RÉPONSE DU CCBE AU COMMUNIQUÉ DE LA COMMISSION SUR UNE APPROCHE GLOBALE DE LA PROTECTION DES DONNÉES DANS L'UNION EUROPÉENNE

Conseil des barreaux européens – Council of Bars and Law Societies of Europe
association internationale sans but lucratif
Avenue de la Joyeuse Entrée 1-5 – B 1040 Brussels – Belgium – Tel.+32 (0)2 234 65 10 – Fax.+32 (0)2 234 65 11/12 – E-mail ccbe@ccbe.eu – www.ccbe.eu

Réponse du CCBE au communiqué de la Commission sur une approche globale de la protection des données dans l'Union européenne

Le Conseil des barreaux européens (CCBE) est l'organe représentatif d'environ un million d'avocats européens, appartenant aux barreaux qui en font partie, dans 31 pays membres effectifs et 11 pays associés et observateurs. Le CCBE répond régulièrement au nom de ses membres aux consultations sur les politiques qui concernent les citoyens et les avocats européens.

Par la présente, le CCBE répond à la Commission européenne qui a souhaité obtenir des avis sur la manière de relever les nouveaux défis en matière de protection des données personnelles (par exemple le développement rapide des technologies ou la mondialisation) afin d'assurer une protection efficace et globale des données à caractère personnel au sein de l'UE, comme souligné dans le communiqué COM (2010) 609 final sur « Une approche globale de la protection des données à caractère personnel dans l'Union européenne ».

Le CCBE soutient et respecte profondément le droit fondamental à la protection des données personnelles, y compris le droit au respect de la vie privée et à la confidentialité des communications. Le cadre juridique actuel n'est cependant ni à jour ni cohérent, et ne prend pas en compte les nouveaux défis de la société de l'information. À cet égard, le CCBE accueille favorablement l'initiative de la Commission européenne visant à revoir le cadre juridique.

Dans ce document, le CCBE partage l'avis de la Commission sur la protection des données depuis la perspective de l'avocat européen. Le CCBE se réfère également à sa prise de position antérieure « Prise de position du CCBE sur le cadre juridique du droit fondamental à la protection des données personnelles » du 4 janvier 2010.

1. La profession d'avocat

La profession d'avocat comprend dans une large mesure le traitement des données, en particulier des données personnelles. Cela ne concerne pas seulement les données du client, mais aussi celle de la partie adverse et, éventuellement, des tiers concernés, par exemple les témoins, la partie requérante adverse dans un procès de promotion dans les procédures de statut de la fonction publique, les membres de la famille dans les affaires de divorce ou les employés touchés par un licenciement sur le principe de critères sociaux. Dans le cadre juridique, l'avocat est tenu de protéger les intérêts de son client de façon unilatérale, à la fois en raison du contrat conclu et de la déontologie de la profession d'avocat.

Les avocats sont soumis au secret professionnel depuis des décennies et des siècles pour la bonne raison que celui-ci protège le client lui-même et, en outre, assure une protection raisonnable des intérêts de toutes les personnes concernées. Par conséquent, le secret professionnel sert à la fois la protection du client en soi et l'ordre juridique de façon objective. De même, le secret professionnel de l'avocat concerne essentiellement les données des parties adverses et des tiers que l'avocat peut apprendre au cours de l'exercice de sa profession. L'avocat conserve ces données uniquement dans le cadre de son activité professionnelle et donc afin de servir les intérêts de son client.

Cette situation particulière distingue la profession d'avocat de presque toute autre personne soumis à des règles de protection des données. Ceci est notamment valable du fait que l'avocat protège des intérêts externes et conserve les données à caractère personnel de personnes différentes. La directive UE sur la protection des données ne règle pas de manière claire les situations de conflit qui surviennent et ne sert donc pas la protection juridique des intérêts qu'un avocat défend. Ceci doit être pris en compte lors de l'examen du cadre juridique.

2. Propositions permettant d'améliorer le cadre juridique de la protection des données

Compte tenu de la situation professionnelle spécifique de l'avocat, les règles suivantes sont nécessaires.

a) Le secret professionnel de l'avocat doit l'emporter sur toutes les règles de protection des données.

