www.fevad.com
fédération e-commerce
et vente à distance

11.01.2019

Observations de la FEVAD sur le projet de référentiel CNIL relatif aux traitements de données à caractère personnel mis en œuvre aux fins de gestion des activités commerciales

Le 28 novembre dernier, la CNIL a lancé une consultation sur son nouveau projet de référentiel sur la gestion commerciale dans le but de recueillir l'avis des personnes intéressées avant le 11 janvier.

Ce référentiel, présenté comme un instrument de régulation ayant vocation à donner davantage de sécurité juridique aux entreprises, concerne la mise en œuvre de tout fichier « clients » et « prospects ». Il vise donc l'ensemble des entreprises ayant une activité commerciale, quel que soit le ou les secteurs (en dehors des secteurs de la banque, de l'assurance et des jeux en ligne) et quel que soit le ou les canaux de communication concernés.

En tant qu'organisation représentative des acteurs du commerce électronique, la FEVAD salue la démarche de concertation mise en place par la CNIL. Elle regrette cependant le peu de temps laissé aux parties prenantes pour contribuer à sa consultation, au regard de la portée et des conséquences considérables de ce référentiel pour des millions d'entreprises.

Après avoir consulté ses adhérents, et sur la base des retours reçus dans le temps imparti, la FEVAD est en mesure de formuler une première série d'observations, sous réserve des remarques qui pourraient résulter d'un examen plus approfondi du texte.

La FEVAD souhaite tout particulièrement attirer l'attention sur les points 4 et 6 du projet de référentiel et se tient à la disposition de la CNIL et des autres parties prenantes pour tout échange complémentaire sur la présente contribution.

1. À QUI S'ADRESSE CE RÉFÉRENTIEL ?

Sur le fond, le document reprend un certain nombre de règles qui figuraient précédemment dans la norme simplifiée NS 48 et que le référentiel entend compléter en s'appuyant sur l'interprétation des dispositions issues du RGPD.

D'une manière générale, la FEVAD reconnaît l'intérêt et l'utilité d'un tel référentiel afin d'accompagner les entreprises dans la mise en œuvre des mesures issues du Règlement Général sur la Protection des Données (RGPD). Compte tenu du caractère général de la norme européenne, il est important pour les entreprises, notamment pour celles qui ne

disposent pas d'expertise juridique interne, d'avoir accès à des outils leur permettant de mieux maîtriser la portée de leurs obligations légales, et donc de mieux s'y conformer.

À cet égard, il convient de saluer l'objectif pédagogique recherché par le référentiel, notamment à travers les différents exemples présents sous forme de tableaux, en annexe.

La lecture du référentiel témoigne cependant de la difficulté d'appréhender, dans un document de quelques pages, des règles parfois complexes qui s'appliquent à des activités aussi nombreuses que variées.

Le référentiel n'en constitue pas moins un outil utile. La FEVAD s'interroge cependant sur l'existence d'une coordination en Europe, entre les Autorités de contrôle compétentes ; dans l'élaboration de ce type de référentiel.

2. PORTÉE DU RÉFÉRENTIEL

> ***« …L'application de ce référentiel permet d'assurer la conformité des traitements de gestion commerciale au regard des principes relatifs à la protection des données. Il constitue également une aide à la réalisation d'une analyse d'impact relative à la protection des données (AIPD) dans les cas où celle-ci est nécessaire… »***

Au-delà de sa valeur pédagogique et d'accompagnement du document, **il conviendrait d'indiquer plus clairement sa valeur juridique, notamment en précisant l'absence de valeur contraignante.**

3. OBJECTIF(S) POURSUIVI(S) PAR LE TRAITEMENT (FINALITÉS)

> ***« Un traitement de gestion des activités commerciales peut être mis en œuvre pour les finalités suivantes : … »***

Le projet de référentiel ne reprend qu'une partie les finalités envisagées dans la norme simplifiée NS 48. On peut s'interroger sur les raisons qui ont conduit à passer sous silence certaines des finalités anciennement visées dans la norme NS 48, telles que la cession, la location ou l'échange de fichiers, lesquelles sont toujours susceptibles de constituer des finalités légitimes en rapport avec la gestion d'activités commerciales. **Il paraît donc souhaitable de compléter la liste des finalités visées.**

