FICHE DE RENSEIGNEMENTS
CONSULTATION JURIDIQUE

Date : 20 /01/2021

Pour mémoire, pour que votre question juridique soit prise en charge par le syndicat, il faut que la réponse puisse être généralisable. Ce présent template anonymisé sera partagé sur l'intranet du syndicat www.relations-publics.org/soutien-administratif-et-jurifique

Catégorie de question : Corporate/fiscal Social x IT/Data

Titre de la question : L'utilisation d'une messagerie google (gmail) est-elle compatible avec la conformité RGPD de l'agence (vs l'hébergement des données à l'étranger).

(*Exemple : Imposer à mes collaborateurs de poser des jours de congés / RTT)*

Contexte : Dans le cadre de notre processus de mise en conformité RGPD, nous nous interrogeons sur la possibilité d'utiliser google comme fournisseur de messagerie électronique. Actuellement, Gmail est le fournisseur de notre messagerie agence.
Notre DPO nous dit que la CNIL nous interdit d'utiliser les services google (G Suite, Drive, google meet, recaptcha, G mail, etc.…), étant donné que ses serveurs sont situés aux USA. Il se réfère à la décision de la CJUE du 15 juillet 2020
Il nous recommande l'utilisation de deux hébergeurs de données, de sites web et de création d'adresses sont sûrs RGPD : OVH et Ionos. Google à bannir

Pourriez-vous nous éclairer sur cette « interdiction » ? Quelle est votre recommandation ?

N'oubliez pas de préciser tous les éléments utiles : type de contrat, CDD/CDI, ancienneté etc. Au besoin, le cabinet d'avocat prendra contact avec vous pour vous demander de plus amples renseignements.

Réponse du cabinet d'avocat :

Les solutions proposées par Google (cf. Gmail, Google Drive, G Suite, Google +, Google Meet, Google Forms, Recaptcha, etc.) sont effectivement des services qui impliquent des transfert de données à caractère personnel hors Union européenne (également désignés sous le vocabulaire de « flux transfrontières de données ») vers les Etats-Unis.

Pour mémoire, il existe un flux transfrontière de données lorsque des données sont transférées depuis un Etat membre de l'Union européenne vers un Etat non membre de l'Union européenne. Un tel transfert peut s'effectuer par communication, copie ou déplacement de données, par l'intermédiaire d'un réseau (ex : accès à distance à une base de données) ou d'un support à un autre, quel que soit le type de support (ex : d'un disque dur d'ordinateur à un serveur).

* *
*

FICHE DE RENSEIGNEMENTS
CONSULTATION JURIDIQUE

I. Les hypothèses dans lesquelles des flux transfrontières de données à caractère personnel hors Union européenne peuvent être mis en œuvre

Les transferts de données à caractère personnel à destination de pays hors Union européenne ou d'organisations internationales, ou flux transfrontières de données, doivent être identifiés dans la mesure où de tels transferts sont autorisés si, et seulement si, certaines conditions sont respectées aux fins de s'assurer que le pays ou l'entreprise destinataire assure un niveau de protection suffisant aux données transférées. En effet, lorsque des données font l'objet de tels transferts, le niveau de protection des données des personnes physiques ne doit pas être compromis (cf. articles 44 et suivants du règlement (UE)2016/679 du 27 avril 2016 dit « RGPD »).

En premier lieu, un tel transfert de données à caractère personnel peut avoir lieu si le pays tiers ou l'organisation internationale a été reconnu(e) par la Commission européenne comme assurant un niveau adéquat de protection des données. Dans cette hypothèse, aucune autorisation spécifique n'est nécessaire pour mettre en œuvre le transfert de données.

