

Résolution

7^{ème} Assemblée générale de l'AFAPDP du 22 novembre 2013 à Marrakech

Version du 6 février 2014

Résolution relative à la procédure d'encadrement des transferts de données personnelles de l'espace francophone au moyen de règles contraignantes d'entreprise (RCE)

Nous, membres de l'Association francophone des autorités de protection des données personnelles (AFAPDP), réunis à Marrakech le 22 novembre 2013 dans le cadre de la 7^{ème} Assemblée générale des commissaires à la protection des données de la Francophonie ;

Rappelant que l'Assemblée générale de l'AFAPDP a adopté en 2011 une résolution soutenant le projet de définir un référentiel de principes commun aux autorités francophones pour encadrer les transferts de données personnelles entre entreprises, et de développer une approche globale et harmonisée pour encadrer les transferts de données au sein de l'espace francophone ;

Constatant qu'il existe généralement un déficit d'échange d'informations entre les autorités membres quant à l'existence de transferts de données personnelles entre pays de l'espace francophone et quant à la nature des garanties qui les encadrent ;

Constatant que, même si les lois des pays membres de l'AFAPDP consacrent des protections fort similaires et si toutes les autorités membres de l'association présentent les meilleures qualités, les contextes économiques, sociaux et institutionnels respectifs des différents pays concernés ne permettent pas, a priori et de manière générale, de garantir dans l'ensemble de l'espace francophone l'existence d'une protection adéquate libérant dès lors les responsables du traitement de tout contrôle frontalier ;

Persuadés que ce constat ne fait toutefois pas obstacle à la mise sur pied d'un dispositif commun aux autorités francophones, organisant leur collaboration, afin d'encadrer de manière plus efficace les traitements transfrontaliers ;

Convaincus, qu'à cet égard, l'utilisation de règles contraignantes d'entreprise (RCE) propres à l'espace francophone reposant sur un mécanisme de conformité à un référentiel commun garantissant un niveau élevé de garanties et sur un mécanisme de coopération renforcée entre autorités, entre autres, est de nature à permettre à la fois la mise en œuvre d'une protection performante ainsi que des modalités pratiques plus accueillantes pour les entreprises ;

Convaincus que le référentiel commun ainsi reconnu par l'ensemble des autorités membres peut également être utilisé aux fins d'évaluer l'adéquation d'autres instruments juridiques visant à garantir la protection des données personnelles ;

Persuadés par ailleurs que l'organisation d'un dispositif simple de partage d'informations et de collaboration renforcée des autorités entre elles pour les transferts qui les concernent permettra à chaque autorité d'exercer ses missions en pleine connaissance de la réalité des traitements ;

Invitant les Etats auxquels les membres de l'association francophone des autorités de protection des données personnelles appartiennent à créer les bases légales nécessaires à permettre la mise en œuvre de cette coopération dans les meilleures conditions ;

A. Déclarons conjointement qu'il est nécessaire, afin d'assurer la meilleure protection possible des données personnelles lors de leur transfert de l'espace francophone par les entreprises, que les autorités de protection s'engagent à mettre en œuvre les principes de coopération suivants :

1. Instruction conjointe des garanties nécessaires aux transferts de données

Les autorités de protection s'engagent à coopérer aux fins d'instruire conjointement tout projet de RCE.

A la réception d'une telle demande, les autorités concernées désignent entre elles l'autorité qui sera le point de contact avec le responsable du traitement.

L'autorité qui sera le point de contact est désignée selon les critères suivants :

- lieu où se trouve la maison-mère du groupe ;
- le lieu où se trouve la société la mieux positionnée (en termes de gestion fonctionnelle, administrative, etc.) en vue de gérer l'application et de faire respecter les RCE dans le groupe ;
- le pays où la plupart des décisions en termes de finalités et moyens de traitement sont prises ;
- le pays à partir duquel a lieu le plus grand nombre de transfert de données ;
- à défaut d'établissement dans un pays membre adhérent de l'AFAPDP, lieu où se trouve la société ayant délégation de responsabilité en matière de protection des données personnelles.