4. BASE(S) LÉGALE(S) DU TRAITEMENT

> ***« …. L'accord doit être libre et non influencé ou contraint (il ne peut conditionner la souscription à un service ou l'achat d'un bien, la création d'un compte en ligne pour accéder à un service, etc.). »***

Cette formulation va au-delà de que ce qui est prévu par le RGPD en matière de conditionnalité du consentement. D'une part, en ce qu'elle ajoute la notion « d'influence » et, d'autre part, en ce qu'elle exclut toute possibilité de relation entre l'accord et l'accès à un service. En effet, l'article 7.4 du RGPD prévoit bien qu'« au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service,

est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.» Pour autant il n'exclut pas de manière aussi ferme toute possibilité de lier valablement le consentement à la fourniture d'un bien ou service. De même, en ce qui concerne le considérant 43 du RGPD, lequel fait référence à une présomption de nullité, sans que cette présomption soit qualifiée d'irréfragable[1].

Par ailleurs, plusieurs textes européens, actuellement en discussion à Bruxelles, vont, au contraire, dans le sens d'une reconnaissance explicite de la possibilité de consentir, sous certaines conditions, à l'usage de ses propres données, en contrepartie de la fourniture d'un service.

C'est le cas notamment de la dernière version du projet de Règlement européen sur la vie privée dans le secteur des communications électroniques, actuellement en cours d'examen par le Conseil (Règlement « e-Privacy »)[2]. Il en va de même dans le projet de Directive « New Deal for Consumers » publié le 11 avril dernier et dans lequel il est directement fait référence à la valeur économique des données personnelles et à la possibilité de payer un service avec de l'argent ou en fournissant des données personnelles [3]

Il conviendrait donc de reformuler le passage en question.

> ***« Un tableau, ci-après, illustre par des exemples pratiques les cas dans lesquels les bases légales peuvent être retenues en fonction de l'objectif poursuivi par le traitement. »***

Concernant la cession de données électroniques, et contrairement à ce que semble indiquer le tableau, le consentement de la personne pour la transmission de ses coordonnées électroniques n'est pas prévu par la réglementation ; il n'y a donc pas lieu d'exiger le consentement sauf dans les cas où la transmission serait l'activité principale du responsable de traitement.

Concernant les données bancaires, la finalité pour laquelle le consentement est requis, n'apparaît pas (dans la colonne de droite).

5. DONNEES PERSONNELLES CONCERNEES

[1] « *Le consentement est **présumé** ne pas avoir été donné librement (..) ou si l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution.* »

[2] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). Cf. rapport de la Présidence du Conseil du 23 novembre 2018 (14491/18).

[3] Directive modifiant la directive 2011/83/UE : « *La proposition étend l'application de la directive 2011/83/UE aux services numériques pour lesquels les consommateurs ne versent pas d'argent mais fournissent des données à caractère personnel, telles que : stockage dans le nuage, réseaux sociaux et comptes de messagerie électronique. Compte tenu de la valeur économique croissante des données à caractère personnel, ces services ne peuvent pas être considérés comme simplement «gratuits».» Les consommateurs devraient donc avoir le même droit aux informations précontractuelles et d'annulation de contrat dans un délai de rétractation de quatorze jours, **indépendamment du fait qu'ils paient pour le service avec de l'argent ou en fournissant des données personnelles***. »

« Un tableau, ci-après, énumère les données pouvant être collectées et traitées selon les finalités du traitement. »

Il conviendrait de préciser que ce tableau est donné à titre indicatif, étant entendu que le caractère « nécessaire » des données au regard de la finalité envisagée, dépend de la nature de l'opération dans le cadre de laquelle elles sont collectées.

6. DESTINATAIRES DES INFORMATIONS

« La transmission des DP à des partenaires commerciaux nécessite en amont :

- d'informer les personnes concernées sur le support de collecte des données (formulaire en ligne ou papier) de la finalité de cette transmission et des catégories de destinataires concernés. La liste précise des destinataires doit être régulièrement actualisée et mise à disposition des personnes à partir de ce même support (par ex en y faisant figurer un lien hyper texte) »

Si l'information sur la finalité de la transmission est incontestable, au titre des règles de transparence et d'information prévues par le RGPD, il n'en pas de même en ce qui concerne la communication de la liste à jour des destinataires des données.

