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

538/14/FR
WP 212

Avis 02/2014 relatif à un référentiel des exigences pour les règles d'entreprise contraignantes soumises aux autorités nationales responsables de la protection des données dans l'UE et les règles transfrontalières de protection de la vie privée soumises aux agents de responsabilisation de l'APEC en matière de RTPVP

adopté le 27 février 2014

Travaux conjoints entre experts du groupe de travail article 29 et de pays de l'APEC, concernant un référentiel des exigences pour les règles d'entreprise contraignantes soumises aux autorités nationales responsables de la protection des données dans l'UE et les règles transfrontalières de protection de la vie privée soumises aux agents de responsabilisation de l'APEC en matière de RTPVP

VUE D'ENSEMBLE

Objectif du référentiel:

L'objectif du présent référentiel est de servir de liste de contrôle pratique informelle pour les organisations sollicitant une autorisation de REC et/ou de certification de RTPVP. Il facilite dès lors la conception et l'adoption de politiques de protection des données à caractère personnel conformes à chacun des systèmes.

Le présent référentiel ne vise pas l'obtention de la reconnaissance mutuelle des deux systèmes. Toutefois, il pourrait servir de base à une **double certification.** En tout état de cause, les politiques de protection des données des entreprises internationales candidates opérant tant dans la zone UE que dans la zone APEC **doivent être respectivement approuvées** par les organes pertinents des États membres de l'UE et des pays de l'APEC, conformément aux procédures d'approbation applicables.

Contexte:

Les experts du groupe de travail «article 29» des autorités pour la protection des données dans l'UE (ci-après le «GT art. 29»)[1] et dans les pays membres du sous-groupe sur la protection des données de l'APEC ont élaboré un outil pratique pour cartographier les exigences respectives des REC et des RTPVP (ci-après le «référentiel») [2].

Le présent référentiel énumère, dans un document unique, les principaux éléments généralement requis par les autorités nationales chargées de la protection des données dans l'UE (ci-après les «APD»), d'une part, et par les organes pertinents des économies de l'APEC, d'autre part, dans les politiques en matière de protection de la vie privée soumises pour autorisation en tant que REC par les APD dans l'UE, conformément aux lois sur la protection des données applicables dans les États membres de l'UE, et/ou en tant que RTPVP, conformément aux règles applicables dans les pays de l'APEC.

[1] Le GT art. 29 a été établi conformément à la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Il se compose d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque État membre de l'UE, d'un représentant du contrôleur européen de la protection des données et d'un représentant de la Commission européenne. Il a un caractère consultatif et agit en toute indépendance.

[2] À l'avenir, les entreprises et la société civile peuvent apporter une contribution à l'APEC et au GT art. 29 conformément aux mécanismes d'engagement des parties prenantes de l'APEC et aux mécanismes de consultation du GT art. 29 respectivement.

Le présent référentiel a été approuvé par les hauts responsables de l'APEC lors de leur réunion des 27 et 28 février 2014 et le groupe de travail «article 29» a adopté un avis/document de travail lors de sa réunion plénière des 26 et 27 février 2014.

Structure du référentiel:

Le référentiel comprend, pour chacun des principes et exigences essentiels des systèmes:

- un «**bloc commun**» décrivant les principaux éléments qui sont communs ou similaires aux REC et RTPVP;

- des «**blocs complémentaires**» présentant leurs principales différences et les éléments complémentaires spécifiques aux REC, d'une part, et aux RTPVP, d'autre part.

Alors que le bloc commun traduit un certain degré de similitude entre ce qui est obligatoire dans les deux systèmes RTPVP et REC, il n'est pas suffisant en soi pour obtenir la certification de RTPVP par un agent de responsabilisation agréé de l'APEC ou l'autorisation de REC par une APD nationale dans l'UE. En outre, les éléments contenus dans le bloc complémentaire des REC **doivent également être pris en considération** par une organisation sollicitant l'approbation de ses REC par les APD, et ceux énumérés dans le bloc complémentaire des RTPVP **doivent également être pris en considération** par une organisation sollicitant la certification de ses RTPVP par un agent de responsabilisation de l'APEC.

RÉFÉRENTIEL DES EXIGENCES POUR LES RÈGLES D'ENTREPRISE CONTRAIGNANTES SOUMISES AUX AUTORITÉS NATIONALES RESPONSABLES DE LA PROTECTION DES DONNÉES DANS L'UE ET LES RÈGLES TRANSFRONTALIÈRES DE PROTECTION DE LA VIE PRIVÉE SOUMISES AUX AGENTS DE RESPONSABILISATION AGRÉÉS DE L'APEC EN MATIÈRE DE RTPVP

RÉSUMÉ

Introduction

Le présent document (ci-après le «référentiel») identifie les exigences communes ou similaires à la fois aux règles d'entreprise contraignantes (ci-après les «REC») telles que généralement autorisées par les autorités nationales responsables de la protection des données dans l'Union européenne (ci-après l'«UE») pour les transferts de données à caractère personnel hors de l'UE mais au sein d'un groupe d'entreprises, et au système des règles transfrontalières de protection de la vie privée (ci-après les «RTPVP») de la Coopération économique Asie-Pacifique (ci-après l'«APEC»).

Le présent référentiel identifie également les éléments complémentaires requis pour l'approbation des REC et la certification des RTPVP en ce qui concerne le processus d'autorisation et d'examen de la conformité tant des autorités nationales chargées de la protection des données dans l'UE (ci-après les «APD») que des agents de responsabilisation agréés en matière de RTPVP de l'APEC. Cela s'entend sans préjudice de l'autorisation individuelle des REC par les APD nationales conformément à la législation européenne sur la protection des données et la certification des RTPVP par les agents de responsabilisation agréés en matière de RTPVP de l'APEC (ci-après les «agents de responsabilisation de l'APEC»). Cela ne porte pas davantage préjudice à la mise en œuvre par les autorités pertinentes de contrôle et/ou de mise en œuvre.

Le présent référentiel n'est pas nécessairement une analyse exhaustive de tous les éléments des REC et des RTPVP, ni la seule façon de cartographier ces deux systèmes et ne doit pas être considéré comme un avis juridique, ni comme reflétant la position officielle des organisations ayant participé à son élaboration.

Objectif et structure

Le présent référentiel vise à aider les organisations à mettre en œuvre les règles de protection des données à caractère personnel et de la vie privée afin de pouvoir plus aisément se conformer aux exigences en ce qui concerne les REC et les RTPVP. Il est destiné à servir de liste de contrôle pratique pour les organisations qui souhaitent concevoir et mettre en œuvre des politiques de protection de la vie privée en vue de la demande simultanée d'une autorisation de REC par des APD nationales dans l'UE et d'une certification de RTPVP par un agent de responsabilisation de l'APEC.

Le présent référentiel est destiné à servir d'outil comparatif au service des organisations envisageant une demande d'approbation de REC par des APD nationales dans l'UE et de certification de RTPVP par un agent de responsabilisation de l'APEC, à savoir une double certification. Il s'agit d'une comparaison des exigences en matière de REC et de RTPVP dans un document unique destiné à aider une organisation à formuler des règles de protection des données à caractère personnel et de la vie privée afin de satisfaire aux exigences des deux systèmes et à appliquer ces règles à ses entités, filiales et sociétés apparentées (ci-après le «groupe»). La détermination formelle de la conformité à chaque système ne peut être accomplie que par les processus agréés prévus dans chaque système, conformément aux exigences énoncées par le cadre applicable.

Le présent référentiel est structuré comme suit: pour chaque exigence identifiée, il existe un bloc d'éléments communs ou similaires qui sont requis tant pour les REC que pour les RTPVP. Les blocs complémentaires pour chaque exigence des REC et des RTPVP sont présentés à la suite et énumèrent les éléments qui sont différents dans les deux systèmes. Ces blocs complémentaires peuvent également énumérer les exceptions et clarifications concernant les exigences dans les deux systèmes. Alors que les blocs communs traduisent un certain degré de similitude entre ce qui est obligatoire dans les deux systèmes RTPVP et REC, ils ne sont pas suffisants en soi pour obtenir la certification de RTPVP par un agent de responsabilisation de l'APEC ou l'autorisation de REC par une APD nationale dans l'UE. En outre, les éléments contenus dans les blocs complémentaires des REC doivent également être pris en considération par une organisation sollicitant l'approbation de ses REC par les APD nationales dans l'UE, et ceux énumérés dans le bloc complémentaire des RTPVP doivent également être pris en considération par une organisation sollicitant la certification de ses RTPVP par un agent de responsabilisation de l'APEC.

Il convient de noter que des différences significatives peuvent exister entre les exigences généralement imposées par les APD nationales dans l'UE pour l'autorisation des REC, notamment celles découlant de la législation européenne sur la protection des données, et les exigences du programme en matière de RTPVP. Il existe également des différences entre les objectifs, les portées et les processus d'examen respectifs des systèmes REC et RTPVP. Par suite de ces différences, certaines exigences des REC et des RTPVP ne sont pas totalement compatibles. Dès lors, afin d'éviter tout conflit avec les lois applicables, les organisations candidates préciseront très clairement la portée de leurs règles de protection des données à caractère personnel et de la vie privée. Dans leur demande, elles doivent clairement distinguer dans quels cas elles appliqueront la législation européenne sur la protection des données et/ou les exigences du programme en matière de RTPVP de l'APEC, étant donné que les données à caractère personnel doivent être traitées conformément aux exigences respectives de la législation européenne sur la protection des données et/ou les lois des pays de l'APEC.

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation doivent être conçues sur mesure afin de refléter la structure du groupe auquel elles s'appliquent, le traitement entrepris par le groupe ainsi que les politiques et les procédures qu'il a mises en place afin de protéger les données à caractère personnel. Dès lors, les organisations doivent noter que les APD nationales dans l'UE et les agents de responsabilisation agréés en matière de RTPVP dans l'APEC n'accepteront pas un simple copier-coller de ce cadre.

Portée

La certification des RTPVP est limitée aux organisations certifiées dans un pays participant aux RTPVP. La portée de la certification des RTPVP d'une organisation particulière sera limitée aux entités, filiales et sociétés affiliées identifiées dans sa demande de certification.

Toute organisation souhaitant transférer des données à caractère personnel des États membres de l'UE vers des destinataires situés dans des pays non membres de l'UE peut déposer une demande auprès d'une APD nationale dans l'UE pour l'approbation de ses REC. La portée des REC d'une organisation particulière sera limitée aux entités, aux filiales et aux sociétés affiliées identifiées

dans sa demande d'approbation. La mise en œuvre correcte des REC, une fois celles-ci approuvées, offre des garanties adéquates pour les transferts de données des entités de l'UE identifiées vers les entités, filiales et sociétés affiliées hors de l'UE également identifiées (comme spécifié dans la demande de l'organisation).