L'autorité point de contact est le relais et coordinateur de la demande de RCE entre autorités. Elle examine la conformité au référentiel commun de l'outil contractuel soumis par l'entreprise, transmet le projet de RCE, à la demande de l'entreprise, aux autres autorités homologues concernées, recueille leurs éventuels commentaires, le finalise avec l'entreprise et communique aux autorités homologues le projet final.

Lorsqu'elles sont également tenues de délivrer une autorisation relative à ces transferts, les autorités concernées prennent en compte le travail d'analyse effectué par l'autorité point de contact dans leur processus de décision afin de pouvoir autoriser, sur cette base, les transferts de données à caractère personnel en vertu de la législation nationale applicable.

Les décisions par lesquelles une autorité de protection autorise ou éventuellement suspend un transfert de données vers un autre pays signataire sont notifiées à l'autorité de protection de données du pays en question et à l'autorité point de contact dans les meilleurs délais à compter de leur adoption.

En outre, chaque autorité de protection répond, dans les meilleurs délais à compter de sa réception, à la demande adéquatement motivée et légitime d'information formulée par une autre autorité, quant aux transferts sollicités, aux responsables du traitement, aux sous-traitants concernés et aux vérifications qu'elles ont pu effectuer quant à la matérialité des traitements concernés, dans le respect des obligations légales en matière de confidentialité qui leur sont applicables.

Dans un objectif de recherche de la meilleure efficacité du dispositif d'instruction conjointe, une autorité bénéficiant d'une plus grande expérience, en particulier en matière d'analyse et de validation de RCE, est associée à l'analyse de conformité.

A cet égard, les autorités les plus expérimentées se tiennent à la disposition des autres autorités en vue de l'organisation immédiate de formations au bénéfice de ces dernières. Ces formations peuvent porter sur les RCE.

En cas de besoin, toute autorité de protection des données concernée peut s'adresser au responsable du traitement pour obtenir toute information complémentaire qu'elle estime nécessaire à l'exercice de ses missions.

Dans le cas où le responsable de traitement disposerait déjà de RCE validées conformément au dispositif existant actuellement au sein de l'Union Européenne (BCR), l'analyse déjà réalisée par les autorités de protection compétentes pourrait être prise en compte par les autorités nationales concernées dans le cadre de leur procédure d'examen des RCE et de décision pour la délivrance de leurs éventuelles autorisations de transferts de données.

2. Coopération en matière de gestion conjointe des plaintes

Les autorités de protection s'engagent à coopérer aux fins de gestion des plaintes, dans le respect de leurs obligations légales et en garantissant le respect de la confidentialité des informations qui leur sont échangées.

3. Coopération aux fins de gestion conjointe des contrôles

Les autorités de protection s'engagent à coopérer aux fins de gestion des contrôles, dans le respect des obligations légales en matière de confidentialité qui leur sont applicables.

4. Respect des obligations légales en matière de confidentialité

Les autorités de protection s'engagent à échanger entre elles des informations utiles à la mise en œuvre des principes de coopération pour autant que leur droit interne ne s'y oppose pas. Sauf si celles-ci sont publiques, elles garantissent la confidentialité des informations échangées, notamment par des mesures techniques et organisationnelles.

L'échange de données à caractère personnel concernant les personnes dont les données sont transférées n'est autorisé qu'avec leur consentement explicite, libre et informé ou est indispensable à la gestion d'une plainte, conformément au droit national applicable.

L'autorité destinataire ne peut en aucun cas transmettre les informations ainsi reçues à une tierce personne, sauf autorisation préalable expresse de l'autorité communicatrice.

5. Interprétation et évaluation

Les dispositions de la présente résolution sont interprétées afin de les rendre conformes au droit national applicable à chaque autorité signataire, et le cas échéant, aux dispositions du Protocole de coopération.

