

Données personnelles et offshoring : un encadrement strict



Ou le principe de l'interdiction de transférer des données à caractère personnel hors Union Européenne, sauf si l'Etat dans lequel se situe le prestataire assure un niveau de protection adéquat ou suffisant...

Par Anne-Sophie Poggi, Avocat Associée et Aude Gérard, Avocat (cabinet Derriennic Associés).

La directive 95/46/CE (1) et la loi Informatique et libertés posent le principe qu'un responsable de traitement peut transférer des données à caractère personnel vers un Etat n'appartenant pas à l'Union Européenne, que si cet Etat assure un niveau de protection adéquat ou suffisant de la vie privée et des libertés et droits fondamentaux des personnes.

C'est à la Commission Européenne et à elle seule qu'il appartient de reconnaître qu'un pays accorde une protection adéquate ou suffisante, dans une décision prise à cet effet, dénommée «décision d'adéquation».

Toutefois, il existe pour des entreprises établies aux Etats-Unis un dispositif dit «Safe Harbor», ayant fait l'objet d'une décision d'adéquation par la Commission Européenne (26 juillet 2000), qui repose sur une démarche volontaire d'entreprises établies aux Etats-Unis. Ces entreprises s'auto-certifient comme adhérent «à une série de principes de protection des données à caractère personnel et de protection de la vie privée, publiés par le ministère du commerce des Etats-Unis».

Les transferts émis à partir de l'Union Européenne vers un prestataire ayant adhéré au Safe Harbor ou situé dans un Etat ayant bénéficié d'une décision d'adéquation

prise par la Commission Européenne, ne donnent lieu à aucune formalité spécifique auprès de la Cnil.

Les responsables de traitement devront uniquement mentionner à la Cnil, lors des formalités préalables,

selon les cas :

- l'existence d'un transfert de données vers une société adhérente au Safe Harbor et communiquer les extraits pertinents de la «Safe Harbor List» permettant d'avoir accès aux détails de l'autocertification de la société adhérente ;

- l'existence d'un transfert de données vers un pays ayant bénéficié d'une décision d'adéquation.

Les exceptions à ce principe...

L'interdiction de principe est tempérée par une série d'exceptions, limitativement énumérées dans la directive 95/46/CE et la loi Informatique et libertés. Il en va ainsi en cas de consentement exprès de la personne dont les données sont transférées ou encore, lorsque ce transfert est indispensable dans certains cas expressément visés, par exemple à la sauvegarde de la vie de la personne concernée.

Il convient toutefois d'attirer l'attention sur le fait que ces exceptions sont d'interprétation stricte si bien qu'elles n'ont vocation à s'appliquer que dans des cas limités, visés expressément par les textes précités.

En cas de recours à un prestataire externe hors Union Européenne pour traiter des données, le principe est alors d'appliquer la procédure dite des clauses contractuelles. La loi Informatique et libertés, conformément à ce que prévoit la directive, permet en effet le transfert de données hors Union Européenne lorsque «le traitement garantit un niveau de protection suffisant de la vie privée, ainsi que des libertés et droits fondamentaux des personnes, notamment en raison des clauses contractuelles ou règles internes dont il fait l'objet».

La Commission Européenne a élaboré deux catégories de clauses contractuelles types que les responsables de traitement peuvent utiliser en cas de transfert de données hors Union Européenne :

- des clauses contractuelles types de «responsable de traitement à responsable de traitement» par deux décisions des 15 juin 2001 et 7 janvier 2005 ;
- des clauses contractuelles types de «responsable de traitement à sous-traitant» par décision du 27 décembre 2001.

En conséquence, un responsable de traitement, qui fait appel à un sous-traitant hors Union Européenne, pourra utiliser la seconde catégorie de clauses élaborées par la Commission Européenne.

Les clauses contractuelles sont soumises à autorisation de la Cnil. L'autorisation est délivrée sans aucune difficulté par la Cnil lorsque le responsable du traitement a recours aux clauses types. En revanche, si le responsable du traitement souhaite modifier ces clauses ou encore utiliser son propre contrat, la Cnil procédera à un examen attentif de son contenu par comparaison avec les clauses contractuelles types de la Commission Européenne.

(1): 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.

28/9/2009