A ce jour, les pays reconnus par une décision d'adéquation comme offrant un niveau suffisant de protection des données à caractère personnel sont les suivants : la Suisse, le Canada, l'Argentine, Guernesey, l'Ile de Man, Jersey, Andorre, les Iles Féroé, Israël, l'Uruguay, la Nouvelle-Zélande et le Japon. Les Etats de l'Espace économique européen non membres de l'Union européenne (la Norvège, l'Islande et le Lichtenstein) sont également considérés comme disposant d'un niveau de protection adéquat.

Il en était de même jusqu'à présent lorsque le destinataire des données était établi aux Etats-Unis et adhérent au Privacy Shield (ce qui est entre autres le cas de Google). Néanmoins, la Cour de justice de l'Union européenne (CJUE, n°C-311/18 du 16 juillet 2020) a invalidé la décision d'adéquation de la Commission européenne relative à ce mécanisme, ce dont il résulte que **l'adhésion au Privacy Shield de l'organisme destinataire n'est plus valable pour encadrer les flux transfrontières de données vers les Etats-Unis conformément aux dispositions européennes et françaises applicables**.

En deuxième lieu, le transfert peut être fondé sur un mécanisme assurant des garanties appropriées. En fonction du mécanisme retenu, une autorisation de l'autorité de contrôle (en France, la Commission nationale de l'informatique et des libertés, ou « Cnil ») peut devoir être obtenue. Ces mécanismes sont listés dans le tableau *infra*, selon qu'une autorisation de l'autorité de contrôle est nécessaire ou non :

Absence de nécessité d'une autorisation particulière	Nécessité d'une autorisation de l'autorité de contrôle
Instrument juridique contraignant et exécutoire entre les autorités ou organismes publics concernés.	Dispositions à intégrer dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits effectifs et opposables pour les personnes concernées.

FICHE DE RENSEIGNEMENTS
CONSULTATION JURIDIQUE

Règles d'entreprise contraignantes (couramment désignées sous le terme anglais « binding corporate rules » ou « BCR »). *<u>Précision</u> : les BCR concernent un groupe d'entreprises, leur contenu est régi par le RGPD et ce document doit être validé par l'autorité de contrôle avant de pouvoir constituer un fondement valable pour les transferts de données.*	Clauses contractuelles ad hoc entre d'une part le responsable de traitement ou le sous-traitant, et d'autre part l'organisme situé dans un pays tiers ou l'organisation internationale.
Clause contractuelles types (ou CCT) adoptées par la Commission européenne ou par l'autorité de contrôle et approuvées par la Commission européenne.	
Code de conduite / mécanisme de certification approuvé, dans les conditions du RGPD, assorti de l'engagement contraignant et exécutoire pris par le destinataire des données dans le pays tiers d'appliquer les garanties appropriées, y compris pour ce qui concerne les droits des personnes concernées.	

Focus sur les clauses contractuelles types

A ce jour, la Commission européenne a élaboré les clauses contractuelles types suivantes :
- clauses contractuelles types pour le transfert des données depuis un responsable de traitement en Union européenne (exportateur) vers un responsable de traitement hors Union européenne (importateur) → version 2001 : décision 2001/497/CE du 15 juin 2001 et version 2004 : décision 2004/915/CE du 27 décembre 2004 ;
- clauses contractuelles types pour le transfert des données depuis un responsable de traitement en Union européenne (exportateur) vers un sous-traitant hors Union européenne (importateur) → version 2010 : décision 2010/87/UE.

Toutefois, la Commission européenne a publié, le 12 novembre 2020, un projet de nouvelles clauses contractuelles types, lesquelles ont vocation à encadrer les flux transfrontières de données à caractère personnel :
- d'un responsable de traitement vers un autre responsable de traitement ;
- d'un responsable de traitement vers un sous-traitant ;
- d'un sous-traitant vers un autre sous-traitant ;
- d'un sous-traitant vers un responsable de traitement.

Ces clauses contractuelles types, une fois entrées en vigueur dans leur version définitive, auront vocation à remplacer celles en vigueur à date et il conviendra donc de les conclure avec les cocontractants appropriés (dans les futurs contrats ou en remplacement -par voie d'avenant- le cas échéant de celles déjà conclues dans leur version en vigueur à ce jour dans les contrats en cours).