Un mécanisme d'évaluation du dispositif de coopération est mis en place afin d'apprécier, notamment, l'impact de la mise en œuvre de la coopération sur la charge de travail respective des autorités signataires, notamment au moyen d'indicateurs statistiques, présentés et discutés lors d'une réunion de l'Association afin de débattre conjointement des éventuels problèmes rencontrés et des solutions qui pourraient y être apportées.

6. Clause de révision

A l'issue d'une période initiale de mise en œuvre de deux ans, l'effectivité des mécanismes d'instruction conjointe et de coopération est évaluée afin de décider de sa reconduction, ainsi que de la nécessité de réviser, le cas échéant, ses modalités.

B. Invitons dès lors individuellement les membres de l'Association :

- A convenir, entre eux, d'un protocole de coopération mettant en œuvre la présente déclaration et à exercer leurs compétences, missions et pouvoirs à l'occasion de transfert de données entre leurs Etats respectifs conformément aux dispositions de ce protocole, encadrées par les législations qui s'imposent à eux ;
- A prendre note de la possibilité qui leur est laissée de mettre fin à leur engagement pour des raisons sérieuses et légitimes, par voie de dénonciation en la forme d'une notification aux autorités signataires.

Annexe A : référentiel définissant les standards minimaux devant être respectés par tout transfert de données opérés dans le cadre de l'espace francophone (pays dont les autorités sont membres de l'AFAPDP¹)

Le présent référentiel commun fixe les éléments minimaux relatifs à la protection des données personnelles qui doivent être garantis et respectés lorsque des entreprises souhaitent mettre en œuvre des transferts de données personnelles et dont l'existence doit être constatée par les autorités de protection dans l'exercice de leurs compétences, notamment lors de décisions sur des demandes d'autorisation de transfert.

Il convient ainsi que les RCE assurant la conformité au présent référentiel et présentés par les entreprises, comportent une obligation explicite pour les sociétés exportatrices et importatrices de données personnelles (ainsi que leurs filiales) de respecter les règles décrites par le référentiel commun et une référence aux textes applicables relatifs à la protection des données (par exemple, pour les données en provenance d'un pays de l'Union européenne, les directives 95/46/CE et 2002/58/CE).

A. Champ d'application

Une description :

- Des transferts et traitements de données à caractère personnel couverts (nature des données, finalités des traitements et des transferts) ;
- De leur portée géographique (pays concernés par le(s) traitement(s) et le(s) transfert(s) de données personnelles) ;
- De leur champ d'application matériel (par exemple, catégories des données : relatives aux salariés, aux clients, ou aux fournisseurs, etc.)

B. Définitions

Une définition des principaux termes et définitions :

- Données à caractère personnel
- Données sensibles (dont les données de santé)
- Données judiciaires
- Personne concernée
- Responsable du traitement
- Sous-traitant
- Traitement de données à caractère personnel
- 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, groupe, siège, filiale, responsable par délégation, délégué/instance chargé(e) de la protection des données.

¹ Il est important de préciser ici que les entreprises sont libres de développer des RCE n'offrant pas le même niveau de garantie que celui ici proposé (et issu du référentiel exigible en matière de RCE). Toutefois, les entreprises qui choisiraient cette voie doivent avoir conscience qu'une telle option aurait pour conséquence que leurs RCE ne pourraient pas être utilisées pour procéder à des transferts de données depuis le territoire d'un Etat membre de l'UE vers un pays hors UE.

Concernant les données transférées hors de l'Union européenne, un engagement à interpréter les termes figurant dans les RCE conformément aux directives européennes 95/46/CE et 2002/58/CE doit être pris par les sociétés du groupe.

C. Principes et éléments essentiels devant figurer dans les RCE

1. Limitation des finalités

- Les données ne seront transférées et traitées qu'à des fins déterminées et légitimes ;
- Les données ne seront pas traitées ultérieurement de manière incompatible avec les finalités déterminées.

