vous coopérerez avec les autorités chargées de la protection des données en ce qui concerne toute décision prise par l'autorité de contrôle et que vous suivrez l'avis de l'autorité chargée de la protection des données sur l'interprétation du document WP74.

Veuillez préciser de quelle façon les règles sont contraignantes à l'extérieur.

6. Vérification du respect des règles

6.1. Le document WP74 indique que les règles d'entreprise contraignantes adoptées par une entreprise doivent prévoir le recours à des contrôleurs internes, à des contrôleurs externes ou à des contrôleurs tant internes qu'externes.

6.2. Le programme d'audit en matière de protection des données et le plan d'audit doivent être clairement exposés, soit dans un document exposant vos normes en matière de protection des données, soit dans d'autres documents de procédure interne, et les audits doivent être communiqués à toute autorité chargée de la protection des données qui en fait la demande. Cette autorité devra s'assurer que le programme d'audit couvre adéquatement les différents aspects des règles d'entreprise contraignantes, notamment les méthodes visant à garantir que des mesures correctives ont été mises en oeuvre. Le plan d'audit doit permettre à l'autorité de contrôle d'avoir toute latitude pour réaliser au besoin un audit de la protection des données.

6.3. Les autorités chargées de la protection des données ne souhaitent pas voir figurer dans les résultats de votre audit des éléments sans lien avec la protection des données. Elles ne se préoccupent pas de la gouvernance d'entreprise, sauf dans la mesure où celle-ci affecte le respect de la protection des données, et ne s'intéressent pas aux informations commerciales sensibles. Les renseignements fournis devront se limiter à ce qui est nécessaire pour se conformer au document WP74. Les autorités chargées de la protection des données sont toutefois conscientes de ce que des questions relatives au respect de la protection des données peuvent figurer dans des rapports contenant d'autres informations: dans certains cas, il peut s'avérer impossible de distinguer les éléments relatifs à la protection d'autres renseignements sans lien avec cette question.

6.4. Veuillez résumer vos dispositions en matière d'audit en ce qui concerne les questions liées à la protection des données et indiquer comment les rapports d'audit sont traités en interne au sein de votre entreprise (veuillez préciser les destinataires du rapport et leur position au sein de la structure de l'entreprise).

Veuillez présenter de façon détaillée votre programme d'audit sur la protection des données, ainsi que votre plan d'audit.

7. Description du traitement et des flux de l'information

7.1. Les règles d'entreprise contraignantes devront définir les éléments suivants:

7.1.1. la nature des données, à savoir si les règles d'entreprise contraignantes ne concernent qu'un type de données, par exemple les données sur les ressources humaines, ou si elles couvrent plusieurs types de données, et la façon dont cette question est traitée dans les règles d'entreprise contraignantes. En tout état de cause, la demande devra être suffisamment détaillée pour permettre à une autorité de contrôle de déterminer si les garanties mises en place sont adéquates pour la nature du traitement opéré;

7.1.2. les finalités du traitement des données;

7.1.3. l'étendue des transferts au sein du groupe qui sont couverts par les règles en question. Veuillez indiquer:

7.1.3.1. les différentes filiales du groupe à l'intérieur de l'UE à partir desquelles des données à caractère personnel sont susceptibles d'être transférées; et

7.1.3.2. les différentes filiales du groupe en dehors de l'EEE à destination desquelles des données à caractère personnel sont susceptibles d'être transférées.

7.2. Vous devez aussi indiquer si les règles d'entreprise contraignantes s'appliquent uniquement aux transferts à partir de l'UE ou si elles concernent la totalité des transferts entre les différentes filiales du groupe. Les autorités chargées de la protection des données doivent comprendre sur quelle base ont lieu les transferts

ultérieurs de données (c'est-à-dire les transferts de données à partir de filiales du groupe situées en dehors de l'EEE vers des tiers).

Veuillez décrire la nature des données, les finalités de leur traitement et l'étendue des transferts au sein du groupe.

8. Garanties concernant la protection des données

8.1. Les règles doivent décrire clairement les garanties types prévues en matière de protection des données conformément à la directive 95/46/CE et préciser comment ces exigences sont respectées au sein de votre entreprise.

8.2. Les règles d'entreprise contraignantes doivent en particulier porter sur les points suivants:

8.2.1. transparence et loyauté à l'égard des personnes concernées;

8.2.2. limitation des finalités;

8.2.3. garantie de la qualité des données;

8.2.4. sûreté;

8.2.5. droits des personnes en matière d'accès, de rectification et d'objection au traitement;

8.2.6. limitations concernant des transferts ultérieurs à l'extérieur de la société multinationale conformément aux règles (bien que de tels transferts soient possibles au titre d'autres dispositions facilitant les transferts).

Veuillez indiquer brièvement comment ces aspects ont été traités dans les règles d'entreprise contraignantes adoptées par votre entreprise, documents à l'appui (par exemple, politiques menées en la matière).

9. Modalités de communication et d'enregistrement des modifications

9.1. Il convient de mettre en place un système d'information des autres parties de l'entreprise et de l'autorité chargée de la protection des données en ce qui concerne les modifications apportées aux règles conformément au point 4.2 du document WP74. Les autorités chargées de la protection des données ne devront être informées de ces modifications que dans la mesure où elles affectent sensiblement le respect de la protection des données. Les modifications de nature administrative, par exemple, ne devront pas être notifiées, sauf si elles ont des répercussions pour le fonctionnement des règles d'entreprise contraignantes. Votre autorité chef de file vous indiquera les éventuelles exigences spécifiques relatives à la communication des modifications ou mises à jour aux autorités chargées de la protection des données.

Veuillez décrire les modalités de communication des modifications mises en œuvre par votre entreprise.

Fait à Bruxelles, le 14 avril 2005.

Pour le groupe de travail,
Le président,
Peter Schaar