<u>En troisième lieu, des dérogations pour des situations particulières sont également prévues par la règlementation applicable en matière de protection des données à caractère personnel en l'absence de décision d'adéquation ou de garanties appropriées, étant précisé que ces dérogations risquent de faire l'objet d'une interprétation restrictive par les autorités de contrôle et ne doivent donc être utilisées pour fonder un transfert de données qu'avec prudence, après une analyse approfondie préalable du respect des conditions posées par le RGPD</u>.

Ainsi, des transferts de données vers des Etats hors Union européenne ou vers une organisation internationale peuvent être mis en œuvre à condition de répondre à une des conditions suivantes :
- la personne concernée a consenti explicitement au transfert ;
- le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable de traitement, ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée ;
- le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable de traitement et un tiers ;
- le transfert est nécessaire pour des motifs importants d'intérêt public reconnus par le droit de l'Union européenne ou le droit de l'Etat membre auquel le responsable de traitement est soumis ;
- le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice ;
- le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité de donner son consentement ;
- le transfert a lieu au départ d'un registre qui est destiné à fournir des informations au public et est ouvert à la consultation du public en général, ou de toute personne justifiant d'un intérêt légitime (uniquement conformément aux conditions prévues dans le droit de l'Union européenne ou de l'Etat membre concerné).

<u>Enfin, si aucune de ces dérogations n'est applicable, un transfert de données vers un Etat hors Union européenne ou une organisation internationale ne peut être mis en œuvre que si les conditions suivantes sont cumulativement remplies</u>, de tels transferts ne devant être mis en œuvre que dans des hypothèses résiduelles :
- absence de caractère répétitif ;
- nombre limité de personnes concernées ;
- transfert nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable de traitement sur lesquels ne prévalent pas les intérêts ou droits et libertés des personnes concernées ;
- évaluation par le responsable de traitement de toutes les circonstances entourant le transfert (notamment au regard de la nature des données transférées, à la finalité et à la durée des opérations, ainsi qu'à la situation du pays d'origine et du pays destinataire) et garanties appropriées prises sur la base de cette évaluation ;
- information de l'autorité de contrôle ;
- information de la personne concernée notamment sur le transfert et les intérêts légitimes impérieux poursuivis.

En l'espèce, s'agissant des transferts de données à caractère personnel mis en œuvre vers les Etats-Unis du fait de l'utilisation des services Google, il apparaît que, la décision d'adéquation du Privacy Shield ayant été « invalidée » par la CJUE, seule la conclusion de clauses contractuelles types (ou CCT) avec l'entité(les entités) importatrice(s) pouvant accéder aux données, traiter les données, etc… aux Etats-Unis pourrait permettre d'encadrer de tels flux transfrontières.

* *
*

II. L'impossibilité de recourir aux « seules » CCT pour les transferts de données à caractère personnel vers les Etats-Unis

La CJUE, dans sa décision précitée du 16 juillet 2020, si elle ne remet pas en cause la validité des clauses contractuelles types (CCT) émises par la Commission européenne, précise cependant que **le recours aux CCT pour le transfert de données à caractère personnel ne peut, à lui seul, permettre d'encadrer valablement un tel transfert vers les Etats-Unis.**

En effet, **la CJUE, après avoir examiné la décision de la Commission européenne relative aux clauses contractuelles types, la juge valide. Toutefois, elle ajoute que cette validité dépend de la question de savoir si cette décision comporte des mécanismes efficaces permettant, en pratique, d'assurer le respect du niveau de protection essentiellement équivalent à celui garanti au sein de l'Union Européenne par le RGPD et de suspendre ou d'interdire les transferts de données à caractère personnel opérés au moyen de telles clauses en cas de violation de ces clauses ou d'impossibilité de les respecter**.