2. Qualité des données et proportionnalité

- Les données doivent être exactes et, si nécessaires, mises à jour ;
- Les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont transférées et traitées ;
- Les données ne seront pas conservées plus longtemps que nécessaire au regard des finalités pour lesquelles elles sont traitées et transférées ;
- Les données sensibles feront l'objet de garanties supplémentaires.

3. Base juridique du traitement :

a. 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, libre, informé et, en tant que de besoin, par écrit, 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 prévu dans le droit interne ou nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis, ou
- 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 soient pas menacés l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

b. Des données à caractère personnel sensibles

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

- la personne concernée a donné son consentement explicite, libre, informé et, en tant que de besoin, par écrit, au traitement des données sensibles en question, sauf dans les cas où la législation prévoit qu'il en va autrement, 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.

4. Transparence et droit à l'information

Les RCE doivent être rendues aisément accessibles à toute personne concernée. En particulier, les personnes bénéficiant de droits au titre de la clause de tiers bénéficiaire doivent pouvoir accéder facilement à cette clause.

Les RCE comportent l'engagement d'informer les personnes concernées, préalablement au traitement de leurs données, de :

- L'identité du ou des responsable(s) du traitement ou de son représentant ;
- Des finalités du traitement ;
- Du ou des destinataire(s) ou catégories de destinataires des données (y compris le pays de destination) ;
- L'existence d'un droit d'accès, de rectification, d'effacement, de verrouillage et d'opposition ;
- De toutes autres informations supplémentaires nécessaires afin d'assurer à l'égard de la personne concernée un traitement loyal de ses données personnelles.

Si les données n'ont pas été collectées auprès de la personne concernée, le responsable du traitement peut être dispensé de cette information lorsque cette dernière se révèle impossible ou implique des efforts disproportionnés, ou encore si la législation nationale applicable prévoit expressément l'enregistrement ou la communication des données.

5. Droits en matière d'accès, de rectification, d'effacement, de verrouillage et d'opposition

Les RCE comportent l'engagement de fournir à chaque personne concernée :

- 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 ;
- le droit d'obtenir la rectification, l'effacement ou le verrouillage de données, notamment au motif que les données sont incomplètes ou inexactes ;
- le droit de s'opposer à tout moment, 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 ;
- le droit de s'opposer, sur simple demande et sans frais, au traitement de données la concernant à des fins de prospection ;
- Une explication quant à la façon dont les personnes concernées peuvent avoir accès à leurs données personnelles ;
- Le droit de connaître les raisonnements qui sous-tendent un traitement automatisé.

6. Décisions individuelles automatisées

Les RCE comportent l'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 nationale applicable qui précise les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée.

7. Sécurité y compris l'obligation de passer des contrats avec les sous-traitants

Les RCE comportent l'engagement selon lequel des 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.

Les RCE comportent des explications sur la façon dont les données personnelles sont protégées lorsqu'il est fait appel à un sous-traitant (que celui-ci soit une filiale du groupe ou une société extérieure au 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 veiller au respect de ces mesures ;

- Les sous-traitants seront liés au responsable du traitement 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 qui lui incombent.

8. Limitations concernant les transferts et les transferts ultérieurs vers des responsables de traitement et des sous-traitants externes (qui ne sont pas des filiales du groupe)

Les RCE doivent décrire les mesures mises en œuvre pour restreindre les transferts et les transferts ultérieurs vers un responsable du traitement ou un sous-traitant extérieur au groupe de l'exportateur :

- a. Si les données personnelles proviennent d'un pays membre de l'AFAPDP situé en-dehors de l'Union européenne : tous les transferts de données devront respecter les règles de protection relatives aux flux transfrontaliers prévues par la législation nationale applicable.
- b. Si les données personnelles proviennent de l'Union européenne et que l'importateur des données est établi dans un pays non membre de l'Union européenne ou dans un pays non reconnu par la Commission européenne comme garantissant un niveau adéquat de protection : tous les transferts de données devront respecter les règles de protection relatives aux flux transfrontaliers de données prévues aux articles 25-26 de la directive 95/46/CE (en utilisant par exemple les clauses contractuelles types adoptées par la Commission européenne) ;

9. Obligation de notification/déclaration

Le responsable du traitement doit déclarer le traitement entièrement ou partiellement automatisé et le transfert de données personnelles, préalablement à sa mise en œuvre et le cas échéant obtenir une autorisation de transfert, auprès de l'autorité de contrôle nationale de protection des données lorsque de telles obligations sont prévues par la législation nationale.

