Qu’est ce que le principe d’« Accountability » dans le Règlement Européen de Protection des Données Personnelles ?

	Qu’est ce que le principe d’« Accountability » dans le Règlement Européen de Protection des Données Personnelles ?

Le principe d'«Accountability » n'est pas nouveau dans le domaine de la protection des données et de la vie privée. Plusieurs textes y ont déjà fait référence et notamment les lignes directrices émises par l'OCDE en 1980, le Standard de la conférence Internationale de Madrid, la norme ISO 29100 ou les règles mises en place au sein de l'APEC. Au sein même de la directive 95/46, le possible recours aux règles internes de groupe pour encadrer les transferts de données en dehors de l'Union Européenne, reflètent cette notion qui vise à responsabiliser le responsable de traitement.

Comment définir le principe d'«Accountability » ?

Ce terme est difficile à traduire en français. Cela revient à montrer comment le principe de responsabilité est mis en œuvre et à le rendre vérifiable. Il est souvent traduit en français par l'« obligation de rendre compte ».
Pour le G29[1] , cela doit s'entendre comme des « mesures qui devraient être prises ou fournies pour assurer la conformité en matière de protection des données ».

Le principe d'«Accountability » dans le Règlement Général de Protection des Données

La traduction française du texte, à savoir « le principe de responsabilité », ne reflète pas toute la signification de ce terme. C'est en lisant le détail des dispositions du règlement, que l'on en saisit la portée.
– Le responsable du traitement est responsable du respect des principes (i.e.de la licéité, de la loyauté, de la transparence des traitements, du respect du principe de finalités, de minimisation des données, de l'exactitude des données, du respect de la durée de conservation et des mesures de sécurité) ;
– Et il est en mesure de démontrer que ces dispositions sont respectées. A cet effet, l'article 22 du Règlement précise que le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées. Lorsque cela est proportionné aux activités de traitement de données, les mesures comprennent la mise en œuvre de politiques appropriées.
– Comme dans tout processus d'amélioration continue, ces mesures doivent être réexaminées et actualisées si nécessaire.

Qui est soumis au principe d'« Accountability » ?

Selon les dispositions de l'article 5 du règlement européen, ce principe concerne le responsable de traitement.
Les sous-traitants auront eux aussi des responsabilités portant sur la mise en œuvre de mesures ou sur la documentation des traitements ; mais si le vocabulaire utilisé dans le texte du règlement est souvent similaire, il ne semble pas que l'on puisse en déduire que les sous-traitants seront soumis au respect du principe d'« Accountability ».
Il en va probablement différemment du représentant qui agit pour le compte et au nom du responsable de traitement établi en dehors de l'Union Européenne et qui de ce fait, doit remplir les obligations qui lui incombent.

De quelles mesures technique et organisationnelles s'agit-il ?

Ces mesures doivent être prise en tenant compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés des personnes.
Le G29 précise que la mise en pratique du principe d' « Accountability » suppose une analyse au « cas par cas ».
L'article 23 du Règlement relatif à la protection des données dès la conception et par défaut, précise que le responsable de traitement met en œuvre des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, destinées à donner effet aux principes de protection des données et notamment à la minimisation.
Il est par ailleurs indiqué à l'article 28 du Règlement, que chaque responsable du traitement tient un registre décrivant les traitements et dans la mesure du possible, les mesures de sécurité techniques et organisationnelles mise en place.
Selon l'article 30 du Règlement européen, le responsable de traitement est tenu de prendre des mesures de sécurité et notamment selon les besoins :
– la pseudonymisation et le cryptage des données à caractère personnel ;
– des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement des données ;
– des moyens permettant de rétablir la disponibilité des données et l'accès à celles-ci (…) en cas d'incident ;
– une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures de sécurité.

Les mesures indiquées dans le Règlement Européen font écho à celles citées en exemple par le G29 à l'occasion de son avis[2] émis sur l'« Accountability »:
– Des politiques et procédures internes permettant de garantir le respect des principes de protection des données (notamment lors de la création ou la modification d'un traitement),
– L'inventaire des traitements,
– La répartition des rôles et responsabilités,
– La sensibilisation et formation du personnel,
– La désignation d'un délégué à la protection des données,
– La vérification de l'efficacité des mesures (contrôles, audits).

Lors de la 31ème Conférence des Commissaires à la Protection des Données et à la Vie Privée de Madrid, le principe d'«Accountability » avait été illustré de la manière suivante:
– Implémentation de procédures destinées à prévenir et détecter les failles,
– La désignation d'un ou de plusieurs délégués à la protection des données,
– Des sessions de sensibilisation et de formation régulières,
– La conduite régulière d'audits indépendants,
– La prise en compte de la réglementation au travers de spécificités techniques,
– La mise en place d'études d'impacts sur la vie privée,
– L'adoption de codes de conduite.
Le G29 a également indiqué que la transparence sur les politiques de confidentialité et sur la gestion interne des plaintes contribuait à un meilleur niveau d'« Accountability ».

Le rôle de la certification

Le Règlement européen précise que l'application d'un code de conduite approuvé ou d'un mécanisme de certification approuvé peut servir à attester du respect des obligations incombant au responsable du traitement au titre de l' « Accountability ».
De manière générale, les actes délégués de la Commission devraient fournir de plus amples informations sur le sujet.

Le principe d'« Accountability » : une évolution plus qu'une révolution

L'« Accountability » n'est pas une révolution dans la mesure où les organisations ont déjà l'obligation de se conformer aux principes de protection des données et notamment à la loi Informatique et Libertés en France. Ce principe est d'ailleurs déjà connu des acteurs du secteur financier.
L'obligation de documentation à des fins de démonstration est en revanche plus novatrice et ce d'autant plus que les entreprises connaissent mal l'étendue de cette réglementation.
Ainsi en cas de violation des principes de protection des données, les autorités de protection des données devraient prendre en considération l'implémentation (ou pas) de mesures et l'existence de procédures de contrôle.
De plus, si les informations relatives aux procédures et politiques ne peuvent être fournies, les autorités de protection des données pourront sanctionner une organisation sur la base de ce seul manquement, indépendamment du fait qu'il y ait eu une violation des données.
Comme l'a indiqué le groupe de travail des autorités européennes de protection des données (G29), les personnes ayant des connaissances techniques et juridiques pointues en matière de protection des données, capables de communiquer, de former le personnel, de mettre en place des politiques et de les auditer seront indispensables à la protection des données.
[1] Opinion 3/2010 on the principle of accountability
[2] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf
… [Lire la suite]

Réagissez à cet article

Source : *Règlement Européen de Protection des Données Personnelles : Le principe d'« Accountability » ou comment passer de la théorie à la pratique – CIL Consulting*