À cet égard, la CJUE rappelle que cette décision :
- impose à l'exportateur et à l'importateur de données l'obligation de vérifier, préalablement à tout transfert hors Union européenne, en prenant en compte les circonstances du transfert, si le niveau de protection est respecté dans le pays tiers concerné ;
- exige que l'importateur de données informe l'exportateur de données de toute incapacité à se conformer aux CCT et, le cas échéant, à toute mesure complémentaire à celles prévues par les clauses, l'exportateur de données étant alors, en contrepartie, dans une telle hypothèse, tenu de suspendre le transfert de données et/ou de résilier le contrat avec l'importateur de données.

La CJUE ajoute que les garanties appropriées, les droits opposables et les voies de droit effectives requis par le RGPD doivent assurer que les droits des personnes dont les données à caractère personnel sont transférées vers un pays tiers sur le fondement de clauses contractuelles types bénéficient d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union européenne. Elle précise qu'à cet effet l'évaluation du niveau de protection assuré dans le contexte d'un tel transfert doit, notamment, prendre en considération tant les stipulations contractuelles convenues entre le responsable du traitement ou son sous-traitant établi dans l'Union européenne et le destinataire du transfert établi dans le pays tiers concerné que, en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données à caractère personnel ainsi transférées, les éléments pertinents du système juridique de celui-ci.

Le Comité européen de la protection des données (CEPD) a publié une première analyse de cette décision de la CJUE (via des FAQ) le 23 juillet 2020, analyse reprise le 31 juillet 2020 dans un communiqué de la Cnil.

Selon cette analyse, il résulte de cette décision que :

- **l'arrêt de la CJUE a un effet immédiat**, cette dernière ayant invalidé la décision d'adéquation du Privacy Shield sans en maintenir les effets ;

- dorénavant, **tout transfert de données à caractère personnel effectué à l'attention d'un organisme aux Etats-Unis et fondé sur le fait que cet organisme a adhéré au Privacy Shield est considéré comme n'étant pas encadré par des garanties appropriées et doit donc être considéré comme illégal** ;

- **tout organisme qui communique des données à un organisme aux Etats-Unis sur la base des clauses contractuelles types émises par la Commission européenne (ou « CCT ») doit tout de même s'assurer**, au moyen d'une évaluation approfondie des circonstances du transfert et des mesures supplémentaires déployées, **(i) que les données bénéficient aux Etats-Unis d'un niveau de protection essentiellement équivalent à celui garantit par le droit de l'Union européenne et (ii) que la législation américaine ne compromet pas sur le niveau de protection adéquat que les clauses contractuelles types et ces mesures garantissent**. S'il est conclu au fait que, compte tenu des circonstances du transfert, **le respect des garanties appropriées n'est pas assuré, alors l'organisme concerné doit suspendre ou mettre fin au transfert de données à caractère personnel** ;

- l'utilisation de CCT pour transférer des données à caractère personnel vers d'autres Etats hors Union européenne est bien entendu toujours possible mais le même raisonnement que précité, s'agissant de la nécessité d'évaluer si le niveau de protection requis par le droit de l'Union européenne est respecté dans le pays tiers concerné afin de déterminer si les garanties fournies par les CCT peuvent être respectées dans la pratique, et les conséquences associées, doivent être suivis ;

- la Cnil peut toujours suspendre ou interdire un transfert de données à caractère personnel hors Union européenne si elle estime que ce transfert n'offre pas un niveau adéquat de protection des données à caractère personnel.

Le CEPD indiquait alors qu'il était en cours d'analyse de l'arrêt de la CJUE afin de déterminer le type de mesures complémentaires qui pourraient être fournies en plus des CCT, qu'il s'agisse de mesures juridiques, techniques ou organisationnelles, pour transférer des données vers des pays tiers où les CCT ne fourniront pas à eux seuls le niveau de garanties suffisant.

