FICHE D'INFORMATION TECHNIQUE | ACTUALISATION : 13 DECEMBRE 2017

LA RÈGLEMENTATION INFORMATIQUE ET LIBERTÉS APPLICABLE AUX AVOCATS

A PARTIR DU 25 MAI 2018

Application, dans tous les pays de l'UE, du règlement n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données - RGPD)

http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR

TEXTES TOUJOURS APPLICABLES

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (sera modifiée en 2018)

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460

Décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000241445

Etablissement d'utilité publique - Art. 21-1 de la loi n°71-1130 du 31 décembre 1971 modifiée
22 rue de Londres 75009 Paris ● Tél 01 53 30 85 60 ● Fax 01 53 30 85 61 ● cnb@cnb.avocat.fr ● www.cnb.avocat.fr

LA REFORME DE LA PROTECTION DES DONNEES IMPOSEE PAR LE RGPD POURSUIT TROIS OBJECTIFS

Le RGPD a pour objectif de moderniser le cadre européen de la protection des données personnelles afin de prendre en compte les avancées technologiques et de réduire, voire supprimer, les écarts juridiques entre les législations des Etats membres de l'Union européenne. En pratique, il vise à :

- Renforcer les droits des personnes, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures ;
- Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants) ;
- Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux et des sanctions renforcées.

Avec le RGPD, la responsabilité des organismes se trouve renforcée : ceux-ci devront en effet assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité.

Les principales mesures imposées par le RGPD sont les suivantes[1] :

- Intégrer les concepts de protection des données personnelles dès la conception et par défaut les impératifs demandés dans toutes les technologies exploitant des données à caractère personnel des dispositifs techniques de protection des données personnelles et des mesures organisationnelles permettant d'anticiper la problématique de protection des données personnelles ;
- Prendre en compte le principe d'accountability qui impose aux entreprises d'être en mesure de justifier l'ensemble des dispositifs de contrôle et d'encadrement mis en place pour assurer la conformité Informatique et libertés ;
- Notifier à la Cnil toute violation de données à caractère personnel ;
- Introduire la fonction de Data Protection Officer au sein de l'entreprise.

[1] Source : www.cnil.fr

Etablissement d'utilité publique - Art. 21-1 de la loi n°71-1130 du 31 décembre 1971 modifiée
22 rue de Londres 75009 Paris ● Tél 01 53 30 85 60 ● Fax 01 53 30 85 61 ● cnb@cnb.avocat.fr ● www.cnb.avocat.fr

DEFINITIONS (RGPD, ARTICLE 4)

- **Données à caractère personnel** : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

- **Traitement** : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

- **Responsable du traitement** : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

- **Sous-traitant** : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

- **Destinataire** : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement.

Etablissement d'utilité publique - Art. 21-1 de la loi n°71-1130 du 31 décembre 1971 modifiée
22 rue de Londres 75009 Paris ● Tél 01 53 30 85 60 ● Fax 01 53 30 85 61 ● cnb@cnb.avocat.fr ● www.cnb.avocat.fr

LES PRINCIPALES NOUVELLES MESURES DE CONFORMITE POUR LES AVOCATS

A. Notification de toute violation de données à caractère personnel

En vertu de l'article 33 du RGPD, un cabinet d'avocats agissant en tant que responsable du traitement des données doit notifier toute violation de données à caractère personnel à l'autorité de contrôle dans les meilleurs délais, et dans tous les cas 72 heures au plus tard après en avoir pris connaissance. Les notifications tardives doivent être justifiées.

Il y a exception lorsque la violation de données n'est pas susceptible de porter atteinte à la ou aux personne(s) concernée(s).

La notification doit, entre autres choses, préciser la nature de la violation des données à caractère personnel (catégories et nombre approximatif de personnes et d'enregistrements de données concernés), les conséquences probables de la violation et les mesures prises ou à prendre en vue d'atténuer les éventuelles conséquences négatives. La notification peut s'effectuer en plusieurs étapes.

En outre, le responsable du traitement doit documenter ces violations de manière suffisamment détaillée pour que l'autorité de contrôle puisse vérifier le respect de l'obligation de notification.

Dans ce cadre, en application de l'article 33-5 du RGPD, il conviendra de tenir un registre des violations de données à caractère personnel qui devra préciser les faits concernant la violation des données, ses effets et les mesures prises pour y remédier.