Les règles de protection des données à caractère personnel et de la vie privée applicables aux transferts transfrontaliers de données à caractère personnel, si elles sont approuvées selon les procédures respectives, peuvent constituer la politique de l'organisation ou du groupe pour toutes les données à caractère personnel traitées par l'organisation ou le groupe, définie conformément à l'approbation des REC par les APD nationales dans l'UE et la certification des RTPVP par les agents de responsabilisation de l'APEC. Lorsque les données à caractère personnel sont traitées[3] dans l'UE[4], les exigences de la législation européenne sur la protection des données s'appliquent également. Lorsque les données à caractère personnel sont traitées dans un pays de l'APEC, les lois de la juridiction pertinente s'appliquent.

Le présent référentiel est basé sur les documents suivants:

UE:

- directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, ci-après la «**directive 95/46**»;

- législation nationale adoptée en application de la directive 95/46/CE;

- *document de travail: transferts de données à caractère personnel 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* (WP74), adopté par le groupe de travail article 29 le 3 juin 2003, ci-après «**WP74**»;

- *document de travail établissant une liste de contrôle type pour les demandes d'approbation des règles d'entreprise contraignante* (WP108), adopté par le groupe de travail article 29 le 14 avril 2005, ci-après «**WP108**»;

[3] Le concept de traitement comprend le stockage ainsi que toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction (voir l'article 2, point b), de la directive 95/46/CE).

[4] La législation nationale sur la protection des données des États membres de l'UE s'applique au traitement des données à caractère personnel (y compris le stockage) lorsque a) le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement **sur le territoire de l'UE**; b) le responsable du traitement n'est pas établi dans l'UE mais en un lieu où la loi nationale de l'État membre s'applique en vertu du droit international public; c) le responsable du traitement **n'est pas établi dans l'UE** et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés dans l'UE, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de l'UE (voir l'article 4, paragraphe 1, de la directive 95/46/CE).

- *recommandation 1/2007 sur l'application type pour l'approbation des règles d'entreprise contraignantes applicables au transfert des données à caractère personnel* (WP133), adopté par le groupe de travail article 29 le 10 janvier 2007, ci-après «**WP133**»;

- *document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes* (WP153), adopté par le groupe de travail article 29 le 24 juin 2008, ci-après «**WP153**»;

- *document de travail établissant un cadre pour la structure des règles d'entreprise contraignantes* (WP154), adopté par le groupe de travail article 29 le 24 juin 2008, ci-après «**WP154**»;

- *document de travail sur les questions fréquemment posées (FAQ) concernant les règles d'entreprise contraignantes* (WP155), adopté par le groupe de travail article 29 le 24 juin 2008, révisé en dernier lieu et adopté le 8 avril 2009, ci-après «**WP155**».

APEC:

- *cadre de protection de la vie privée de l'APEC*, ci-après le «**cadre de protection de la vie privée**»;

- *politiques, règles et lignes directrices concernant le système de règles transfrontalières de protection de la vie privée de l'APEC*, ci-après les «**politiques, règles et lignes directrices**»;

- *accord de coopération de l'APEC sur la protection transfrontière de la vie privée*, ci-après «**CPEA**»;

- *modèle de lettre d'intention de participation au système de règles transfrontalières de protection de la vie privée*, ci-après «**modèle de lettre d'intention**»;

- *demande d'agrément par l'APEC de l'agent de responsabilisation*, ci-après «**demande d'agrément**»;

- *questionnaire d'inscription du système de règles transfrontalières de protection de la vie privée de l'APEC*, ci-après «**questionnaire d'inscription**»;

- *exigences du programme du système de règles transfrontalières de protection de la vie privée de l'APEC*, ci-après «**exigences du programme**».

Référentiel concernant les exigences de protection des données à caractère personnel et de la vie privée des REC et des RTPVP

1. Objectif des règles de protection des données à caractère personnel et de la vie privée d'une organisation

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation doivent:

- fournir une protection adéquate pour le transfert et le traitement des données à caractère personnel par le groupe, conformément aux processus d'approbation des REC et de certification des RTPVP [5]; et
- constituer pour l'organisation une obligation exécutoire afin d'assurer la conformité aux règles de protection des données à caractère personnel et de la vie privée [6] (voir les sections 3 et 21 du référentiel);
- contenir une référence aux lois en vigueur sur la protection des données [7].

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent une obligation claire pour tous les membres du groupe et du personnel d'interpréter et de respecter les règles de protection des données à caractère personnel et de la vie privée de l'organisation conformément aux lois applicables [8].	Lorsque les exigences juridiques nationales sont plus strictes que celles du système RTPVP, la législation et la réglementation nationales s'appliquent dans toute leur mesure. Lorsque les exigences du système RTPVP sont plus strictes que les exigences des législation et réglementation nationales, l'organisation devra volontairement exécuter ces exigences supplémentaires afin de participer. Néanmoins, les autorités chargées de la protection de la vie privée dans ce pays doivent avoir la capacité de prendre des mesures d'exécution, en vertu de la législation et de la réglementation nationales applicables, qui ont pour effet de protéger les informations à caractère personnel conformes aux exigences du programme en matière de RTPVP [9] (*voir également 26, relations entre la législation locale et les règles de protection des données à caractère personnel et de la vie*

	privée de l'organisation).

Références

[5] UE: voir WP74, point 3.1, pp. 7-9; APEC: voir cadre de protection de la vie privée, partie iii, principe I, 14, p. 11.

[6] UE: voir WP154, Introduction, p. 3 et WP74 p. 10-14; APEC: voir politiques, règles et lignes directrices en matière de RTPVP, 8, p. 4; exigences du programme en matière de RTPVP 39, 40.

[7] UE: voir WP154, Introduction, p. 3; APEC: voir demande d'agrément, annexe A, 4, p. 5.

[8] UE: voir WP74, point 3.3.1, pp. 10-11; WP153, point 1.1, p. 3.

[9] APEC: voir politiques, règles et lignes directrices, 44, p. 10.

2. Portée des règles de protection des données à caractère personnel et de la vie privée d'une organisation

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation doivent comprendre une description de leur champ d'application dont:

- la portée géographique (voir les sections 4 et 15 du présent référentiel) [10];
- la portée matérielle (à savoir la nature des données, clients effectifs/potentiels, travailleurs effectifs/potentiels, fournisseurs…) [11];
- la liste des entités liées par les règles de protection des données à caractère personnel et de la vie privée d'une organisation [12]; et
- les objectifs du transfert et/ou du traitement [13].

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
Le traitement des données à caractère personnel qui sont accessibles au public est soumis aux exigences de la législation européenne sur la protection des données et n'est pas exempté des REC. Les organisations qui choisissent de participer au système REC mettent en œuvre les politiques et pratiques de protection de la vie privée dans le respect des exigences du programme en matière de REC pour toutes les données à caractère personnel qui sont transférées dans le groupe hors de l'Union européenne. Bien qu'elles n'y soient pas tenues pour l'approbation des REC, les organisations participantes peuvent appliquer les mêmes politiques et procédures de protection de la vie privée à toutes les données à caractère personnel qui sont traitées au sein du groupe au niveau mondial, à condition que la conformité à la législation européenne sur la protection des données soit assurée lorsque des données à caractère personnel sont traitées dans l'UE.	S.O.
Clarification de la portée des REC S.O.	**Clarification de la portée des RTPVP** Dans certains cas, les règles de protection des données à caractère personnel et de la vie

	privée de l'organisation peuvent ne pas s'appliquer aux informations accessibles au public [14]. Les organisations qui choisissent de participer au système RTPVP doivent mettre en œuvre les politiques et pratiques de protection de la vie privée dans le respect des exigences du programme en matière de RTPVP pour toutes les données à caractère personnel qu'elles ont collectées ou reçues et qui font l'objet d'un transfert transfrontalier vers d'autres pays participants de l'APEC. Bien qu'elles n'y soient pas tenues au titre du système RTPVP, les organisations participantes sont encouragées à appliquer les mêmes politiques et procédures de protection de la vie privée à toutes les informations à caractère personnel qu'elles ont collectées ou reçues, même si elles ne font pas l'objet d'un transfert transfrontalier ou si elles ne sont soumises à un tel transfert qu'en dehors des pays participants de l'APEC [15].

Références

[10] UE: voir WP153, point 4.2 et WP108, point 7.1 et 7.2, pp. 7-8; APEC: voir questionnaire d'inscription, v-vi, pp. 2-3.

[11] UE: voir WP153, point 4.2 et WP108, point 7.1.1 et 7.2, pp. 7-8; APEC: voir questionnaire d'inscription, iv, p. 2.

[12] UE: voir WP153 point 6.2; WP108, point 7.1.3, p. 8; APEC: voir questionnaire d'inscription, ii, p. 2.

[13] UE: voir WP153 point 4.1; WP108, point 7.1.2, p. 8; APEC: voir exigence du programme en matière de RTPVP 1(b) et 1(c).

[14] APEC: voir cadre de protection de la vie privée de l'APEC, 11 p. 7.

[15] APEC: voir politiques, règles et lignes directrices, 8, p. 4.

3. Obligation exécutoire au sein d'une organisation

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Toutes les entités du groupe sollicitant soit l'approbation d'une REC par une APD dans l'UE, soit la certification d'une RTPVP par un agent de responsabilisation de l'APEC doivent être soumises à une obligation exécutoire de satisfaire aux règles de protection des données à caractère personnel et de la vie privée de l'organisation conformément aux lois applicables qui peuvent être appliquées par la personne individuelle/concernée et l'autorité de régulation le cas échéant [16].

Éléments complémentaires requis pour l'approbation des REC: caractère contraignant au sein d'un groupe (REC)	**Éléments complémentaires requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée de l'organisation doivent être rendues juridiquement contraignantes entre les entités dans le groupe par un ou plusieurs des instruments suivants [17]: i) mesures ou règles juridiquement contraignantes pour tous les membres du groupe; ii) contrats entre membres du groupe; iii) les déclarations formulées ou engagements donnés de façon unilatérale par la société mère qui sont contraignants pour les autres membres du groupe [18]; iii) intégration d'autres mesures règlementaires, par exemple obligations contenues dans les codes statutaires dans un cadre juridique défini; iv) intégration des règles de protection des données à caractère personnel et de la vie privée de l'organisation dans ses principes généraux d'entreprise, étayée par des politiques, des audits et des sanctions appropriés; v) autres moyens [19]. En outre, les règles de protection des données à caractère personnel et de la vie privée de l'organisation doivent également être rendues	S.O.

contraignantes pour les employés par un ou plusieurs des instruments suivants [20]: i) accord/engagement individuel et distinct avec sanctions; ii) clause dans le contrat de travail avec sanctions; iii) politiques internes avec sanctions; iv) conventions collectives avec sanctions.	
Clarification du caractère contraignant pour une organisation (REC) S.O.	**Clarification de la responsabilisation d'une organisation (RTPVP)** L'organisation doit respecter ses engagements en matière de responsabilité en démontrant l'applicabilité de ses règles de protection des données à caractère personnel et de la vie privée par un ou plusieurs des instruments suivants [21]: i) lignes directrices ou politiques internes; ii) contrats; iii) conformité aux lois et règlements applicables de l'industrie ou du secteur; iv) autres moyens. En outre, l'organisation doit mettre en place des procédures pour la formation du personnel en ce qui concerne ses règles de protection des données à caractère personnel et de la vie privée [22].