En conclusion, il résulte de l'arrêt de la CJUE précité, et de son interprétation relayée par le CEPD et par la Cnil, que **l'encadrement de flux transfrontières de données à caractère personnel vers un Etat situé hors Union européenne (tels que les Etats-Unis) au moyen des clauses contractuelles types élaborées par la Commission européenne peut donc ne pas suffire pour que de tels flux soient considérés comme mis en œuvre de manière licite,** notamment dans le cas où la règlementation du pays destinataire des données ne permet pas au cocontractant hors Union européenne de respecter les obligations contenues dans lesdites clauses contractuelles types, ce qui semble être le cas des Etats-Unis.

Dans une telle hypothèse, **le déploiement de mesures complémentaires pour encadrer de tels flux transfrontières apparaît nécessaire** afin que ces transferts de données à caractère personnel soient conformes à la règlementation applicable en matière de protection des données à caractère personnel.

* *
*

III. Précisions sur l'analyse à mener et sur les mesures complémentaires à déployer

Compte tenu de ce qui précède, le CEPD a élaboré des documents ayant vocation à aider et à guider les responsables de traitements et les sous-traitants en vue de l'analyse par leurs soins des flux transfrontières de données à caractère personnel qu'ils mettent en œuvre et de la détermination des mesures complémentaires devant éventuellement être déployées.

Aussi, aux termes de sa recommandation 02/2020 telle que définitivement adoptée le 10 novembre dernier, le CEPD vient tout d'abord insister sur la nécessité, en cas de flux transfrontière, **d'évaluer le niveau de protection des données à caractère personnel existant dans le pays destinataire desdites données**, notamment en examinant si des mesures de surveillances existantes localement et permettant l'accès aux données à caractère personnel par les autorités publiques, les agences de sécurité nationale ou les autorités chargées de l'application de la loi peuvent être considérées comme une ingérence justifiable ou pas, afin de déterminer si une telle ingérence va au-delà ou non de ce qui est nécessaire et proportionné dans une société démocratique.

Pour ce faire, **le CEPD précise qu'il convient de vérifier si :**
- le traitement de données à caractère personnel est basé sur des règles claires, précises et accessibles ;
- peuvent être démontrées la nécessité et la proportionnalité de cette ingérence au regard des objectifs légitimes poursuivis ;
- il existe un mécanisme de contrôle indépendant ;
- des recours efficaces sont mis à la disposition des personnes concernées.

Une telle analyse a pour objectif de déterminer si l'ingérence dans les droits et libertés des personnes concernées, et donc **si la législation applicable dans le pays destinataire des données répond ou non aux exigences des garanties essentielles européennes**.

Si tel n'est pas le cas, alors il convient de considérer que **le pays destinataire des données n'assure pas une protection des données essentiellement équivalente** à celle garantie par l'Union européenne et donc, dans une telle hypothèse, **de suspendre ou mettre fin par principe aux transferts de données à caractère personnel concernés**.

En outre, dans un projet de recommandation 01/2020 soumis à consultation publique, le CEPD présente aux exportateurs de données à caractère personnel **une série d'étapes à suivre et quelques exemples des mesures complémentaires qui pourraient être mises en place** pour assurer la licéité des flux transfrontières de données.

A cet égard, le CEPD recommande de procéder aux actions suivantes, qu'il convient de documenter :

- recenser les transferts de données à caractère personnel effectivement mis en œuvre ou dont la mise en œuvre est envisagée (en tenant compte des transferts dits « ultérieurs ») et s'assurer, pour chacun des transferts ainsi identifiés, que les données transférées sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont transférées et traités dans le pays situé hors Union européenne ;

- identifier les garanties sur lesquelles repose chaque transfert de données à caractère personnel (décision d'adéquation, règles d'entreprise contraignantes ou « Binding corporate rules », clauses contractuelles types,…) ou si des dérogations en raison de la situation particulière autorisant la mise en œuvre de transferts occasionnels et non répétitifs sont applicables ;