10. Supervision

La mise en œuvre et le contrôle du respect des principes repris dans le présent référentiel doivent être assurés par l'autorité de contrôle de chaque Etat membre, ou par une autre autorité désignée par celle-ci.

Dans tous les cas, ces autorités de surveillance doivent être impartiales, indépendantes et disposer des compétences techniques et organisationnelles suffisantes afin de traiter les plaintes des citoyens et s'assurer du respect, par les responsables du traitement, du présent référentiel ainsi que des règles nationales relatives à la protection de la vie privée des individus.

11. Coopération entre les entités du groupe pour appliquer les règles contraignantes d'entreprise

Les RCE comportent l'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 des autorités de protection des données ;

- les entités appliquent les conseils des autorités de protection des données portant sur l'interprétation des règles définies par le présent référentiel.

12. Mise à jour des RCE

Les entités du groupe et les autorités de protection des données devront être informées de toute modification significative apportée aux RCE 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 des RCE par les autorités de protection des données ;
- les mises à jour des RCE ou de la liste des filiales concernées sont possibles sans qu'il soit nécessaire d'introduire une nouvelle demande d'autorisation des règles, moyennant le respect des conditions suivantes :
 - a. une personne désignée actualise la liste des filiales soumises au respect des RCE, 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;
 - b. aucun transfert n'est effectué vers une nouvelle filiale tant que celle-ci n'est pas véritablement liée aux RCE et tant qu'elle n'est pas en mesure de garantir leur respect;
 - c. toute modification des RCE 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 de transferts.

Toute modification substantielle des RCE doit être communiquée aux personnes concernées.

13. Clause de tiers bénéficiaire, juridiction compétente et droit national applicable en cas de litige (droits des personnes)

Le référentiel accorde aux personnes concernées des droits en matière d'application des RCE en tant que tiers bénéficiaires.

La personne concernée peut choisir d'introduire une plainte auprès des juridictions et autorités compétentes.

Dans le cadre de données en provenance de l'Union européenne, il s'agit :

- 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.

Toutes les personnes concernées bénéficiant de droits de tiers bénéficiaires doivent avoir facilement accès à cette clause.

Les RCE comportent l'engagement que les personnes dont les données sont traitées et transférées par les groupes qui mettent en place des BCR pourront se prévaloir de tout manquement aux principes suivants :

- Limitation des finalités,
- Qualité et proportionnalité des données personnelles traitées,
- Traitement de données personnelles fondé sur une base légale,
- Information des personnes concernées par les traitements et accès aisé aux BCR par celles-ci,

- Droit d'accès, de rectification, d'effacement et de verrouillage des données, et objet du traitement,
- Droits en cas de décisions individuelles automatisées,
- Sécurité et confidentialité,
- Restrictions en cas de transferts ultérieurs en-dehors du groupe,
- Toute entité membre du groupe doit informer le responsable à la protection des données désigné au sein du groupe de l'existence d'une législation locale risquant d'empêcher cette entité de respecter les BCR,
- Mise en place d'un mécanisme interne de gestion des plaintes afin de recevoir les plaintes des personnes concernées,
- Devoir de coopération du groupe avec les autorités de protection des données personnelles compétentes
- Responsabilité juridique du groupe et voies de recours.