Références

[16] UE: voir WP153 points 1.1 et 1.2; WP74, point 3.3.1, pp. 10-11; APEC: voir exigences du programme, Q39, p. 24; annexes A et B.

[17] UE: voir WP153, point 1.2.i, p. 3; WP108, point 5.6, p. 5.

[18] Il convient de noter que, dans certains États membres de l'UE, de simples déclarations unilatérales ne peuvent être considérées comme légalement contraignantes en droit civil et administratif. Le cas échéant, seuls les contrats sont considérés comme contraignants. Une organisation locale devrait dès lors prendre conseil au niveau local si elle entend invoquer d'autres moyens juridiques que les contrats.

[19] UE: WP74, point 3.3.1, pp. 10-11; WP153, point 1.1, p. 3.

[20] UE: voir WP74, point 3.3.1, pp. 10-11; WP 153, point 1.1, p. 3 et point 1.2.ii, p. 3.

[21] APEC: voir exigences du programme, Q39, p. 24; Q46, p. 26; annexes A et B.

[22] APEC: voir exigences du programme, Q44, p. 25-26.

4. Voies de recours des personnes concernées et droits pour les tiers bénéficiaires

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

S.O.

Éléments requis pour l'approbation des REC	**Éléments requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée d'une organisation accordent clairement des droits aux personnes concernées pour faire respecter lesdites règles en tant que tiers bénéficiaires. Elles doivent exposer les voies de recours juridictionnel claires, accessibles et efficaces pour toute violation des règles de protection des données à caractère personnel et de la vie privée et le droit d'obtenir réparation (voir les articles 22 et 23 de la directive 95/46/CE) [23]. Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également une déclaration selon laquelle les personnes concernées ont le droit de choisir une des voies suivantes pour déposer une plainte: - la juridiction de l'exportateur des données situé dans l'UE, ou - la juridiction du siège dans l'UE/membre de l'UE avec des responsabilités déléguées, ou - les APD nationales compétentes dans l'UE. Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent l'assurance que toutes les personnes concernées bénéficiant des droits des tiers bénéficiaires auront facilement accès à cette clause [24].	Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent une déclaration selon laquelle les personnes concernées peuvent les faire respecter par: - le processus de règlement des plaintes du responsable du traitement [25]; ou - le processus de résolution des litiges de l'agent de responsabilisation de l'APEC [26]. Les personnes concernées peuvent également déposer une plainte contre un agent de responsabilisation directement auprès du panel commun de surveillance de l'APEC [27]. Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également une exigence selon laquelle les personnes concernées peuvent déposer une plainte devant les agents de responsabilisation de l'APEC [28]. Dans certains pays participants aux RTPVP, les personnes concernées peuvent disposer, en vertu de la législation locale sur la protection des données personnelles, d'un droit privé pouvant être invoqué pour faire respecter la conformité aux RTPVP.

Références

[23] UE: voir WP74, point 3.3.2, pp. 11-13.

[24] UE: voir WP153, point 1.7, p. 5.

[25] APEC: voir questionnaire d'inscription, Q41-43, pp. 21-22.

[26] APEC: voir demande d'agrément, annexe A, 9-10, p. 7.

[27] APEC: voir politiques, règles et lignes directrices, 35, p. 9.

[28] APEC: voir demande d'agrément, annexe A, 9-10, p. 7.

5. Responsabilité

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation disposent, en principe, que la responsabilité incombe à une entité [29].

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également un engagement selon lequel [30]: - soit le siège dans l'UE, soit le membre de l'UE avec des responsabilités déléguées assume la responsabilité et accepte de prendre les mesures nécessaires pour remédier aux actes d'autres membres du groupe hors de l'UE et verser une indemnisation pour tous dommages résultant de la violation des règles de protection des données à caractère personnel et de la vie privée de l'organisation par les membres du groupe; - il incombe soit au siège dans l'UE, soit au membre de l'UE avec des responsabilités déléguées, de démontrer que le membre hors de l'UE n'est pas responsable de la violation justifiant la demande d'indemnisation présentée par la personne concernée. Si le siège dans l'UE ou le membre de l'UE avec des responsabilités déléguées peut prouver que le membre hors de l'UE n'est pas responsable de la violation, il peut se décharger de toute responsabilité. S'il est impossible à certains groupes ayant une structure d'entreprise particulière d'imposer à une entité spécifique toute la responsabilité d'une violation des REC hors de l'UE, les APD nationales dans l'UE pourraient accepter d'autres mécanismes de responsabilité au cas par cas à condition qu'ils	Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également un engagement selon lequel la responsabilité incombe à l'entité certifiée selon les RTPVP. Toutefois, cela ne subroge aucune responsabilité supplémentaire des filiales/sociétés affiliées en vertu de la législation locale dans le cadre de laquelle une violation peut avoir été commise.

fournissent la garantie suffisante que les droits des personnes concernées seront applicables et qu'elles ne seront pas désavantagées en les faisant valoir [31].	

Références

[29] UE: voir WP74, point 5.5.2, pp. 18-19; APEC: voir questionnaire d'inscription, ii, p. 2.

[30] UE: voir WP74, point 5.5.2, pp. 18-19.

[31] Concernant ces éventuels régimes de responsabilité, il s'agirait du mécanisme de responsabilité solidaire entre importateurs de données et exportateurs de données prévu par les clauses contractuelles types de l'UE faisant l'objet de la décision 2001/497/CE du 15 juin 2001 ou du régime de responsabilité reposant sur des obligations de diligence prévu par les clauses contractuelles types de l'UE faisant l'objet de la décision 2004/915/CE du 27 décembre 2004. Une dernière possibilité, spécifiquement consacrée aux transferts entre responsables du traitement des données et sous-traitants, est l'application du mécanisme de responsabilité prévu par les clauses contractuelles types faisant l'objet de la décision 2002/16/CE du 27 décembre 2001.

6. Obligations exécutoires concernant les transferts aux tiers

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent une obligation exécutoire en vertu de laquelle l'organisation ne transfère de données qu'à des tiers qui appliquent la protection au traitement des données à caractère personnel, ainsi qu'une explication quant à la façon dont les règles de protection des données à caractère personnel et de la vie privée de l'organisation sont rendues applicables aux destinataires des données dans la juridiction pertinente [32].

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent des règles visant à restreindre les transferts et transferts ultérieurs hors du groupe et l'obligation de veiller à ce que [33]: - les sous-traitants externes situés dans l'UE ou dans un pays reconnu par la Commission européenne comme assurant un niveau de protection adéquat soient liés par un accord écrit stipulant que le sous-traitant n'agit que sur instructions du responsable du traitement et assume la responsabilité de la mise en œuvre des mesures de sécurité et de confidentialité adéquates; - tous les transferts de données vers les sous-traitants externes situés hors de l'UE et non dans un pays reconnu par la Commission européenne comme assurant un niveau de protection adéquat doivent respecter les règles européennes sur les flux de données transfrontaliers (articles 25 et 26 de la directive 95/46/CE: par exemple, en utilisant les clauses contractuelles types de l'UE approuvées par la décision 2001/497/CE ou 2004/915/CE de la Commission européenne ou d'autres moyens contractuels	S.O.

conformément aux articles 25 et 26 de la directive de l'UE); - tous les transferts de données vers les sous-traitants externes situés hors de l'UE doivent respecter les règles relatives aux sous-traitants (articles 16 et 17 de la directive 95/45/CE) en plus des règles sur les flux transfrontaliers des données (articles 25 et 26 de la directive 95/46/CE).	
Clarification du caractère contraignant pour les tiers (REC) S.O.	**Clarification de la responsabilisation en ce qui concerne les transferts aux tiers (RTPVP)** Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent une explication de la façon dont les données à caractère personnel sont protégées lors du recours à un sous-traitant, un agent, un contractant ou un autre prestataire de services, plus particulièrement, une exigence selon laquelle: - le responsable du traitement doit choisir un sous-traitant, un agent, un contractant ou un autre prestataire de services offrant des garanties suffisantes en ce qui concerne les mesures de sécurité technique et les mesures organisationnelles régissant le traitement à exécuter, et doit assurer la conformité à ces mesures [34]; - le responsable du traitement donne instruction au sous-traitant de veiller notamment à ce que: i) le sous-traitant, l'agent, le contractant ou autre prestataire de services agisse uniquement sur instructions du responsable du traitement [35]; ii) les règles relatives à la sécurité et à la confidentialité incombent au sous-traitant, à l'agent, au

	contractant ou autre prestataire de services [36]. Les règles de protection des données à caractère personnel et de la vie privée d'une organisation peuvent être rendues contraignantes par un ou plusieurs des instruments suivants [37]: i) lignes directrices ou politiques internes; ii) contrats; iii) conformité aux lois et règlements applicables de l'industrie ou du secteur; iv) autres moyens.

Références

[32] UE: voir WP74, point 3.2, pp. 9-10; APEC: voir exigences du programme, Q39, p. 24; Q46, p. 26; annexes A et B; questionnaire d'inscription, Q47, p. 22.

[33] UE: voir WP153, point 6.1 vi); WP154, point 12, p. 7.

[34] APEC: voir questionnaire d'inscription, Q35, p. 15.

[35] APEC: voir questionnaire d'inscription, Q47-48, pp. 22-23.

[36] APEC: voir questionnaire d'inscription, Q35, pp. 15-16.

[37] APEC: voir exigences du programme, Q39, p. 24; Q46, p. 26; annexes A et B.

7. Relations avec les sous-traitants qui sont membres du groupe

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent une explication de la façon dont les données à caractère personnel sont protégées lorsqu'il est fait appel à un sous-traitant qui est un membre du groupe, notamment une exigence selon laquelle [38]:

- le responsable du traitement doit choisir un sous-traitant offrant des garanties suffisantes en ce qui concerne les mesures de sécurité technique et les mesures organisationnelles régissant le traitement à exécuter, et doit assurer la conformité à ces mesures [39];
- le responsable du traitement donne instruction au sous-traitant de veiller notamment à ce qui suit:
  - le sous-traitant agit uniquement sur instructions du responsable du traitement [40];
  - les règles relatives à la sécurité et à la confidentialité incombent au sous-traitant [41].