Le secret professionnel de l'avocat doit l'emporter sur toutes les règles de protection des données. Aucune règle de protection des données ne doit constituer une atteinte à ce secret professionnel, qui devrait être une priorité inconditionnelle de la pratique professionnelle de l'avocat. En outre, les règles de protection des données ne doivent pas obliger l'avocat à respecter les intérêts de tiers. À cet égard, le secret professionnel de l'avocat constitue une règle spécifique de protection des données. Cela implique une réglementation claire à condition que le traitement des données spécifiques au client de l'avocat soit soumis uniquement au secret professionnel de l'avocat (qui n'est généralement pas limité dans le temps) et à aucune autre règle de protection des données. Cependant, le traitement d'autres données pourrait également être soumis à des règles générales de protection des données.

b) Le contrôle de la conformité par une autorité indépendante spéciale

Le contrôle de la conformité aux règles de protection des données doit être réalisé exclusivement par une autorité indépendante spéciale qui soit familière aux particularités de la profession d'avocat. Seule une autorité indépendante spéciale est capable de prendre en considération les intérêts spécifiques des avocats au moment de prendre une décision. En Allemagne, ce contrôle est déjà effectué par les barreaux régionaux membres de la *Bundesrechtsanwaltskammer* (BRAK). La directive européenne sur la protection des données doit contenir des règles claires qui permettent à chaque Etat membre d'établir une autorité de contrôle spéciale conformément à sa législation nationale spécifique.

Assurer l'indépendance de l'autorité de contrôle au sujet des avocats est une condition préalable pour éviter les conflits d'intérêts résultant d'une implication de cette autorité dans la procédure, par exemple s'il s'agit de l'autorité qui lance la procédure administrative dans le secteur administratif, social ou celui du transport.

Quant à l'indépendance en ce qui concerne la directive sur la protection des données de l'UE, le CCBE tient à rappeler que la Cour européenne de justice stipule dans son arrêt du 9 mars 2010 concernant la Commission européenne contre République fédérale d'Allemagne que « l'indépendance des autorités de contrôle, en ce qu'elles doivent être soustraites à toute influence extérieure susceptible d'orienter leurs décisions, est un élément essentiel au regard des objectifs de la directive 95/46.Elle est nécessaire pour créer, dans tous les États membres, un niveau également élevé de protection des personnes physiques à l'égard du traitement des données à caractère personnel et contribue de cette façon à la libre circulation des données, qui est nécessaire à l'établissement et au fonctionnement du marché intérieur »[1]. Dans sa conclusion du même arrêt, la Cour a donc déclaré que « La République fédérale d'Allemagne a manqué aux obligations qui lui incombent en vertu de l'article 28, paragraphe 1, second alinéa, de la 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, en soumettant à la tutelle de l'État les autorités de contrôle compétentes pour la surveillance du traitement des données à caractère personnel par les organismes non publics et les entreprises de droit public prenant part à la concurrence sur le marché (öffentlich-rechtliche Wettbewerbsunternehmen) dans les différents Länder, transposant ainsi de façon erronée l'exigence selon laquelle ces autorités exercent leurs missions « en toute indépendance ».

Eu égard à ces considérations, le CCBE estime que les barreaux des États membres respectifs remplissent entièrement l'exigence d'indépendance complète des avocats exposée par la Cour.

[1] Affaire C-518/07 du 9 mars 2010, Commission européenne contre République fédérale d'Allemagne, considérant 50.

c) La clarification des règles applicables aux avocats en qualité d'agents de protection de données

La Commission envisage de rendre obligatoire de désigner un haut responsable indépendant à la protection des données et d'harmoniser les règles relatives à leurs tâches et leurs compétences.

À cet égard, il sera nécessaire de clarifier, à la lumière de leurs obligations en vertu du secret professionnel, les règles applicables aux avocats en qualité d'agents de la protection des données.

Le CCBE souhaite se référer aux règles nationales relatives aux avocats agissant à titre d'agents de protection des données, qui permettent aux avocats d'assumer leur rôle d'agents de la protection des données tout en conservant leurs obligations de secret professionnel. Le CCBE renvoie par exemple à l'article français 6.2.2 sur l'activité d'agent de protection des données dans le *Règlement intérieur national de la profession d'avocat* en France[2].

d) La participation du CCBE aux activités du GT29

La Commission européenne indique dans son communiqué que le groupe de travail sur l'article 29 devrait devenir un organe plus transparent.

Tenant compte de l'impact énorme de ce groupe de travail sur l'interprétation et l'application pratique du cadre juridique de la protection des données dans l'Union européenne et au-delà, le CCBE partage pleinement l'avis de la Commission selon lequel le groupe de travail doit devenir plus transparent dans ses procédures et ses méthodes de travail.

Étant donné que la profession juridique est considérée comme une profession totalement indépendante comportant des exigences très précises en matière de respect de la protection des données, le CCBE estime que les activités du groupe de travail devraient être ouvertes aux représentants de la profession d'avocat.

e) La redéfinition des données judiciaires comme données sensibles

En ce qui concerne le traitement des données sensibles, une catégorie devant être examinée de manière plus approfondie est celle des données personnelles utilisés dans les procédures civiles ou pénales, également appelées données judiciaires. À l'heure actuelle, les données judiciaires ne sont pas explicitement mentionnées comme constituant une catégorie spéciale de données dans le cadre de l'article 8 de la directive relative à la protection des données. La directive actuelle prévoit simplement que le traitement des données à caractère personnel utilisées dans les procédures civiles ou pénales « ne peut être effectué que sous le contrôle de l'autorité publique ou si des garanties appropriées et spécifiques sont prévues par le droit national, sous réserve des dérogations qui peuvent être accordées par l'État membre sur la base de dispositions nationales prévoyant des garanties appropriées et spécifiques ».