- procéder à une analyse spécifique pour évaluer si la règlementation en vigueur et/ou les pratiques effectives au sein de l'Etat destinataire des données pourraient affecter l'efficacité des garanties encadrant chaque transfert (par exemple si cette règlementation et/ou ces pratiques pourraient avoir pour conséquences d'empêcher l'application effective des clauses contractuelles types ayant vocation à encadrer le transfert), en vérifiant notamment si des dispositions pourraient faire obstacle à l'exercice effectif des droits des personnes concernées ou à leur droit à un recours effectif en cas d'accès par des autorités publiques à leurs données à caractère personnel ;

étant précisé en conclusion que :

- si le pays destinataire des données assure une protection des données essentiellement équivalente à celle garantie par l'Union européenne et ne remet pas en cause la possibilité de respecter les stipulations des garanties encadrant le transfert (par exemple les stipulations des clauses contractuelles types), alors la mise en œuvre de telles garanties est suffisante ;

- si le pays destinataire des données n'assure pas une protection des données essentiellement équivalente à celle garantie par l'Union européenne et/ou si l'importateur de données à caractère personnel ne peut pas se conformer à ses obligations issues des garanties encadrant le transfert (par exemple à ses obligations figurant dans les clauses contractuelles types) en raison de la législation et / ou des pratiques du pays tiers, il convient d'**identifier et adopter les mesures complémentaires (contractuelles, techniques et/ou organisationnelles) nécessaires** pour assurer un niveau de protection équivalente, en collaborant avec l'importateur des données à caractère personnel, étant précisé que le CEPD considère que les seules mesures organisationnelles et/ou contractuelles ne pourront généralement pas empêcher efficacement l'accès aux données par les autorités publiques locales mais qu'elles pourraient opportunément compléter des mesures techniques mises en œuvre (par exemple, le chiffrement des données sous réserve que la clé de déchiffrement soit détenue uniquement par l'exportateur des données, ou encore la pseudonymisation des données à condition que seul l'exportateur des données détienne les informations supplémentaires nécessaires pour identifier les personnes concernées – pour en savoir plus et pour d'autres exemples pratiques de mesures complémentaires pouvant opportunément être déployées, voir le projet de recommandation du CEPD);

- s'il n'est pas possible de mettre en œuvre des mesures appropriées efficaces garantissant la licéité et la conformité aux dispositions et recommandations applicables de tels transferts hors Union européenne de données à caractère personnel, alors il conviendra de suspendre ou mettre fin à ces transferts.

Le CEPD insiste également sur la nécessité de réévaluer à intervalles réguliers, le cas échéant en collaboration avec les importateurs de données, le niveau de protection des données encadrant les transferts mis en œuvre.

Il résulte de ce qui précède que **la mise en œuvre de tout flux transfrontière de données, effective ou envisagée, et ayant vocation à être encadrée par la conclusion de clauses contractuelles types ou par**

d'autres garanties contractuelles, doit nécessairement faire l'objet d'une analyse spécifique préalable en vue (i) de vérifier si le pays destinataire des données assure ou non un niveau de protection essentiellement équivalent à celui garanti au sein de l'Union européenne et, si tel n'est pas le cas, (ii) de déterminer et de déployer les **mesures complémentaires nécessaires** pour que de tels flux puissent être encadrés conformément à la règlementation applicable en matière de protection des données à caractère personnel et aux recommandations des autorités en la matière.