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée d'une organisation prévoient un engagement selon lequel des instructions sont données par un moyen contractuel écrit conformément au droit applicable [42].	Lorsque le responsable du traitement entend transférer des données à caractère personnel à des sous-traitants, des agents, des contractants ou autres prestataires de services, il doit obtenir le consentement de la personne concernée ou agir avec la diligence requise et prendre des mesures raisonnables pour s'assurer que la personne ou l'organisation destinataire protègera les données conformément aux règles de protection des données à caractère personnel et de la vie privée de l'organisation [43]. Dans des situations où la diligence requise et des mesures raisonnables pour assurer la conformité aux règles de protection des données à caractère personnel et de la vie privée de l'organisation sont peu pratiques ou impossibles, le responsable du traitement fournit une explication et décrit les autres moyens utilisés pour s'assurer que les données sont néanmoins protégées conformément aux principes de protection de la vie privée de l'APEC. Les instructions peuvent être données par le

	responsable du traitement par [44]: - des lignes directrices ou politiques internes; ou - des contrats; ou - la conformité aux lois et règlements applicables de l'industrie ou du secteur; ou - la conformité au code et/ou aux règles d'autorégulation d'une organisation; ou - d'autres moyens. Ces accords requièrent généralement que les sous-traitants en charge du traitement des données à caractère personnel, les agents, les contractants ou autres prestataires de services [45] prennent les dispositions de protection appropriées parmi les options suivantes: - respecter les politiques et pratiques de protection de la vie privée, conformes à l'APEC, du responsable du traitement, telles que mentionnées dans sa déclaration de confidentialité; - mettre en œuvre des pratiques en matière de protection de la vie privée qui soient similaires en substance aux politiques ou pratiques en matière de protection de la vie privée du responsable du traitement, telles que mentionnées dans sa déclaration de confidentialité; - suivre les instructions fournies par le responsable du traitement concernant la manière dont ses données à caractère personnel doivent être traitées; - imposer des restrictions concernant la sous-traitance sauf avec le consentement du responsable du traitement; - faire certifier leurs RTPVP par un agent de responsabilisation de l'APEC dans leur juridiction. Les sous-traitants, les agents, les contractants ou autres prestataires de services informent le responsable du traitement lorsqu'ils ont

	connaissance d'un cas de violation de la confidentialité ou de la sécurité de ses données à caractère personnel [46]. Les sous-traitants, les agents, les contractants ou autres prestataires de services prennent des mesures immédiates pour corriger/remédier à la défaillance ayant causé la violation de la vie privée ou de la sécurité [47]. Les sous-traitants, les agents, les contractants ou autres prestataires de services fournissent au responsable du traitement des autoévaluations pour assurer la conformité à ses instructions et/ou accords/contrats [48]. Le responsable du traitement soumet à des vérifications ou contrôles réguliers, sur place, ses sous-traitants en charge du traitement des données à caractère personnel, agents, contractants ou autres prestataires de services afin d'assurer le respect de ses instructions et/ou accords/contrats [49].

Références

[38] UE: voir directive 95/46, article 17, paragraphe 2; WP154, point 11, pp. 6-7.

[39] APEC: voir questionnaire d'inscription, Q35, p. 15.

[40] APEC: voir questionnaire d'inscription, Q47-48, pp. 22-23.

[41] APEC: voir questionnaire d'inscription, Q35, pp. 15-16.

[42] UE: voir directive 95/46, article 17, paragraphe 2; WP154, point 11, pp. 6-7.

[43] APEC: voir cadre de protection de la vie privée, partie iii, principe IX, 26, p. 28.

[44] APEC: voir questionnaire d'inscription, Q46, p. 22.

[45] APEC: voir questionnaire d'inscription, Q47, pp. 22-23.

[46] APEC: voir questionnaire d'inscription, Q35-b), p. 15.

[47] APEC: voir questionnaire d'inscription, Q35-c), p. 16.

[48] APEC: voir questionnaire d'inscription, Q48, p. 23.

[49] APEC: voir questionnaire d'inscription, Q49, p. 23.

8. Restrictions aux transferts ainsi qu'aux transferts ultérieurs vers les responsables externes du traitement et du contrôle (non membres du groupe)

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent l'exigence selon laquelle les contractants qui reçoivent des données et les traitent sont tenus de protéger les données à caractère personnel conformément aux règles de protection des données à caractère personnel et de la vie privée de l'organisation [50].

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également une explication des mesures en place pour restreindre les transferts ainsi que les transferts ultérieurs hors du groupe et une obligation de veiller à ce que: - les sous-traitants externes situés dans l'UE ou dans un pays reconnu par la Commission européenne comme assurant un niveau de protection adéquat soient liés par un accord écrit stipulant que le sous-traitant agit uniquement sur instructions du responsable du traitement et assume la responsabilité de la mise en œuvre de mesures de sécurité et de confidentialité adéquates [51]; - tous les transferts de données aux responsables de contrôle externes situés hors de l'UE ou n'étant pas situés dans un pays reconnu par la Commission européenne comme assurant un niveau de protection adéquat respectent les règles européennes sur les flux transfrontaliers de données (articles 25 et 26 de la directive 95/46/CE: par exemple, en utilisant les clauses contractuelles types de l'UE approuvées par la décision 2001/497/CE ou 2004/915/CE de la Commission européenne ou par d'autres moyens contractuels conformément aux articles 25 et 26 de la	Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également une explication de la façon dont les données à caractère personnel sont protégées lorsqu'il est fait appel à un sous-traitant, un agent, un contractant ou autre prestataire de services, plus particulièrement, une exigence selon laquelle: - le responsable du traitement doit choisir un sous-traitant, un agent, un contractant ou un autre prestataire de services offrant des garanties suffisantes en ce qui concerne les mesures de sécurité techniques et les mesures organisationnelles régissant le traitement à exécuter, et doit assurer la conformité à ces mesures [54]; - le responsable du traitement donne instruction au sous-traitant, à l'agent, au contractant ou autre prestataire de services de veiller notamment à ce que ce dernier: i) agisse uniquement sur instructions du responsable du traitement [55]; ii) observe les règles relatives à la sécurité et à la confidentialité qui incombent au sous-traitant, à l'agent, au contractant ou autre prestataire de services [56]. Des instructions peuvent être données par le

directive de l'UE) [52]; - tous les transferts de données vers des sous-traitants externes situés hors de l'UE respectent les règles relatives aux sous-traitants (articles 16 et 17 de la directive 95/45/CE) en plus des règles sur les flux transfrontaliers des données (articles 25 et 26 de la directive 95/46/CE) [53].	responsable du traitement par [57]: - des lignes directrices ou politiques internes; ou - des contrats; ou - la conformité aux lois et règlements applicables de l'industrie ou du secteur; ou - la conformité au code et/ou aux règles d'autorégulation d'une organisation; ou - d'autres moyens. Ces accords requièrent généralement que les sous-traitants en charge du traitement des données à caractère personnel, les agents, les contractants ou autres prestataires de services prennent les dispositions de protection appropriées parmi les options suivantes [58]: - respecter les politiques et pratiques de protection de la vie privée, conformes à l'APEC, du responsable du traitement, telles que mentionnées dans sa déclaration de confidentialité; - mettre en œuvre des pratiques en matière de protection de la vie privée qui soient substantiellement similaires aux politiques ou pratiques en matière de protection de la vie privée du responsable du traitement, telles que mentionnées dans sa déclaration de confidentialité; - suivre les instructions fournies par le responsable du traitement concernant la manière dont ses données à caractère personnel doivent être traitées; - imposer des restrictions concernant la sous-traitance sauf avec le consentement du responsable du traitement; - faire certifier leurs RTPVP par un agent de responsabilisation de l'APEC dans leur juridiction; - d'autres moyens. Les sous-traitants, les agents, les contractants

	ou autres prestataires de services informent le responsable du traitement lorsqu'ils ont connaissance d'un cas de violation de la confidentialité ou de la sécurité de ses données à caractère personnel [59]. Les sous-traitants, les agents, les contractants ou autres prestataires de services prennent des mesures immédiates pour corriger/remédier à la défaillance ayant causé la violation de la vie privée ou de la sécurité [60]. Les sous-traitants, les agents, les contractants ou autres prestataires de services fournissent au responsable du traitement des autoévaluations pour assurer la conformité à ses instructions et/ou accords/contrats [61]. Le responsable du traitement soumet à des vérifications ou contrôles réguliers, sur place, ses sous-traitants en charge du traitement des données à caractère personnel, agents, contractants ou autres prestataires de services afin d'assurer le respect de ses instructions et/ou accords/contrats [62].

Références

[50] UE: voir WP74, point 3.2, pp. 9-10; APEC: voir questionnaire d'inscription, Q47, p. 22.

[51] UE: voir la directive 95/46, article 17, paragraphe 2; WP154, point 12, p. 7.

[52] UE: voir WP74, point 3.2, pp. 9-10.

[53] UE: voir WP154, point 12, p. 7.

[54] APEC: voir questionnaire d'inscription, Q35, p. 15.

[55] APEC: voir questionnaire d'inscription, Q47-48, pp. 22-23.

[56] APEC: voir questionnaire d'inscription, Q35, pp. 15-16.

[57] APEC: voir questionnaire d'inscription, Q46, p. 22.

[58] APEC: voir questionnaire d'inscription, Q47, pp. 22-23.

[59] APEC: voir questionnaire d'inscription, Q35-b), p. 15.

[60] APEC: voir questionnaire d'inscription, Q35-c), p. 16.

[61] APEC: voir questionnaire d'inscription, Q48, p. 23.

[62] APEC: voir questionnaire d'inscription, Q49, p. 23.

9. Définitions

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Une organisation est tenue d'interpréter les termes utilisés dans ses règles de protection des données à caractère personnel et de la vie privée conformément à la législation applicable de l'UE, notamment la directive 95/46/CE et la directive 2002/58/EC, à la législation applicable dans les pays participant aux RTPVP et au glossaire de l'APEC en matière de RTPVP [63].

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent un engagement à interpréter les termes conformément à la législation applicable de l'UE, en particulier la directive 95/46/CE et la directive 2002/58/CE, et contiennent une description des principaux termes et de leurs définitions: données à caractère personnel [64]; responsable du traitement [65]; sous-traitant [66]; personnes concernées [67]; données sensibles à caractère personnel [68]; traitement [69]; tiers [70]; et autorités pour la protection des données dans l'UE [71].	S.O.

Références

[63] UE: voir WP154, point 2, p. 4; WP155 Q8, p. 5; APEC: voir glossaire des RTPVP.

[64] UE: voir la directive 95/46, article 2, point a.

[65] UE: voir la directive 95/46, article 2, point d.

[66] UE: voir la directive 95/46, article 2, point e.

[67] UE: voir la directive 95/46, article 2, point a.

[68] UE: voir la directive 95/46, article 8.

[69] UE: voir la directive 95/46, article 2, point b.

[70] UE: voir la directive 95/46, article 2, point f.

[71] UE: voir la directive 95/46, article 2, point f.

10. Collecte, traitement et utilisation des informations à caractère personnel

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation prévoient que les données à caractère personnel ne doivent être collectées et traitées que loyalement et licitement [72] pour des finalités déterminées, explicites et légitimes et ne pas être traitées de manière incompatible avec ces finalités, ainsi que ce terme peut être défini par la législation applicable [73].

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée d'une organisation prévoient également que les données à caractère personnel ne seront transférées et traitées que pour des finalités explicites et légitimes [74].	S.O.
Clarification du traitement des données à caractère personnel (REC) S.O.	**Clarification de l'utilisation des informations à caractère personnel (RTPVP)** Les informations à caractère personnel peuvent être utilisées à d'autres fins compatibles ou liées, avec le consentement de la personne dont les informations à caractère personnel sont collectées; en cas de besoin pour fournir un service ou un produit demandés par la personne; ou en application d'une décision de justice et d'autres instruments juridiques, proclamations et déclarations à effet légal [75].