Les cabinets d'avocats sont également tenus d'instaurer des **procédures internes** relatives à la gestion des violations de données à caractère personnel, ainsi qu'un **mécanisme de notification** à l'autorité de contrôle.

Dans certains cas à risque élevé, le cabinet d'avocats est également tenu de **notifier directement ses clients** (RGPD, art. 34), bien qu'il y ait des exemptions particulières.

En vertu de l'article 70.1 g) et h) du RGPD, le comité européen de la protection des données publiera vraisemblablement des lignes directrices, des recommandations et des bonnes pratiques pour :

a) décrire la nature des violations,

b) définir les « meilleurs délais » et

c) préciser les circonstances dans lesquelles un responsable du traitement ou un sous-traitant est tenu de notifier la violation à l'autorité de contrôle ou à ses clients.

Etablissement d'utilité publique - Art. 21-1 de la loi n°71-1130 du 31 décembre 1971 modifiée
22 rue de Londres 75009 Paris ● Tél 01 53 30 85 60 ● Fax 01 53 30 85 61 ● cnb@cnb.avocat.fr ● www.cnb.avocat.fr

B. Droit à l'oubli

L'article 17 du RGPD inclut le droit à l'effacement (« droit à l'oubli »), ce qui signifie que les personnes concernées ont le droit d'obtenir du responsable du traitement, dans les meilleurs délais, l'effacement des données à caractère personnel les concernant.

L'article 17 du RGPD oblige par ailleurs le responsable du traitement à **effacer des données à caractère personnel dans les meilleurs délais** lorsque l'un des motifs exposés au point 1 a) à f) s'applique. Cette disposition a des antécédents dans l'affaire Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, dans laquelle la Cour a déclaré que les personnes physiques ont le droit (sous réserve de certaines conditions et garanties) de demander à un moteur de recherche de supprimer les liens renvoyant à des données à caractère personnel les concernant. Néanmoins, le point 3 e) de l'article 17 comporte une restriction importante que les cabinets d'avocats peuvent invoquer dans la mesure où leurs activités de traitement sont nécessaires « à la constatation, à l'exercice ou à la défense de droits en justice ».

Il est important de noter que cela ne prévaut évidemment pas sur certaines obligations d'archivage de données pendant des périodes déterminées, par exemple pour des raisons de conformité aux obligations fiscales ou de prescription.

C. Analyses d'impact

En vertu de l'article 35 du RGPD, lorsqu'un type de traitement est susceptible d'engendrer un **risque élevé pour les droits et libertés des personnes physiques**, y compris le **traitement à grande échelle de catégories particulières de données,** le responsable du traitement doit effectuer, avant le traitement, une analyse d'impact (en particulier en cas de recours aux nouvelles technologies, etc.).

Il est important de noter que le **considérant 91 explique que le traitement de données à caractère personnel de clients par un avocat exerçant à titre individuel ne devrait pas être considéré comme étant à grande échelle.** Il s'agit d'une exemption qui peut manifestement s'appliquer aux avocats exerçant seuls. **Néanmoins, même un cabinet d'avocats de petite taille pourrait avoir à fournir ce genre d'analyses d'impact de temps à autre.**

Bien qu'elles représentent une charge supplémentaire, les analyses d'impact visent à permettre aux responsables de traitements d'identifier et de traiter les risques qui n'auraient pas été détectés en d'autres temps et d'empêcher des violations qui se seraient autrement produites.

Pour expliquer l'article 35 et en proposer une interprétation commune, les autorités de protection des données européennes (le G29) ont adopté des « lignes directrices » sur les DPIA et les traitements susceptibles d'engendrer des risques : https://www.cnil.fr/fr/reglement-europeen/lignes-directrices

Le 22 novembre 2017, la CNIL a mis en ligne sur son site un logiciel open source PIA facilitant la conduite et la formalisation d'analyses d'impact sur la protection des données telles prévues par le RGPD : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

La CNIL a également publié trois catalogues de bonnes pratiques destinées à traiter les risques que les traitements de données à caractère personnel (DCP) peuvent faire peser sur les libertés et la vie privée des personnes concernées : https://www.cnil.fr/fr/PIA-privacy-impact-assessment

22 rue de Londres 75009 Paris ● Tél 01 53 30 85 60 ● Fax 01 53 30 85 61 ● cnb@cnb.avocat.fr ● www.cnb.avocat.fr

D. Portabilité des données

Les personnes concernées ont le droit d'obtenir du responsable du traitement une copie des données à caractère personnel leur appartenant qui font ou ont fait l'objet d'un traitement. L'article 20 du RGPD exige que ces données soient remises dans un format structuré, couramment utilisé et lisible par machine, mais il s'agit uniquement d'exigences génériques.

