Les Verts | Alliance Libre Européenne
au Parlement Européen

17 octobre 2013

Règlement général sur la protection des données en 10 points

Rapporteur pour le PE : Jan Philipp Albrecht

De la directive au règlement général

La situation actuelle : Les 28 États membres de l'Union européenne adoptent leurs propres lois fondées sur la directive de 1995. La mise en œuvre, différente dans chaque État membre a conduit à un niveau inégal de protection et à un patchwork de règles sur la protection des données dans l'UE.

Des mêmes standards pour tous!
Un règlement dans un cadre général consacré à la protection des données dans l'Union qui remplace la directive de 1995 mène à une harmonisation intégrale au niveau le plus élevé, garantissant la sécurité juridique et un niveau uniforme et élevé de protection des personnes en toutes circonstances. Ainsi, les entreprises sont empêchées de choisir leur siège dans l'État membre avec les plus bas niveaux de protection des données. («forum shopping»). Mais la proposition de réforme va encore plus loin: à l'avenir, des normes européennes de protection des données devront être appliquées une fois que les données des citoyens européens seront traitées - tant à l'intérieur qu'à l'extérieur de l'UE.

Principales revendications du rapporteur :

- **Les droits à l'effacement, à l'information et à la rectification :** Celui qui veut que ses propres données personnelles soient supprimées de l'environnement numérique, doit avoir un "droit de supprimer" contre Google, Facebook et autres. Celui qui a publié les données d'une personne de manière illégale doit également assurer que chaque copie de ces données soit effacée. Le rapporteur et les groupes politiques appellent à un juste équilibre entre la liberté d'expression et d'information et la protection des données personnelles. Les contextes dans lesquels les données personnels sont traitées doivent être indiqués sur demande par voie électronique en langage clair, gratuitement et rapidement.

- **Le consentement explicite:** Si un fournisseur de services souhaite traiter des données personnelles, il doit toujours demander aux utilisateurs s'ils sont d'accord avec le traitement et la diffusion de leurs données. Les conditions d'utilisation devraient être présentées de façon simple et compréhensible. Cela en remplacement de conditions générales très longues et incompréhensibles, des symboles standardisés peuvent simplifier l'accord ou le rejet. Les fournisseurs sont seulement autorisés à créer des profils d'utilisateurs si les utilisateurs indiquent à travers les paramètres de confidentialité de leur navigateur d'internet qu'ils sont d'accord. Des normes techniques applicables doivent être certifiées au niveau européen.

- **Information et transparence :** Avec plus d'exigences d'information, le rapporteur et les groupes politiques vont bien au-delà de la proposition de la Commission européenne. Les utilisateurs, doivent également recevoir des informations complètes sur la façon dont leurs données sont traitées ou si le fournisseur a transmis l'information à la police ou les services de renseignement.

- **Transferts de données à destination de pays tiers :** Après les révélations du whistleblower Edward Snowden, les groupes politiques avaient accepté que les entreprises comme Google puissent transférer des données personnelles uniquement s'il y a une base juridique en droit européen. Cela veut dire que sans accords concrets avec les pays concernés, il n'y a pas de transfert de données personnelles par les entreprises de télécommunications et internet. Cette référence a été incluse dans le premier projet de la Commission, puis supprimé du projet présenté publiquement après un lobbying intense de la part du gouvernement américain. Maintenant, la référence a été à nouveau incluse dans le texte.

- **Des définitions résistant aux changements futures :** Toutes les informations qui sont directement ou indirectement attribuées à une personne ou qui peuvent être utilisées pour filtrer une personne à partir d'un grand nombre de personnes sont considérées comme des données personnelles et doivent être protégés.

- **Sanctions en cas de violation :** Les infractions ne sont pas banales et les sanctions devraient être sévères. Le rapporteur et les groupes politiques souhaitent que les entreprises payent de fortes amendes si elles ne respectent pas la nouvelle loi. Dans le cas d'une grande entreprise, cela peut aller jusqu'à des milliards et va empêcher les entreprises de prendre simplement en compte les violations de données personnelles.

- **Privacy by Design/Privacy by Default :** Les entreprises doivent concevoir leurs services de telle manière que la protection des données et de la vie privée soit introduite par défaut et dès la conception. Un principe fort de limitation de la finalité signifie que seules les

données sont collectées, qui sont nécessaires pour fournir le service. Il doit également être possible d'utiliser les services anonymement et sous un pseudonyme.

- **Moins de bureaucratie:** La nomination d'un délégué de la protection des données doit non seulement se baser sur la taille des entreprises, mais également et principalement sur l'importance du traitement des données. Les notifications préalables aux autorités de contrôle devraient être limitées dans le but de réduire la bureaucratie. Un délégué de la protection des données sera mis en place dans toute l'Europe et est obligatoire à partir d'un certain seuil.

- **Exécution uniforme de la loi:** Une autorité de contrôle européenne de la protection des données doit imposer le droit de manière plus efficace et peut prendre des décisions qui étaient auparavant aux mains des autorités nationales de protection des données - ainsi que dans le droit européen de la concurrence et de la supervision bancaire de l'UE. Ainsi, une «course vers le bas» dans les États membres avec une faible application de la loi dans l'avenir n'est plus possible. La nouvelle autorité de protection des données de l'UE doit soutenir les autorités nationales. En générale les autorités de protection des données ont besoin de plus de personnel et plus de financement.

- **Un interlocuteur désigné à l'échelle européenne:** l'approche «one-stop-shop» signifie que les citoyens et les entreprises à travers l'UE peuvent s'adresser à l'autorité de protection des données dans leur État membre. Les entreprises doivent également coopérer seulement avec l'autorité de l'État membre de la protection des données dans laquelle le siège de la société se trouve. Pour les questions controversées l'autorité de contrôle de protection des données de l'UE nouvellement créé aura le dernier mot et non la Commission européenne. Ainsi l'indépendance des autorités de protection des données est maintenue.

Planning

21 Octobre 2013:
Vote à la commission des libertés civiles, de la justice et des affaires intérieures sur le mandat de négociation ("vote d'orientation").

Une fois que le Conseil a convenu d'une position commune:
Début des négociations tripartites entre le Parlement européen, le Conseil de l'Union européenne (Conseil des ministres) et la Commission européenne. Le Conseil européen siège du 24 au 25 octobre au sujet de «l'Agenda numérique».