Références

[72] UE: voir directive 95/46, article 6, paragraphe 1, point a; WP108, point 8.2.1, p. 8; WP153, point 6.1.i, p. 10; WP154, point 5, p. 4, point 6, p. 5; APEC: voir cadre de protection de la vie privée, partie iii, principe III, 18, p. 15; exigences du programme, Q7, p. 7.

[73] UE: voir directive 95/46, article 6, paragraphe 1, point b; WP108, point 8.2.2, p. 8; WP153, point 6.1.ii, p. 10; WP154, point 3, p. 4; APEC: voir cadre de protection de la vie privée, partie iii, principes III et IV, 18 et 19, p. 15-16, exigences du programme, Q6, et Q8, p 6 & 8.

[74] UE: voir directive 95/46, article 6, paragraphe 1, point b; WP108, point 8.2.2, p. 8; WP153, point 6.1.ii, p. 10; WP154, point 3, p. 4.

[75] APEC: voir cadre de protection de la vie privée, partie iii, principe IV, 19, pp. 16-17, exigences du programme, Q9 &13, pp. 8-10.

11. Qualité et proportionnalité / intégrité des données

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent un engagement selon lequel:

- les données à caractère personnel sont exactes, complètes et, si nécessaire, mises à jour. Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également un engagement à communiquer ces corrections à toutes les parties pertinentes le cas échéant [76];
- les données à caractère personnel sont adéquates et pertinentes au regard des finalités pour lesquelles elles sont transférées et/ou traitées ultérieurement [77].

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également une exigence implicite selon laquelle les données à caractère personnel sont non excessives au regard des finalités pour lesquelles elles sont transférées et traitées ultérieurement [78]. Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également une exigence selon laquelle données à caractère personnel ne peuvent être traitées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou, si nécessaire, traitées ultérieurement [79].	S.O.

Références

[76] UE: voir directive 95/46, article 6, paragraphe 1, point d); WP153 point 6.1.iii, p. 10; WP108, point 8.2.3, p. 8; APEC: voir cadre de protection de la vie privée, partie iii, principe VI, 21, p. 20; exigences du programme 21; 22, p. 15; questionnaire d'inscription Q22, Q23 et 24, p. 13.

[77] UE: voir directive 95/46, article 6, paragraphe 1, point c); WP153 point 6.1.iii, p. 10; WP108, point 8.2.3, p. 8; APEC: voir cadre de protection de la vie privée, partie iii, principe III, 18, p. 15, exigences du programme, Q6, p. 6.

[78] UE: voir directive 95/46, article 6, paragraphe 1, point d); WP153 point 6.1.iii, p. 10.

[79] UE: voir directive 95/46, article 6, paragraphe 1, point e); WP153 point 6.1.iii, p. 10; WP108, point 8.2.3, p. 8.

12. Motifs pour le traitement des données à caractère personnel

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent un engagement selon lequel:

- les données à caractère personnel ne sont traitées (y compris collectées, utilisées, transférées, divulguées ou mises à disposition) que lorsqu'il existe un motif de traitement valable, comme lorsque la personne concernée a donné son consentement éclairé [80];
- les données à caractère personnel sont traitées conformément à la législation applicable [81].

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
Lorsque le consentement est la base juridique du traitement, il est sans équivoque, spécifique, librement donné et éclairé [82]. Le consentement en tant que base juridique du traitement ne peut être subrogé aux motifs de l'évidence, ni au motif que les données à caractère personnel sont accessibles au public, que le consentement est technologiquement irréalisable, ou que les données à caractère personnel ont été reçues d'un tiers. Le consentement n'est que l'une des bases juridiques possibles du traitement des données à caractère personnel. Les données à caractère personnel peuvent également être traitées pour les motifs suivants [83]: - le traitement est nécessaire pour l'exécution d'un contrat auquel la personne concernée est partie ou afin de prendre des mesures à la demande de la personne concernée avant de conclure un contrat; ou - le traitement est nécessaire pour la conformité à une obligation légale de l'UE à laquelle le responsable du traitement est soumis; ou - le traitement est nécessaire afin de	S.O.

protéger les intérêts vitaux de la personne concernée; ou - le traitement est nécessaire pour l'exécution d'une tâche effectuée dans l'intérêt public ou dans l'exercice de l'autorité officielle de l'UE dont est investi le responsable du traitement ou un tiers auquel les données sont divulguées; ou - le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par le ou les tiers auxquels les données sont divulguées, sauf lorsque prévalent sur ces intérêts les intérêts liés aux droits et libertés fondamentaux de la personne concernée.	
Clarification des motifs pour le traitement (REC) S.O.	**Clarification des motifs pour le traitement (RTPVP)** Les personnes ont le choix en ce qui concerne la collecte, l'utilisation et la divulgation de leurs informations à caractère personnel. Toutefois ce principe reconnaît, par les mots d'introduction «le cas échéant» dans le cadre de protection de la vie privée lui-même, qu'il existe certaines situations dans lesquelles le consentement peut être clairement implicite ou dans lesquelles il ne serait pas nécessaire de prévoir un mécanisme pour exercer un choix. Ces situations sont détaillées dans «*Qualifications to the Provision of Choice Mechanisms*» *[conditions de la fourniture de mécanismes de choix]* [84]. Sous réserve des conditions énumérées, les personnes disposent: - d'un mécanisme clair et évident pour exercer un choix en ce qui concerne la collecte de leurs informations à caractère personnel; - d'un mécanisme clair et évident pour exercer un choix en ce qui concerne

	l'utilisation de leurs informations à caractère personnel; - d'un mécanisme clair et évident pour exercer un choix en ce qui concerne la divulgation de leurs informations à caractère personnel; - ces mécanismes doivent être clairement libellés, faciles à comprendre, facilement accessibles et abordables. Les conditions applicables sont notamment: - évidence; - collecte d'informations accessibles au public; - impossibilité technologique; - réception de tiers; - divulgation à une institution gouvernementale ayant présenté une demande d'information légalement autorisée; - divulgation à un tiers conformément à un processus légal; - fins d'enquête légitime; - mesure en cas d'urgence. En dehors du consentement, les données à caractère personnel peuvent également être traitées pour les motifs suivants [85]: - motifs compatibles ou liés tels qu'identifiés dans la déclaration de confidentialité et/ou dans l'avis fourni au moment de la collecte; - nécessité de fournir un service ou un produit demandé par la personne; - motifs imposés par la législation applicable.

Références

[80] UE: voir directive 95/46, article 7, point a); WP154, point 5, p. 4; APEC: voir cadre de protection

de la vie privée, partie iii, principe III, 18, p. 15.

[81] UE: voir WP153, point 6.4, p. 11; WP155 Q10, p. 6; APEC: voir exigences du programme, Q7, p. 7.

[82] UE: voir directive 95/46, article 7, point a); WP154, point 5, p. 4.

[83] UE: voir directive 95/46, article 7; WP154, point 5, p. 4.

[84] APEC: voir exigences du programme Q14; 15; 16; 17; 18; 19, pp. 11-14.

[85] APEC: voir exigences du programme Q8; 9; 10; 11; 12; 13, pp. 8-10.

13. Données sensibles

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation identifient les protections applicables aux données sensibles [86].

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également un engagement interdisant le traitement de données sensibles (par exemple, données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, données relatives à la vie sexuelle ou à la santé) sauf si [87]: - la personne concernée a donné son consentement explicite au traitement de ces données sensibles, sauf lorsque la législation applicable l'interdit; ou - le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail de l'UE, dans la mesure où il est autorisé par la 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 se trouve dans l'incapacité physique ou juridique de donner son consentement; ou - le traitement est effectué dans le cadre de leurs activités légitimes, avec des garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse ou syndicale, à	Lors de la détermination des utilisations autorisées des informations, il convient de prendre en considération la nature des informations [89]. Les garanties mises en œuvre en matière de sécurité sont raisonnables et proportionnelles à la probabilité et à la gravité du préjudice attendu, à la sensibilité des données et au contexte dans lequel elles sont conservées [90].

condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité 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 qui sont 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 requis 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 et, lorsque le traitement de ces données sensibles est effectué par un praticien de la santé soumis, par le droit national ou par des réglementations arrêtées par les autorités nationales compétentes, au secret professionnel ou par une autre personne également soumise à une obligation de secret équivalente. Les données sensibles doivent être traitées avec des mesures de sécurité renforcées [88].	

Références

[86] UE: voir directive 95/46, article 8; WP154, point 6, p. 5; APEC: voir cadre de protection de la vie privée, partie iii, principe VII, 22, p. 21.

[87] UE: voir directive 95/46, article 8; WP154, point 6, p. 5.

[88] UE: voir directive 95/46, article 17, paragraphe 1; WP154, point 10, p. 7.

[89] APEC: voir exigences du programme, p. 8.

[90] APEC: voir cadre de protection de la vie privée, partie iii, principe VII, 22, p. 21; exigences du programme, Q28, 30, 35(a), pp. 18-20.

14. Transparence et droit à l'information / avis

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

L'organisation doit faire une déclaration de confidentialité aisément accessible à toute personne concernée avant ou au moment de la collecte [91]. Cette déclaration décrit:

- la façon dont les personnes concernées sont informées du transfert et du traitement de leurs données à caractère personnel [92];
- l'identité du ou des responsables du traitement et de leurs représentants, le cas échéant, et un point de contact [93];
- les finalités du traitement auquel les données collectées sont destinées [94];
- toute information supplémentaire telle que:
  i. les destinataires ou les catégories de destinataires des données [95];
  ii. l'existence d'un droit d'accès aux données la concernant et de rectification de ces données, ainsi que la façon dont les personnes concernées peuvent avoir accès à leurs données à caractère personnel [96];

Lorsque les données n'ont pas été collectées auprès de la personne concernée, il existe certaines circonstances dans lesquelles l'obligation d'informer la personne concernée peut ne pas s'appliquer [97]. Ces exceptions diffèrent dans les REC et les RTPVP. Les exigences spécifiques au programme en matière de REC et de RTPVP sont précisées dans les règles de protection des données à caractère personnel et de la vie privée d'une organisation.

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
De plus amples informations sont communiquées aux personnes concernées dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont collectées, ces informations sont nécessaires pour assurer, à l'égard de la personne concernée, un traitement loyal des données [98]. Lorsque les données n'ont pas été collectées auprès de la personne concernée, l'obligation d'informer cette dernière ne s'applique pas lorsque 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 [99]. Si l'obligation d'informer la personne	L'organisation doit également indiquer aux personnes concernées la façon dont les données sont collectées et si elles sont collectées [100]: - directement auprès de la personne; ou - auprès de tiers qui les collectent pour le compte du responsable du traitement; ou - autrement (à préciser). Il existe des circonstances où l'avis peut ne pas être nécessaire ou réalisable [101]: - évidence; - collecte d'informations accessibles au public; - impossibilité technologique;

concernée peut ne pas s'appliquer dans la circonstance susmentionnée, elle ne disparaît pas aux motifs de l'évidence, ni de la disponibilité publique des données à caractère personnel traitées, ni de l'impossibilité technologique d'informer la personne concernée, ni au seul motif que les données à caractère personnel ont été reçues d'un tiers.	- réception de tiers; - divulgation à une institution gouvernementale ayant présenté une demande d'information légalement autorisée; - divulgation à un tiers conformément à un processus légal; - fins d'enquête légitime; - mesure en cas d'urgence. Informations supplémentaires à communiquer aux personnes concernées: - le fait que les données à caractère personnel sont collectées [102]; - les finalités pour lesquelles les données sont mises à la disposition de tiers [103]; - les informations concernant l'utilisation et la divulgation des données des personnes concernées [104]; - le choix et les moyens proposés aux personnes concernées pour limiter l'utilisation et la divulgation de leurs données à caractère personnel [105].