En vertu des lignes directrices du groupe de travail « Article 29 » sur le droit à la portabilité des données, les expressions « structuré », « couramment utilisé » et « lisible par machine » forment un ensemble d'exigences minimales qui ont pour objectif de faciliter l'interopérabilité du format des données fournies par le responsable du traitement. Les lignes directrices du groupe de travail « Article 29 » indiquent par ailleurs qu'étant donné le vaste éventail de données pouvant être potentiellement traitées par un responsable du traitement des données, le RGPD n'impose aucune recommandation spécifique quant au format des données à caractère personnel à fournir :
https://www.cnil.fr/fr/reglement-europeen/lignes-directrices

E. Capacité à suivre les destinataires de données à caractère personnel

Les responsables du traitement de données sont tenus d'être en mesure de suivre les destinataires de données à caractère personnel appartenant à une personne donnée (nom et coordonnées électroniques au minimum). Il s'agit également d'une obligation que de nombreux cabinets d'avocats ne pourraient respecter qu'en apportant certains changements à leur système informatique, par exemple en le configurant de manière à retracer de manière fiable les destinataires de données à caractère personnel.

F. Tenue d'un registre des activités de traitement

Le RGPD impose dans certains cas aux responsables de traitement de tenir un registre des activités de traitement effectuées sous leur responsabilité.

En tout état de cause, la tenue d'un registre contribue au respect du principe d'accountability (consistant à documenter la conformité pour pouvoir la prouver) et, à ce titre, est vivement conseillée.

Le registre doit, conformément à l'article 30 du règlement, comporter les informations suivantes :

- Le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données;
- Les finalités du traitement ;
- Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et les documents attestant de l'existence de garanties appropriées ;
- Une description des catégories de données traitées, ainsi que les catégories de personnes concernées par le traitement ;
- Dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles mises en œuvre.

22 rue de Londres 75009 Paris ● Tél 01 53 30 85 60 ● Fax 01 53 30 85 61 ● cnb@cnb.avocat.fr ● www.cnb.avocat.fr

G. Délégué à la protection des données

Obligation des cabinets d'avocats de désigner un délégué à la protection des données

Autre nouveauté de la réforme : l'exigence de la désignation d'un délégué à la protection des données dans certains cas. Aux termes de l'article 37 du RGPD, les responsables de traitement et les sous-traitants devront obligatoirement désigner un délégué :

- S'ils appartiennent au secteur public,
- Si leurs activités de base (principales) les amènent à réaliser **un suivi régulier et systématique des personnes à grande échelle**,
- Si leurs activités de base (principales) les amènent à traiter (toujours à grande échelle) **des catégories particulières de données**, dites « sensibles », et **des données relatives à des condamnations pénales et à des infractions.**

En dehors de ces cas, la désignation d'un délégué à la protection des données sera bien sûr possible, et même **recommandée**.

Les responsables de traitement peuvent opter pour un délégué à la protection des données mutualisé ou externe.

Le groupe de travail « Article 29 » (G29), composé de représentants des autorités de protection des données des États membres de l'UE, a publié des lignes directrices sur le rôle des délégués à la protection des données et a fourni des recommandations concernant les bonnes pratiques.

Si un délégué à la protection des données est désigné, l'organisation est tenue de publier les informations relatives au délégué à la protection des données et de les communiquer à l'autorité de contrôle compétente.

L'article 9 du RGPD définit des catégories particulières de données à caractère personnel[2], dont le traitement est interdit, sauf exceptions : dans le cadre de l'article 9.2 f), cette interdiction ne s'applique pas au traitement de données nécessaires à « la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ». **Par conséquent, cette disposition valide le traitement de catégories particulières de données dans le cadre d'activités juridiques contentieuses de cabinets d'avocats.**

Néanmoins, l'article 37 (de même que l'article 35, voir ci-dessous) s'applique toujours au responsable du traitement ou au sous-traitant de catégories particulières de données. Ces dispositions exigent la désignation du délégué à la protection des données dans les cas où les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement **à grande échelle de catégories particulières de données visées à l'article 9.** Selon les lignes directrices sur les délégués à la protection des données, les « **activités de base** peuvent être considérées comme l'ensemble des activités pour lesquelles le traitement de données fait partie intégrante des activités du responsable du traitement ou du sous-traitant».