A titre d'exemple, s'agissant des mesures complémentaires pouvant être déployées pour assurer la protection des données à caractère personnel, le CEPD précise que :

- à titre d'exemple, si :
(i) les données à caractère personnel sont traitées à l'aide d'un chiffrement fort avant leur transmission vers un pays tiers ;
(ii) l'algorithme de chiffrement et son paramétrage (par exemple, longueur de clé, mode de fonctionnement,…) sont conformes à l'état de l'art et peuvent être considérés comme robustes contre la cryptanalyse pouvant être effectuée par les autorités publiques du pays bénéficiaire en tenant compte des ressources et capacités (par exemple, puissance de calcul pour les attaques par force brute) dont elles disposent ;
(iii) la force du chiffrement tient compte de la période de temps spécifique pendant laquelle la confidentialité des données à caractère personnel chiffrées doit être préservée ;
(iv) l'algorithme de chiffrement est parfaitement implémenté par un logiciel correctement mis à jour dont la conformité à la spécification de l'algorithme choisi a été vérifiée, par exemple par certification ;
(v) les clés sont gérées de manière fiable (générées, administrées, stockées, le cas échéant, liées à l'identité d'un destinataire prévu, et révoquées) ;
(vi) les clés sont conservées uniquement sous le contrôle de l'exportateur de données ou d'autres entités chargées de cette tâche qui résident dans l'Union européenne ou dans un pays tiers pour lequel la Commission européenne a établi qu'un niveau de protection adéquat est assuré ;
alors le CEPD considère que le chiffrement effectué fournit une mesure complémentaire efficace pour permettre le transfert des données ;

- pour une autre illustration, si :
(i) un exportateur de données transfère les données à caractère personnel traitées de telle manière que ces données ne peuvent plus être attribuées à une personne concernée spécifique, ni être utilisées pour isoler la personne concernée dans un groupe, sans utilisation d'informations supplémentaires (cf. pseudonymisation) ;
(ii) les informations supplémentaires sont détenues exclusivement par l'exportateur de données et conservées séparément dans l'Union européenne ou dans un pays tiers pour lequel la Commission européenne a établi qu'un niveau de protection adéquat est assuré ;
(iii) la divulgation ou l'utilisation non autorisée de ces informations supplémentaires est empêchée par des moyens techniques appropriés et des garanties organisationnelles, et il est garanti que l'exportateur de données conserve le contrôle exclusif de l'algorithme ou du référentiel permettant la ré-identification à l'aide des informations supplémentaires ;
(iv) le responsable du traitement a établi au moyen d'une analyse approfondie, en tenant compte de toutes les informations que les autorités publiques du pays bénéficiaire peuvent posséder, que les données à caractère personnel pseudonymisées ne peuvent pas être attribuées à une personne physique identifiée ou identifiable même en cas de recoupement avec de telles informations ;
alors le CEPD considère que la pseudonymisation effectuée fournit une mesure complémentaire efficace pour permettre le transfert des données.

A l'inverse, le fait que l'importateur de données puisse accéder aux données à caractère personnel traitées et ré-identifier les personnes concernées ne permet pas de considérer, si le pouvoir accordé aux autorités publiques du pays destinataire d'accéder aux données transférées va au-delà de ce qui est nécessaire et proportionné dans une société démocratique, et ce quelles que soient les mesures techniques, contractuelles ou organisationnelles déployées (ex : chiffrement des données pendant le transport ou au repos s'il est tout de même possible à l'importateur d'accéder, même ponctuellement, aux données au moyen de la clé de déchiffrement), que des mesures complémentaires efficaces sont déployées, ce dont il résulte que les flux transfrontières de données à caractère personnel vers ce pays destinataire ne peuvent pas être mis en œuvre conformément à la règlementation européenne applicable.

Attention, en tout état de cause, même dans l'hypothèse où des mesures techniques efficaces sont déployées, alors des mesures contractuelles et/ou organisationnelles complémentaires doivent être mises en œuvre conformément aux recommandations du CEPD.