14. Forme contraignante et caractère opposable de ces garanties

Les éléments assurant que les droits et obligations fixés dans les RCE revêtent un caractère contraignant tant interne (caractère contraignant à l'égard des filiales et des salariés, par exemple au moyen d'un engagement contractuel de conformité au référentiel,) qu'externe (droits des personnes concernées doivent être précisés à l'autorité de protection des données point de contact

15. Programme de formation adéquat

Les RCE comportent l'engagement de dispenser une formation adéquate sur les principes qu'elles contiennent auprès du 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.

16. Système interne de traitement des plaintes

Les RCE comportent l'engagement d'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 ses engagements ;
- les plaintes doivent être traitées par un département ou une personne clairement identifié(e) jouissant de l'indépendance nécessaire dans l'exercice de ses fonctions.

17. Réalisation d'audits indépendants

Les RCE comportent l'engagement selon lequel des audits concernant le respect des RCE au sein du groupe seront effectués, et notamment sur les points suivants :

- le programme d'audit couvre tous les aspects des RCE, y compris les méthodes visant à garantir que des mesures correctives seront mises en œuvre ;
- ces audits sont menés régulièrement (par exemple tous les deux ans) 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 aux engagements décrits par le présent référentiel.

18. Désignation d'un/de responsable(s) à la protection des données

Les RCE comportent l'engagement de 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 engagements de conformité au référentiel.

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 du référentiel. 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 du référentiel, en garantit le respect 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 du référentiel au niveau local.

19. Entités liées par les RCE

Les RCE doivent contenir la liste des entités liées par les RCE.

20. Engagements au cas où la législation nationale applicable aux filiales du groupe les empêcherait de respecter les règles de protection des données contenues dans les RCE

Les RCE comportent l'engagement selon lequel, lorsqu'une entité 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 RCE et d'avoir un impact négatif sur les garanties fournies par celles-ci, ladite entité en informe immédiatement le siège du groupe ou la filiale responsable par délégation de la protection des données par l'intermédiaire du délégué ou de l'instance chargé(e) de la protection 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, en cas de conflit entre la législation nationale et les engagements pris en vertu des RCE, l'entité concernée s'engage à ce que ou le siège, la filiale responsable par délégation de la protection des données, ou tout autre délégué ou instance chargé(e) de la protection des données prenne une décision raisonnable sur l'action à entreprendre et, en cas de doute, consulte les autorités de protection des données compétentes.

21. Responsabilité des parties en cas de violation des RCE

Les RCE comportent l'engagement selon lequel le siège du groupe, ou la filiale responsable par délégation de la protection des données, à condition que ce siège ou cette filiale soit situé dans un pays membre de l'AFAPDP, accepte d'endosser la responsabilité et de prendre les mesures nécessaires pour réparer les actes commis par d'autres filiales du groupe et de verser une indemnité à la personne concernée pour tout préjudice résultant de la violation des règles du référentiel commun par les filiales.

C'est au siège du groupe ou à la filiale responsable par délégation de la protection des données que revient la charge de prouver que la filiale destinataire des données n'est pas responsable de la violation ayant abouti à la demande de réparation.

Si le siège du groupe ou la filiale responsable par délégation de la protection des données est en mesure de prouver que les filiales destinataires des données ne sont pas responsables de la violation, il (elle) pourra être déchargé(e) de toute responsabilité.

Pour les données en provenance de l'Union européenne, l'entité responsable devra nécessairement être située sur le territoire de l'Union européenne, afin de garantir aux personnes concernées la possibilité d'agir contre une entité située sur le territoire de l'Union européenne.

22. Liens entre la législation nationale et l'engagement contractuel de conformité au référentiel

Les RCE devront comporter l'engagement selon lequel, si la législation locale de l'exportateur exige un degré supérieur de protection des données personnelles, celle-ci prime sur les RCE et que si les RCE exigent un degré supérieur de protection des données personnelles, ce seront elles qui primeront.

Résolution modifiée adoptée par voie électronique

Membres votants : 16

Votes exprimés : 13

Votes pour : 12

Vote contre : 0

Abstention : 1