Le CCBE invite les institutions européennes à chercher à harmoniser les règles de protection minimale des données à caractère personnel dans les procédures judiciaires en respectant cependant toujours les règles et pratiques en vigueur dans les juridictions des États membres en ce qui concerne le caractère public des procédures judiciaires.

f) Une réduction du nombre de formalités administratives

Le système actuel de notifications des des activités de traitement données impose un fardeau inutile au contrôleur de données, en particulier à l'avocat qui travaille seul.

---

[2] Article 6.2.2 du Règlement intérieur national de la profession d'avocat (RIN) : l'activité de correspondant à la protection des données personnelles (L. n° 78-17 du 6 janv. 1978, art.22 ; D. n° 2005-1309 du 20 oct. 2005, art. 49 et s.)
6.2.2.1 Dans son activité de correspondant à la protection des données personnelles, l'avocat reste tenu de respecter les principes essentiels et les règles du conflit d'intérêt.
6.2.2.2 L'avocat correspondant à la protection des données personnelles doit mettre un terme à sa mission s'il estime ne pas pouvoir l'exercer, après avoir préalablement informé et effectué les démarches nécessaires auprès de la personne responsable des traitements ; en aucun cas il ne peut dénoncer son client.

Le CCBE soutient la proposition de la Commission européenne de réduire la charge administrative pour les entreprises et les organisations tout en assurant une protection efficace des données.

g) Questions extraterritoriales : participations aux négociations des accords internationaux contraignants avec les pays hors UE

Quelle que soit l'efficacité d'un régime européen révisé de protection des données, il sera inefficace si l'activité qu'il visait à réglementer est exploitée par des entités ne relevant pas de la compétence territoriale.

Le CCBE est d'avis que l'expertise européenne dans les règles de protection des données et les solutions techniques devrait être encouragée au niveau international, surtout depuis que les nouvelles technologies de l'information et de la communication (l'informatique dématérialisée par exemple) peuvent conduire à ce que des données personnelles soient conservées en dehors de l'Union européenne sans que le contrôleur ni la personne concernée ne soit informée de son emplacement géographique.

Le CCBE encourage la Commission à s'engager dans la négociation d'accords internationaux contraignants avec les pays non-membres de l'UE afin d'augmenter l'étendue de la protection des données personnelles à l'échelle internationale.Les éléments essentiels à prendre en compte dans le cadre de négociations d'accords internationaux sont les suivants :

- les conditions générales de licéité des traitement prévues dans la réglementation européenne sont respectées (chapitre II de la Directive95/46/CE).
- la personne concernée peut défendre ses intérêts en cas de non-respect de ces principes (droit d'accès, de rectification et d'agir en justice).
- un organisme de surveillance indépendant est prévu.

h) Codes de pratique et autorégulation

La Commission européenne envisage d'étudier la création éventuelle de systèmes de certification communautaires (des « sceaux de protection », par exemple) pour des processus, technologies, produits et services « respectant la vie privée ».

Bien qu'étant favorable à des codes de pratiques et à l'autorégulation, le CCBE met en garde contre l'excès de zèle que présente l'idée selon laquelle les régimes complémentaires de certification ou d'enregistrement seraient nécessairement souhaitables.

Dans chaque cas, il conviendrait de demander, le cas échéant, ce qui pourrait être réalisé au-delà de ce qui est déjà susceptible d'être atteint dans les codes de pratique et les programmes d'auto-réglementation ou non obligatoires. Les suggestions indiquant qu'il devrait y avoir une certaine forme de certification ou d'enregistrement par un « sceau » pourraient s'avérer à la fois bureaucratiques et inutiles et ne serviraient qu'à augmenter le coût des affaires.

Dans cet esprit, le recours à des régimes de certification en matière de protection des données, applicables aux responsables du traitement de données, constitue une voie qui mérite toute notre attention. Il est en définitive plus aisé de contrôler qu'une procédure et un cahier des charges ont été respectés, plutôt que de déterminer que les interdictions posées par la législation ont été violées. L'obtention de tels labels, attestant que le responsable du fichier a respecté ses obligations, présente les avantages suivants :

- démarche volontaire et proactive
- domaine délimité et entièrement audité
- les problèmes sont préalablement solutionnés et des contrôles ultérieurs sont programmés

Au contraire, une démarche purement coercitive de contrôle présente les inconvénients suivants :