Références

[91] UE: voir directive 95/46, articles 10 et 11; WP153, point 1.7, p. 5; WP74, point 5.7, p. 19; WP154, point 7, p. 5; APEC: voir cadre de protection de la vie privée, partie iii, principe II, 15 et 16, pp. 12-13 et 16, p. 13.

[92] UE: voir WP74, point 5.7, p. 19; WP153, point 6.1.i, p. 10; APEC: voir questionnaire d'inscription, Q1, p. 4; Q17-19, pp. 10-11.

[93] UE: voir WP154, point 7, p. 5; APEC: voir questionnaire d'inscription, Q1-d), pp. 4-5.

[94] UE: voir WP154, point 7, p. 5; APEC: voir questionnaire d'inscription, Q1-b) and Q3, pp. 4-5.

[95] UE: voir WP154, point 7, p. 5; APEC: voir cadre de protection de la vie privée, partie iii, principe II, 15-c), p. 12.

[96] UE: voir WP154, point 7, p. 5; APEC: voir cadre de protection de la vie privée, partie iii, principe II, 15-e), p. 12; questionnaire d'inscription, Q38- a), p. 18.

[97] UE: voir directive 95/46, articles 10 et 11; APEC: voir questionnaire d'inscription, *Qualifications to the Provision of Notice*, p. 6.

[98] UE: voir directive 95/46, article 10.

[99] UE: voir directive 95/46, article 11.

[100] APEC: voir questionnaire d'inscription, Q1-a), p. 4 and Q5, p. 7.

[101] APEC: voir questionnaire d'inscription, *Qualifications to the Provision of Notice*, p. 6.

[102] APEC: voir cadre de protection de la vie privée, partie iii, principe II, 15-a), p. 12.

[103] APEC: voir questionnaire d'inscription, Q1-c), p. 4.

[104] APEC: voir questionnaire d'inscription, Q1-e), p. 5.

[105] APEC: voir cadre de protection de la vie privée, partie iii, principe II, 15-e), p. 12; questionnaire d'inscription, Q15-16, p. 10.

15. Droits d'accès, rectification, effacement et verrouillage des données/accès et correction

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

L'organisation doit veiller à ce que [106]:

- toute personne concernée puisse obtenir du responsable du traitement la confirmation que ce dernier détient ou non des données à caractère personnel la concernant [107];
- toute personne concernée puisse obtenir une copie de toutes les données la concernant qui sont détenues par l'organisation. Les données pertinentes doivent être fournies sans contrainte, à des délais raisonnables et sans tarifs excessifs (le cas échéant) [108];
- toute personne concernée puisse demander à un responsable du traitement de rectifier ou de supprimer des données qui sont notamment incomplètes ou inexactes [109].

Ces obligations sont soumises à des exceptions et des conditions conformément à la législation applicable [110].

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
Les éléments énumérés dans le référentiel commun ci-dessus sont des droits accordés aux personnes concernées. Les règles de protection des données à caractère personnel et de la vie privée d'une organisation doivent également veiller à ce que toute personne concernée ait le droit d'obtenir du responsable du traitement le verrouillage des données, notamment en raison du caractère incomplet ou inexact des données [111].	Les responsables du traitement prennent des mesures pour confirmer l'identité de la personne concernée qui demande l'accès [112]. Lorsque des informations sont communiquées à une personne concernée ayant exercé son droit d'accès, les informations sont communiquées d'une manière raisonnable, généralement compréhensible et de façon compatible avec la forme d'interaction régulière avec la personne [113]. Un engagement selon lequel les corrections ou les suppressions sont effectuées dans un délai raisonnable [114]. Les responsables du traitement fournissent une copie des données à caractère personnel corrigées ou donnent aux personnes concernées une confirmation de la correction ou de la suppression de leurs données [115]. Les responsables du traitement fournissent aux personnes concernées une explication de la raison pour laquelle l'accès ou la correction ne seront pas accordés, accompagnée de coordonnées pour d'autres demandes de

	renseignements concernant le refus d'accès ou de correction [116].
Exceptions aux droits d'accès (REC) Les lois nationales de protection des données dans l'UE peuvent prévoir certaines exceptions au droit d'accès des personnes concernées, fondées sur le droit national dans l'UE et à interpréter de façon restrictive, auxquels cas il peut être nécessaire pour les organisations de refuser des demandes d'accès afin de sauvegarder les intérêts des États membres de l'UE en ce qui concerne [117]: a) la sureté de l'État; b) la défense; c) la sécurité publique; d) la prévention, la recherche, la détection et la poursuite d'infractions pénales, ou de manquements à la déontologie dans le cas des professions réglementées; e) un intérêt économique ou financier important d'un État membre de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal; f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e); g) la protection de la personne concernée ou des droits et libertés d'autrui. Les lois nationales de protection des données dans l'UE peuvent disposer que, sous réserve de garanties légales appropriées, excluant notamment que les données puissent être utilisées aux fins de mesures ou de décisions se rapportant à des personnes précises, le droit d'accès des personnes concernées peut, dans le cas où il n'existe manifestement aucun risque d'atteinte à la vie privée de la personne	**Exceptions aux demandes d'accès (RTPVP)** Il existe des circonstances dans lesquelles il peut être nécessaire pour les organisations de refuser les demandes d'accès [118]: - charge disproportionnée; - protection des informations à caractère confidentiel; - risque lié aux tiers.

concernée, être limité lorsque les données sont traitées exclusivement aux fins de la recherche scientifique ou sont stockées sous la forme de données à caractère personnel pendant une durée n'excédant pas celle nécessaire à la seule finalité d'établissement de statistiques.	

Références

[106] UE: voir directive 95/46, article 12; WP153, point 6.1.v., p. 10; WP108, point 8.2.5, p. 8.

[107] APEC: voir cadre de protection de la vie privée, partie iii, principe VIII, 23-a), p. 22; questionnaire d'inscription, Q36, p. 17.

[108] APEC: voir cadre de protection de la vie privée, partie iii, principe VIII, 23-b), p. 22, questionnaire d'inscription, Q37, 37-b, 37-e), pp. 17-18.

[109] APEC: voir cadre de protection de la vie privée, partie iii, principe VIII, 23-c), p. 22; questionnaire d'inscription, Q38, 38-b, pp. 18-19.

[110] UE: voir directive 95/46, article 13; APEC: voir questionnaire d'inscription, conditions de la fourniture de mécanismes d'accès et de correction, pp. 19-20., pp. 19-20.

[111] UE: voir directive 95/46, article 12.

[112] APEC: voir questionnaire d'inscription, Q37-a), p. 17.

[113] APEC: voir questionnaire d'inscription, Q37-c) et d), p. 18.

[114] APEC: voir questionnaire d'inscription, Q38-a), p. 19.

[115] APEC: voir questionnaire d'inscription, Q38-d), p. 19.

[116] APEC: voir cadre de protection de la vie privée, partie iii, principe VIII, 25, p. 24, questionnaire d'inscription, Q38-e), p. 19

[117] UE: voir directive 95/46, article 13.

[118] APEC: voir questionnaire d'inscription, conditions de la fourniture de mécanismes d'accès et de correction, pp. 19-20.

16. Droit d’opposition / choix

Éléments communs requis à la fois pour l’approbation des REC et la certification des RTPVP

Le cas échéant ou si la législation applicable l’exige, l’organisation doit veiller à ce que la personne concernée puisse s’opposer à ce que les données à caractère personnel la concernant fassent l’objet d’un traitement ou choisir que ses données à caractère personnel ne fassent pas l’objet d’un traitement, conformément à la législation applicable [119].

Éléments complémentaires requis pour l’approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée d’une organisation doivent veiller également à ce que toute personne concernée ait le droit de s’opposer au traitement de ses données à caractère personnel, étant donné qu’il s’agit d’un droit accordé aux personnes concernées. Le droit d’opposition peut être exercé par les personnes concernées à tout moment. Plus particulièrement, toute personne concernée à le droit de s'opposer, sur demande et gratuitement, au traitement des données à caractère personnel la concernant, envisagé par le responsable du traitement à des fins de prospection ou d'être informée avant que des données à caractère personnel ne soient communiquées pour la première fois à des tiers ou utilisées pour leur compte à des fins de prospection et de se voir expressément offrir le droit de s'opposer, gratuitement, à cette communication ou utilisation.	S.O.
Exceptions au droit d’opposition (REC) S.O.	**Exceptions au choix (RTPVP)** Il existe certaines circonstances dans lesquelles il peut ne pas être nécessaire ou réalisable pour les organisations de fournir des mécanismes de choix aux personnes [120 - évidence; - collecte d'informations accessibles au public;

	- impossibilité technologique; - réception de tiers; - divulgation à une institution gouvernementale ayant présenté une demande d'information légalement autorisée; - divulgation à un tiers conformément à un processus légal; - fins d'enquête légitime; - mesure en cas d'urgence.
Clarification du droit d'opposition (REC) Une personne concernée a toujours le droit de retirer son consentement. En outre, lorsqu'il existe une autre base légale légitimant le traitement, les personnes concernées peuvent toujours s'y opposer. De plus, les lois nationales de protection des données dans l'UE prévoient les circonstances dans lesquelles la personne concernée peut, du moins lorsque la base légale du traitement découle de l'article 7, points e) ou f), de la directive 95/46/CE, s'opposer, pour des raisons impérieuses et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf en cas de disposition contraire du droit national des États membres de l'UE. En cas d'opposition justifiée, le traitement mis en œuvre par le responsable du traitement ne peut plus porter sur ces données [121]. Le droit de s'opposer ne disparaît pas aux motifs de l'évidence, ni de la disponibilité publique des données à caractère personnel traitées, ni de l'impossibilité technologique d'informer la personne concernée, ni au seul motif que les données à caractère personnel ont été reçues d'un tiers.	**Clarification du choix (RTPVP)** Les organisations sont tenues de fournir aux personnes des mécanismes de choix en ce qui concerne la collecte, l'utilisation et la divulgation de leurs informations à caractère personnel [122].

Références

[119] UE: voir directive 95/46, article 14, WP153, point 6.1.v, p. 10; WP108, point 8.2.5, p. 8; APEC: voir questionnaire d'inscription, Q14-16.

[120] APEC: voir questionnaire d'inscription, «*Qualifications to the Provision of Choice Mechanisms*», pp. 11-12.

[121] UE: voir directive 95/46, article 14.