En l'espèce, s'agissant de l'utilisation des services de Google, il apparaît que :

- des flux transfrontières de données à caractère personnel vers les Etats-Unis sont nécessairement mis en œuvre ;
- seules les CCT pourraient éventuellement permettre d'encadrer valablement les flux de données à caractère personnel vers les Etats-Unis ;
- toutefois, **il apparaît que de telles CCT ne sont pas suffisantes, compte tenu de la législation locale aux Etats-Unis, pour encadrer de tels flux conformément aux dispositions applicables, et notamment au RGPD**. En effet, tant l'invalidation de la décision d'adéquation du « privacy shield » que la position de la CJUE selon laquelle les CCT ne sont pas suffisantes pour encadrer valablement les flux transfrontières de données vers ce pays, résultent de la possibilité, au regard de la législation locale, que des autorités publiques américaine accèdent aux données traitées sans que ne soient prévues des garanties appropriées, suffisantes et effectives notamment pour les personnes concernées (cf. le pouvoir accordé aux autorités publiques des Etats-Unis d'accéder aux données transférées va au-delà de ce qui est nécessaire et proportionné dans une société démocratique selon les critères posés par le CEPD) ;
- des **garanties complémentaires doivent être déployées aux fins de rendre licites les flux transfrontières de données à caractère personnel vers les Etats-Unis**.

Or, compte tenu de ce qui précède, il semble à date que seuls des transferts de données qui ne permettraient pas à l'importateur (aux importateurs) de données aux Etats-Unis d'avoir connaissance des données pourraient être mis en œuvre dans des conditions conformes aux dispositions européennes et françaises applicables.

* *
*

IV. Conclusion et plan d'actions

Il résulte de ce qui précède qu'il convient de :

- **vérifier, au regard des mesures proposées par le CEPD notamment, dans sa recommandation 01/2020, si des mesures complémentaires considérées comme efficaces par ce dernier sont déployées** dans le cadre du recours aux services proposés par Google ;

- **à défaut, ne pas déployer ou mettre fin auxdits flux transfrontières de données vers les Etats-Unis** mis en œuvre du fait du recours aux services proposés par Google (et donc ne pas recourir auxdits services…).

NB1 : la présente consultation ne porte que sur l'analyse de la conformité du recours aux outils et services de Google au regard de l'existence de flux transfrontières de données à caractère personnel qui peuvent exister vers les Etats-Unis du fait du recours à de tels outils et services, sans audit des caractéristiques de ces outils et services, de la qualification des parties, des modalités de réutilisation éventuelles des données par Google ou encore des conditions contractuelles applicables, et sans analyse de la conformité de ces outils et services aux autres principes directeurs et obligations résultant de la règlementation européenne et française en matière de traitements de données à caractère personnel. Par conséquent, et si les mesures complémentaires déployées pour encadrer les flux transfrontières de données à caractère personnel visés ci-dessus permettaient, après vérification, de procéder de manière licite à des tels flux, alors une analyse complémentaire des outils et services proposés par Google devrait en tout état de cause être menée, pour chacun d'entre eux, aux fins d'audit et de vérification de leur conformité aux dispositions européennes et françaises applicables (ex : respect du principe de loyauté, de transparence et de minimisation des données, existence de documents contractuels conclus avec Google conformes aux dispositions notamment du RGPD, vérification de la conformité des autres flux transfrontières éventuellement mis en œuvre vers d'autres Etats non membres de l'Union européenne,…).

NB2 : par ailleurs, l'analyse à déployer pour s'assurer de la conformité des flux transfrontières de données vers les Etats-Unis qui seraient encadrés par les CCT doit être également suivie pour tout autre flux transfrontière qui serait mis en œuvre vers tout autre Etat non membre de l'Union européenne. ***En tout état de cause, les questions à se poser et l'analyse à mener aux fins de répondre aux exigences du RGPD notamment en termes de flux transfrontières de données se posent de la même manière pour tous les outils et toutes les solutions dont les acteurs et/ou les caractéristiques et/ou le fonctionnement impliquent un transfert de données à caractère personnel vers un pays hors Union européenne, et notamment vers les Etats-Unis.***