- opération subie et réactive
- domaine délimité et souvent partiellement audité

- Les problèmes constatés sont résolus ultérieurement

Dans cette perspective et afin d'éviter la multiplication des labels impliquant une inévitable disparité des exigences minimales, une multiplication des procédures nationales et l'augmentation des coûts, l'instauration d'un régime européen de certification serait utile.

i) Les règles de protection des données dans le domaine de la coopération policière et judiciaire en matière pénale

La directive relative à la protection des données s'applique à toutes les activités de traitement des données à caractère personnel dans les États membres, aussi bien dans les secteur public que privé. Elle ne s'applique cependant pas au traitement des données à caractère personnel dans le cadre d'activités ne relevant pas du champ d'application du droit communautaire, telles que les activités du domaine de la coopération policière et judiciaire en matière pénale.

Le CCBE approuve l'analyse de la Commission européenne dans son communiqué[3] et soutient donc l'extension de l'application des règles générales de protection des données aux domaines de la coopération policière et judiciaire en matière pénale, y compris pour le traitement de données sur le plan national tout en assurant, le cas échéant, des limitations harmonisées de certains droits de protection des données à caractère personnel, par exemple concernant le droit d'accès ou le principe de transparence. Néanmoins, cette extension doit dans tous les cas tenir compte des caractéristiques spécifiques des activités des avocats, ainsi que la prévalence du droit de se faire assister par un conseil et du droit à une protection juridique effective.

3. Recommandations du CCBE

Le CCBE invite donc instamment les institutions européennes à prendre en compte les lignes directrices suivantes lors de l'élaboration du cadre juridique de l'Europe sur le droit fondamental à la protection des données à caractère personnel :

1. Prendre en compte la situation spécifique de l'avocat qui défend les intérêts d'une partie en particulier et est soumis à des règles déontologiques et légales strictes
2. Veiller à ce que le secret professionnel de l'avocat l'emporte sur toutes les règles de protection des données.
3. Veiller à ce que le contrôle de la conformité aux règles de protection des données par les avocats soit exclusivement réalisé par une autorité indépendante spéciale familière aux intérêts de la profession d'avocat
4. Clarifier, à la lumière de leurs obligations en vertu du secret professionnel, les règles applicables aux avocats en qualité d'agents de protection de données
5. Ouvrir les activités du groupe de travail 29 à des représentants de la profession d'avocat
6. Chercher à harmoniser les règles de protection minimale des données à caractère personnel dans les procédures judiciaires en respectant cependant toujours les règles et pratiques en vigueur dans les juridictions des États membres en ce qui concerne le caractère public des procédures judiciaires
7. Réduire la charge administrative liée au système actuel de notification pour les contrôleurs de données
8. S'engager dans la négociation d'accords internationaux contraignants avec les pays non-membres de l'UE afin d'augmenter l'étendue de la protection des données personnelles à l'échelle internationale
9. Adopter une approche réaliste/pragmatique en matière de programmes de certification de confidentialité
10. Étendre l'application des règles générales de protection des données aux domaines de la coopération policière et judiciaire en matière pénale en prévoyant, si nécessaire, des

[3] Voir COM (2010) 609 final, chapitre 2.3, pp. 13-14.

limitations harmonisées de certains droits individuels à la protection des données et en tenant compte des caractéristiques spécifiques des activités des avocats ainsi que la prévalence du droit de se faire assister par un conseil et du droit à une protection juridique effective.

En outre, le CCBE tient à réaffirmer une fois de plus les lignes directrices suivantes, découlant de sa prise de position[4] antérieure à un examen du cadre juridique de protection des données :

1. Veiller à ce que le secret professionnel des avocats soit garanti dans le cadre de la protection des données lorsque les gouvernements et autres autorités compétents accèdent aux données de trafic et de communication conservées
2. Veiller à ce que l'accès aux données conservées soit accordé en vertu de la législation uniquement avec une autorisation judiciaire préalable
3. Veiller à ce que, lorsque le gouvernement ou l'autorité d'exécution des lois a consulté les données, celles-ci ne soient utilisées et conservées qu'aussi longtemps que nécessaire aux fins pour lesquelles les données ont été fournies à l'origine, telle qu'elle sont protégées en vertu de l'article 6 de la directive 95/46/CE et l'article 6, paragraphe 1 de la directive 2002/58/CE
4. Veiller à faire figurer dans la législation un niveau élevé de mesures de protection sauvegardant le principe de respect de la vie privée et la confidentialité des communications, tels qu'ils sont protégés en vertu des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne et l'article 8 de la Convention européenne des droits de l'homme

Enfin, le CCBE tient à exprimer sa volonté d'apporter de nouvelles contributions ainsi que son expertise aux futures consultations ou propositions de la Commission européenne en la matière.

[4] Prise de position du CCBE sur le cadre juridique du droit fondamental à la protection des données personnelles