[122] APEC: voir exigences du programme, Q14 à 16, pp. 11-13.

17. Décisions individuelles automatisées

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

S.O.

Éléments requis pour l'approbation des REC	**Éléments requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent un engagement selon lequel aucune évaluation ou décision relative à la personne concernée et affectant cette dernière de manière significative ne sera uniquement basée sur le traitement automatisé de ses données sauf si la décision [123]: - est prise lors 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 ses intérêts légitimes; ou - est autorisée par une loi qui précise également les mesures garantissant la sauvegarde des intérêts légitimes de la personne concernée.	S.O.

Références

[123] UE: voir WP154, point 9, p. 6.

18. Sécurité et confidentialité

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent une exigence selon laquelle des mesures techniques et d'organisation appropriées ont été mises en œuvre pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la divulgation ou l'accès non autorisés ainsi que contre toute autre forme de traitement illicite [124].

Ces mesures doivent assurer un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger [125].

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également une exigence selon laquelle les mesures de sécurité doivent être mises en œuvre compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre [126].	Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également une exigence selon laquelle les mécanismes de sécurité doivent faire l'objet d'un examen et d'une réévaluation périodiques [127]. Une politique relative à la sécurité de l'information [128] et une politique pour le retrait sécurisé de données à caractère personnel sont mises en œuvre [129]. Des mécanismes sont mis en œuvre afin de détecter, prévenir et répondre aux attaques, intrusions ou autres défaillances en matière de sécurité [130]. Le personnel doit également avoir conscience de l'importance de la préservation de la sécurité des données à caractère personnel et des obligations afférentes par le biais d'une formation régulière et d'une surveillance telles que démontrées par des procédures [131].

Références

[124] UE: voir directive 95/46, article 17, paragraphe 1; WP108, point 8.2.4, p. 8; APEC: voir cadre de protection de la vie privée, partie iii, principe VII, 22, p. 2; questionnaire d'inscription, Q27, p. 14.

[125] UE: voir directive 95/46, article 17, paragraphe 1; APEC: voir cadre de protection de la vie privée, partie iii, principe VII, 22, p. 21, questionnaire d'inscription, Q28, p. 14.

[126] UE: voir directive 95/46, article 17, paragraphe 1.

[127] APEC: voir cadre de protection de la vie privée, partie iii, principe VII, 22, p. 21.

[128] APEC: voir questionnaire d'inscription, Q26, p. 14.

[129] APEC: voir questionnaire d'inscription, Q31, p. 15.

[130] APEC: voir questionnaire d'inscription, Q32 and 33, p. 15.

[131] APEC: voir questionnaire d'inscription, Q29 and 30-a), p. 14.

19. Programme de formation

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation prévoient une formation appropriée concernant lesdites règles pour son personnel [132].

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
L'exigence de formation concerne le personnel qui a un accès permanent ou régulier aux données à caractère personnel et participe à leur collecte ou à l'élaboration d'outils pour les traiter [133].	La formation couvre les politiques et procédures de protection de la vie privée, y compris la manière de répondre aux plaintes en matière de protection de la vie privée [134]. Le personnel doit également avoir conscience de l'importance de la préservation de la sécurité des données à caractère personnel et des obligations afférentes par le biais d'une formation régulière et d'une surveillance telles que démontrées par des procédures [135].

Références

[132] UE: voir WP74, point 5.1, p. 16; APEC: voir questionnaire d'inscription, Q44, p. 22.

[133] UE: voir WP153, point 2.1, p. 5.

[134] APEC: voir exigences du programme, Q44, pp. 25-26.

[135] APEC: voir questionnaire d'inscription, Q30-a), p. 14.

20. Programme de contrôle et d'audit

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation prévoient un contrôle de l'application desdites règles ainsi que de la conformité à ces règles [136].

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également une obligation de contrôler le respect desdites règles par le groupe, et notamment une obligation en vertu de laquelle [137]: - le programme d'audit couvre tous les aspects des règles de protection des données à caractère personnel et de la vie privée de l'organisation, y compris les méthodes garantissant la mise en œuvre de mesures correctives; - cet audit doit être réalisé régulièrement (préciser le moment) par l'équipe d'audit interne ou externe accréditée ou sur demande spécifique du responsable/agent de la protection de la vie privée (ou de tout autre agent compétent dans l'organisation); - les résultats de tous les audits doivent être communiqués au responsable/agent de la protection de la vie privée (ou à tout autre agent compétent dans l'organisation) et au conseil d'administration; - les APD de l'UE reçoivent une copie de ces audits sur demande; - le plan d'audit doit permettre aux APD de l'UE d'exécuter un audit de la protection des données en cas de besoin; - chaque membre du groupe accepte d'être soumis à un audit réalisé par les APD de l'UE et déclare qu'il se	Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également une exigence selon laquelle le responsable du traitement atteste, tous les ans, du respect continu des exigences du programme RTPVP [138]. Des examens réguliers et complets seront réalisés par des agents de responsabilisation de l'APEC afin de garantir l'intégrité ou la re-certification [139]. Le responsable du traitement procédera régulièrement à une vérification ou à un contrôle sur place de ses sous-traitants en charge du traitement des données à caractère personnel, agents, contractants ou autres prestataires de services afin de s'assurer du respect de ses instructions et/ou accords/contrats [140].

conformera à l'avis des APD de l'UE sur toute question liée à ces règles.	

Références

[136] UE: voir WP74, point 5.2, p. 16; APEC: voir demande d'agrément, annexe A, 6-8, p. 6.

[137] UE: voir WP153, point 2.3, p. 7.

[138] APEC: voir demande d'agrément, annexe A, 8, p. 6.

[139] APEC: voir demande d'agrément, annexe A, 8, p. 6.

[140] APEC: voir questionnaire d'inscription, Q49, p. 23.

21. Conformité et contrôle de la conformité

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation prévoient la désignation du personnel approprié (tel qu'un réseau de responsables de la protection de la vie privée) afin de surveiller et garantir la conformité auxdites règles [141].

Éléments complémentaires requis pour l'approbation des REC [142]	**Éléments complémentaires requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également une brève description de la structure interne, du rôle et des responsabilités du réseau des responsables de la protection de la vie privée ou de la fonction similaire créée afin de garantir la conformité auxdites règles. Le personnel approprié ainsi désigné bénéficie du soutien de la direction. Exemple de structure interne, de rôle et de responsabilités du réseau des responsables de la protection de la vie privée ou de la fonction similaire créée afin de garantir la conformité aux règles de protection des données à caractère personnel et de la vie privée de l'organisation: le responsable principal de la protection de la vie privée formule des conseils à l'intention du conseil d'administration, s'occupe des enquêtes menées par les APD nationales dans l'UE, rend compte chaque année de la conformité, garantit la conformité au niveau mondial et veille à ce que les responsables de la protection de la vie privée puissent être chargés de traiter les plaintes locales émanant des personnes concernées, de lui rendre compte des principaux problèmes relatifs au respect de la vie privée et de garantir la conformité au niveau local.	Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également une exigence selon laquelle la ou les personnes désignées mettent en œuvre des procédures opportunes pour recevoir, donner suite et répondre aux plaintes liées au respect de la vie privée, en donnant une explication de toute mesure corrective le cas échéant [143].

Références

[141] UE: voir WP74, point 5.1, p. 16; APEC: voir questionnaire d'inscription, Q40, p. 21.

[142] UE: voir WP153, point 2.4, p. 8.

[143] APEC: voir exigences du programme, Q40, pp. 24-25.

22. Mécanismes de plaintes internes

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation mettent en place un processus de traitement des plaintes dans le cadre duquel [144]:

- toute personne concernée peut se plaindre du non-respect des règles de protection des données à caractère personnel et de la vie privée de l'organisation par un membre du groupe;
- les plaintes sont traitées par un département/une personne clairement identifié(e).

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
Le département ou la personne identifié(e) qui traite les plaintes doit bénéficier d'un niveau d'indépendance approprié dans l'exercice de ses fonctions [145].	L'engagement que la réponse fournie aux personnes concernées à propos de leurs plaintes comprend une explication de l'action corrective relative à leurs plaintes [146].

Références

[144] UE: voir WP74, point 5.3, p. 17; APEC: voir questionnaire d'inscription, Q41-42, p. 21.

[145] UE: voir WP74, point 5.3, p. 17.

[146] APEC: voir questionnaire d'inscription, Q43, p. 21.

23. Mises à jour des règles de protection des données à caractère personnel et de la vie privée d'une organisation

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation prévoient la notification de toute modification significative apportée auxdites règles ou à la liste des membres, à tous les membres du groupe ainsi qu'aux APD de l'UE et agents de responsabilisation de l'APEC, afin de prendre en compte les modifications de l'environnement règlementaire et de la structure de l'entreprise et, plus précisément, du fait que certaines modifications pourraient exiger une nouvelle autorisation des APD nationales de l'UE et/ou entraîner un examen par les agents de responsabilisation de l'APEC [147].

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également un engagement selon lequel les modifications substantielles apportées auxdites règles seront également communiquées aux personnes concernées [148]. Il est possible de mettre à jour les règles de protection des données à caractère personnel et de la vie privée de l'organisation ou la liste des membres du groupe liés par lesdites règles sans devoir redemander une autorisation, à condition que [149]: i) une personne identifiée garde une liste constamment actualisée des membres du groupe et conserve une trace de toute mise à jour des règles de protection des données à caractère personnel et de la vie privée de l'organisation, les enregistre et fournisse les informations nécessaires aux personnes concernées ainsi qu'aux APD nationales de l'UE sur demande; ii) aucun transfert ne soit effectué vers un nouveau membre jusqu'à ce que ce dernier soit effectivement lié par les règles de protection des données à caractère personnel et de la vie privée	Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent également une exigence selon laquelle, lorsqu'une modification matérielle desdites règles (telle que raisonnablement déterminée de bonne foi par l'agent de responsabilisation de l'APEC) est intervenue, un processus d'examen immédiat est exécuté par l'agent de responsabilisation [150]. Les organisations doivent fournir une déclaration actualisée de leurs pratiques et politiques en ce qui concerne les informations à caractère personnel [151]. En outre, les organisations sont tenues de fournir aux personnes des mécanismes de choix en ce qui concerne la collecte, l'utilisation et la divulgation de leurs informations à caractère personnel [152].

de l'organisation et puisse garantir la conformité; iii) toute modification des règles de protection des données à caractère personnel et de la vie privée de l'organisation ou de la liste des membres soit communiquée une fois par an aux APD nationales de l'UE qui délivrent les autorisations, avec une brève explication des raisons justifiant la mise à jour.	

Références

[147] UE: voir WP74, point 4.2, p. 15; APEC: voir demande d'agrément, annexe A, 8, p. 6.

[148] UE: voir WP154, point 21, pp. 9-10.

[149] UE: voir WP74, point 4.2, p. 15.

[150] APEC: voir demande d'agrément, annexe A, 8, p. 6.

[151] APEC: voir cadre de protection de la vie privée, partie iii, principe II, 15; questionnaire d'inscription, Q1, p. 4.