Une telle obligation ne figure pas aujourd'hui dans le RGPD.

En effet, l'article 13 qui dresse la de l'ensemble des informations devant être communiquées sur le support de collecte des données prévoit que le responsable du traitement devra informer « des destinataires ou catégories de destinataires ».

Cette option laissée à l'entreprise de choisir entre l'information sur les destinataires ou les catégories de destinataires n'est pas nouvelle. Elle figurait déjà, dans les mêmes termes, en droit français ainsi que dans la directive européenne sur la protection des données, avant le RGPD.

La question du maintien de cette alternative a, par ailleurs, été clairement posée lors des débats au Parlement européen. En effet, plusieurs députés européens avaient alors proposé de supprimer la notion de « catégories de destinataires », pour imposer une information sur le « destinataire », comme l'indique le nouveau projet référentiel.

Or, cet amendement en question a clairement été rejeté, ce qui témoigne de la volonté du Législateur européen de maintenir le droit en l'état.

Vouloir imposer aux entreprises de communiquer et de tenir à jour la liste des destinataires irait donc bien au-delà de ce qui est prévu et voulu par le RGPD.

Outre la question de sa compatibilité avec le droit européen, cette obligation soulève d'innombrables difficultés pratiques pour les entreprises (par exemple, en cas de collecte sur un coupon-réponse, lors d'un achat en magasin ou encore au téléphone), sans parler du coût de mise en œuvre que cela représenterait pour les TPE/PME/.

D'autant que se pose également la question de l'utilité d'une telle information généralisée des destinataires en temps réel, lorsque l'on sait que cette information (au-delà de la catégorie de destinataires) peut être obtenu dans le cadre de l'exercice du droit d'accès à ses données.

Enfin, les entreprises consultées font aussi état d'un risque de divulgation d'informations relatives au secret des affaires. En effet, cette obligation imposerait aux entreprises françaises la diffusion publique d'informations relatives à la vie des affaires (par exemple,

dans le cas d'un partenariat stratégique), là où leurs concurrents étrangers en seraient dispensés.

Compte tenu de ce qui précède, il convient donc de supprimer l'obligation d'information sur la liste des destinataires et de réintroduire la notion de « destinataires ou catégories de destinataires » afin d'assurer la conformité du référentiel avec l'article 13.

7. DURÉES DE CONSERVATION

Le projet de référentiel prévoit différentes durées de conservation en fonction de la finalité, ce qui soulève de nombreuses questions relatives à l'articulation entre les différentes durées de conservation pour les mêmes données. **Ces questions mériteraient d'être clarifiées.**

8. INFORMATION DES PERSONNES

9. DROITS DES PERSONNES

10. SÉCURITÉ

> ***« L'organisme doit prendre toutes les précautions utiles au regard des risques présentés par son traitement pour préserver la sécurité des données à caractère personnel (…). En particulier, dans le contexte spécifique du présent référentiel, soit l'organisme adopte les mesures suivantes, soit il justifie de leur équivalence ou du fait de ne pas avoir besoin ou pouvoir y recourir … »***

L'ensemble des mesures préconisées semblent devoir être appliquées par défaut, à charge pour l'organisme de justifier l'équivalence des mesures qu'il a adoptées « ou du fait de ne pas en avoir besoin ou pouvoir y recourir ».

La liste des mesures de sécurité énoncée est particulièrement lourde et détaillée. Mais surtout, elle ne prend pas en compte la taille du traitement, ni la nature des données traitées. **Il conviendrait donc d'apporter un certain nombre de précisions visant à mieux définir les types de traitements pour lesquelles chacune des mesures concernées sont « nécessaires », de manière à accompagner les entreprises et notamment les TPE/PME dans la mise en place de mesures fondées sur une approche sur les risques**.

À propos de la FEVAD :

La Fédération du e-commerce et de la vente à distance fédère aujourd'hui 600 entreprises et plus de 800 sites internet. Elle est l'organisation représentative du secteur du commerce électronique et de la vente à distance. La FEVAD a notamment pour mission de recueillir et diffuser l'information permettant l'amélioration de la connaissance du secteur et d'agir en faveur du développement durable et éthique de la vente à distance et du commerce électronique en France.

http://www.fevad.com

Contact :

Marc LOLIVIER
Délégué général
mlolivier@fevad.com