[152] APEC: voir exigences du programme, Q14 to 16, pp. 11-13.

24. Actions en cas de risque de législation locale empêchant le respect des règles de protection des données à caractère personnel et de la vie privée d'une organisation et en cas de demande d'accès par les autorités chargées de l'application du droit

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

S.O.

Éléments requis pour l'approbation des REC [153]	**Éléments requis pour la certification des RTPVP**
Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent une disposition indiquant clairement que lorsqu'un membre du groupe a des raisons de croire que la législation qui lui est applicable l'empêche de satisfaire à ses obligations, conformément aux règles de protection des données à caractère personnel et de la vie privée de l'organisation, et a un impact important sur les garanties qui y sont prévues, ce membre informe rapidement le siège dans l'UE ou le membre de l'UE ayant des responsabilités déléguées en matière de protection des données ou l'autre agent chargé de la protection de la vie privée (sauf en cas d'interdiction par une autorité judiciaire, telle qu'une interdiction en vertu du droit pénal afin de préserver la confidentialité d'une enquête judiciaire). En outre, les règles de protection des données à caractère personnel et de la vie privée d'une organisation prévoient qu'en cas de conflit entre la législation nationale et les obligations, les exigences et les engagements prévus dans lesdites règles, le siège dans l'UE, le membre de l'UE ayant des responsabilités déléguées en matière de protection des données ou l'autre agent chargé de la protection de la vie privée doivent consulter les APD nationales compétentes de l'UE et arrêter une décision responsable sur les mesures à prendre. Tout incident concernant ce point des règles	Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contiennent une exigence selon laquelle une procédure doit avoir été instaurée pour couvrir les cas d'assignation, de mandat ou d'ordonnance des autorités judiciaires ou gouvernementales, y compris ceux exigeant la divulgation de données à caractère personnel [154].

de protection des données à caractère personnel et de la vie privée de l'organisation sera décrit en détail et examiné lors des audits réguliers mentionnés à la section 20.	

Références

[153] UE: voir WP74, point 3.3.3, pp. 13-14 et WP154, point 16, p. 8.

[154] APEC: voir questionnaire d'inscription, Q45, p. 22.

25. Assistance et coopération mutuelles avec les autorités nationales chargées de la protection des données dans l'UE / autorités chargées de protéger la vie privée de l'APEC

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

S.O.

Éléments requis pour l'approbation des REC	Éléments requis pour la certification des RTPVP
Les règles de protection des données à caractère personnel et de la vie privée d'une organisation contraignent [155]: - les membres du groupe à coopérer et à s'assister mutuellement afin de traiter toute demande ou plainte d'un particulier ou toute enquête ou investigation d'APD dans l'UE; - les entités à se soumettre à l'avis des APD nationales dans l'UE sur toute question concernant l'interprétation des règles de protection des données à caractère personnel et de la vie privée de l'organisation.	Les organisations des pays participants peuvent recevoir une certification des RTPVP. Les pays membres ne peuvent participer au système RTPVP que si leur autorité chargée de la protection de la vie privée (APVP) est une autorité participant à l'accord de coopération de l'APEC sur la protection transfrontière de la vie privée (CPEA) [156].

Références

[155] UE: voir WP74, point 5.4, p. 17.

[156] APEC: voir la charte du panel «JOP», point 2.2i, p. 15.

26. Relations entre la législation locale et les règles de protection des données à caractère personnel et de la vie privée de l'organisation

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

S.O.

Éléments requis pour l'approbation des REC	**Éléments requis pour la certification des RTPVP**
Lorsque des données à caractère personnel sont traitées dans l'UE, la législation européenne relative à la protection des données doit être appliquée. Les règles de protection des données à caractère personnel et de la vie privée d'une organisation confirment dès lors que [157]: - si la législation locale, la législation de l'UE par exemple, exige un niveau plus élevé de protection pour les données à caractère personnel, elle primera sur les règles de protection des données à caractère personnel et de la vie privée de l'organisation; - en tout état de cause, les données sont traitées conformément au droit de l'État membre concerné, conformément aux dispositions de l'article 4 de la directive 95/46/CE.	S.O.
Clarification des relations entre les lois locales et les REC S.O.	**Clarification des relations entre la législation locale et les RTPVP** [158] La participation au système RTPVP ne subroge pas les obligations juridiques nationales d'une organisation participante. Lorsqu'il n'existe pas d'exigences nationales applicables en matière de protection de la vie privée dans un pays, les règles de protection des données à caractère personnel et de la vie privée de l'organisation visent à offrir un niveau minimum de protection.

	Lorsque les exigences juridiques nationales sont plus strictes que celles prévues dans les règles de protection des données à caractère personnel et de la vie privée de l'organisation, cette législation et cette réglementation nationales s'appliquent dans toute leur mesure. Lorsque les exigences prévues dans les règles de protection des données à caractère personnel et de la vie privée de l'organisation sont plus strictes que celles de la législation et de la réglementation nationales, l'organisation devra respecter ces exigences supplémentaires afin de participer. Néanmoins, les autorités chargées de la protection de la vie privée dans ce pays doivent être habilitées à prendre des mesures d'application conformément à la législation et à la réglementation nationales applicables ayant pour effet de protéger les informations à caractère personnel en application des exigences des RTPVP.

Références

[157] UE: voir WP74, point 3.3.3, pp. 13-14.

[158] APEC: voir politiques, règles et lignes directrices, points 43 et 44, pp. 10-11.

27. Dispositions finales

Éléments communs requis à la fois pour l'approbation des REC et la certification des RTPVP

Les règles de protection des données à caractère personnel et de la vie privée d'une organisation précisent leur date d'entrée en vigueur [159].

Références

[159] UE: voir WP154, point 23, p. 10; APEC: voir exigences du programme, Q1, p. 2

Fait à Bruxelles, le 27 février 2014

Pour le groupe de travail
Le président
Jacob KOHNSTAMM

Annexes

Annexe 1. Les documents à fournir par une organisation sollicitant l'approbation de ses REC par les APD nationales dans l'UE et par une organisation sollicitant une certification de ses RTPVP par les agents de responsabilisation de l'APEC

Annexe 1. Documents à fournir par une organisation sollicitant l'approbation de ses REC par les APD nationales dans l'UE et par une organisation sollicitant la certification de ses RTPVP par les agents de responsabilisation de l'APEC

Une organisation demandant l'approbation de ses REC et la certification de ses RTPVP fournit aux APD nationales dans l'UE et à l'agent de responsabilisation de l'APEC tout document qui démontre que les obligations, les exigences et les engagements compris dans les règles de protection des données à caractère personnel et de la vie privée de l'organisation sont respectés, par exemple [160]:

- les politiques de protection de la vie privée (par exemple, la politique relative au respect de la vie privée du client, la politique relative au respect de la vie privée des RH) visant à informer les personnes concernées (par exemple, les clients, le personnel) quant à la façon dont l'entreprise protège leurs données à caractère personnel [161];

- les lignes directrices pour les membres du personnel ayant accès aux données à caractère personnel afin qu'ils puissent aisément comprendre et appliquer les règles prescrites dans le règlement sur le respect de la vie privée (par exemple, des lignes directrices sur la façon de répondre à une plainte émanant d'une personne concernée, sur la façon de fournir des informations aux personnes concernées, sur les mesures de sécurité/confidentialité appropriées à respecter) [162];

- des exemples et/ou explications du programme de formation [163];

- une description du système interne relatif aux plaintes [164];

- la politique de sécurité pour les systèmes informatiques traitant les données à caractère personnel de l'UE et de l'APEC [165];

- tous les contrats types devant être utilisés avec les sous-traitants (membres ou non du groupe) traitant des données à caractère personnel de l'UE et des données à caractère personnel de l'APEC, le cas échéant [166].

Éléments complémentaires requis pour l'approbation des REC	**Éléments complémentaires requis pour la certification des RTPVP**
L'organisation candidate fournit également aux APD nationales de l'UE: - une description de poste des responsables de la protection des données ou d'autres personnes chargées de la protection des données dans l'entreprise; - un formulaire de candidature	L'organisation candidate fournit également aux agents de responsabilisation de l'APEC: - un questionnaire d'inscription; - des exemples de documents complémentaires pouvant être nécessaires aux agents de responsabilisation de l'APEC afin de

type WP133 [167]; - un plan et un programme d'audit de la protection des données définis avec les personnes concernées (auditeurs accrédités internes/externes de l'entreprise); - des documents démontrant que le membre qui est à l'origine du transfert de données hors de l'UE et le siège dans l'UE ou le membre de l'UE ayant des responsabilités déléguées disposent d'avoirs suffisants pour permettre le paiement d'une indemnité couvrant les dommages résultant de la violation des règles de protection des données à caractère personnel et de la vie privée de l'organisation.	procéder à l'examen des règles de protection des données à caractère personnel et de la vie privée de l'organisation; - des exemples d'avis fournis aux personnes concernées [168]; - des documents démontrant la conformité aux limitations en matière de collecte des données, avec identification de [169]: i) chaque type de données collectées; ii) l'objectif déclaré de la collecte pour chaque type; iii) toutes les utilisations qui s'appliquent à chaque type de données; et iv) une explication de la compatibilité ou de l'interrelation entre chaque utilisation identifiée et l'objectif déclaré de la collecte. - des documents démontrant que les données à caractère personnel sont collectées, utilisées et divulguées aux fins identifiées ou à d'autres fins compatibles ou liées, sauf en cas de collecte autorisée dans des circonstances spécifiques [170]; - des documents montrant les mécanismes proposés aux personnes concernées afin qu'elles puissent exercer un choix en ce qui concerne la collecte, l'utilisation et la divulgation de leurs données à caractère personnel et démontrant que ces mécanismes sont en place et opérationnels et que les finalités de la collecte sont clairement mentionnées [171]; - des procédures mises en œuvre afin de vérifier et garantir que les données à caractère personnel détenues sont mises à jour, exactes et complètes, dans la

	mesure nécessaire aux fins de l'utilisation [172]; - des documents démontrant l'existence d'accords avec les sous-traitants, agents, contractants ou autres prestataires de services afin de garantir que les obligations du responsable du traitement envers les personnes concernées seront satisfaites [173].

Références

[160] UE: voir WP154, documents à fournir aux APD, pp. 10-11.

[161] APEC: voir exigences du programme, Q1, pp. 2-4.

[162] APEC: voir exigences du programme, Q29, p. 18; Q44, pp. 25-26.

[163] APEC: voir exigences du programme, Q44, pp. 25-26.

[164] APEC: voir exigences du programme, Q41-43, p. 25.

[165] APEC: voir exigences du programme, Q26, p. 17; Q31, p. 19.

[166] APEC: voir exigences du programme, Q46, pp. 26-27.

[167] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp133_en.doc

[168] APEC: voir exigences du programme, Q2, p. 4.

[169] APEC: voir exigences du programme, Q6, p. 6.

[170] APEC: voir exigences du programme, Q8, p. 8.

[171] APEC: voir exigences du programme, Q14-17, pp. 11-13.

[172] APEC: voir exigences du programme, Q21, p. 15.