[2] Par exemple « […] [l]es données à caractère personnel qui révèle[nt] l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique […] ».

22 rue de Londres 75009 Paris ● Tél 01 53 30 85 60 ● Fax 01 53 30 85 61 ● cnb@cnb.avocat.fr ● www.cnb.avocat.fr

La signification de l'expression **« à grande échelle »** revêt une importance particulière, étant donné qu'un petit cabinet d'avocats peut avoir à traiter des dossiers impliquant des quantités considérables de données. Néanmoins, le considérant 91 permet de soutenir facilement que cette exigence ne s'appliquera pas aux avocats qui exercent à titre individuel (voir ci-dessus le point relatif à l'analyse d'impact).

Ainsi, l'appréciation de l'obligation de désigner ou non un délégué à la protection des données doit se faire au cas par cas, en fonction notamment du nombre de personnes concernées par les traitements de données à caractère personnel, du volume des données traitées, de la durée ou de la permanence des activités de traitement, de l'étendue géographique de l'activité de traitement.

Obligations et missions du délégué à la protection des données

Le RGPD impose des obligations importantes aux délégués à la protection des données.

« Chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme, le délégué à la protection des données est principalement chargé :

- D'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- De s'assurer du respect du règlement et du droit national en matière de protection des données ;
- De conseiller l'organisme sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution ;
- De coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Pour vous accompagner dans la mise en place des nouvelles obligations imposées par le règlement européen, le délégué doit notamment :

- S'informer sur le contenu des nouvelles obligations ;
- Sensibiliser les décideurs sur l'impact de ces nouvelles règles ;
- Réaliser l'inventaire des traitements de données de votre organisme ;
- Concevoir des actions de sensibilisation ;
- Piloter la conformité en continu.

En conséquence, la personne qui agit en tant que délégué à la protection des données endossera d'importantes responsabilités.

Avocat agissant en tant que délégué à la protection des données

La décision à caractère normatif portant réforme des articles 6 « Le champ d'activité professionnelle de l'avocat » et 19 « Prestations juridiques en ligne » du Règlement intérieur national (RIN) de la profession d'avocat, adoptée par l'assemblée générale du Conseil national des barreaux des 9 et 10 décembre 2016[3] sur la base d'un rapport de sa commission des règles et usages, et après concertation de la profession, a modifié les dispositions encadrant la mission d'avocat-CIL : https://www.cnb.avocat.fr/reglement-interieur-national-de-la-profession-davocat-rin#

[3] publiée au Journal officiel du 13 avril 2017

22 rue de Londres 75009 Paris ● Tél 01 53 30 85 60 ● Fax 01 53 30 85 61 ● cnb@cnb.avocat.fr ● www.cnb.avocat.fr

L'article 6.3.3 « Correspondant à la protection des données à caractère personnel – Correspondant Informatique et libertés (CIL) » du RIN prévoit désormais :

« L'avocat correspondant à la protection des données à caractère personnel 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.

L'avocat correspondant à la protection des données à caractère personnel doit refuser de représenter toute personne ou organisme pour lesquels il exerce ou a exercé la mission de correspondant à la protection des données à caractère personnel dans le cadre de procédures administratives ou judiciaires mettant en cause le responsable des traitements. »

A compter du 25 mai 2018, ces dispositions seront remplacées par les dispositions suivantes :

« 6.3.3 : Délégué à la Protection des Données.

L'avocat Délégué à la Protection des Données 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.

L'avocat Délégué à la Protection des Données doit refuser de représenter toute personne ou organisme pour lesquels il exerce ou a exercé la mission de correspondant à la protection des données à caractère personnel (CIL) ou de Délégué à la Protection des Données dans le cadre de procédures administratives ou judiciaires mettant en cause le responsable des traitements. »

L'avocat-CIL était déjà soumis à deux devoirs qui ne s'imposent pas au CIL non avocat : le devoir de non-dénonciation de son client et le devoir de démission en cas de conflit d'intérêts. Il est apparu nécessaire de préciser que l'avocat doit refuser de représenter les clients pour lesquels il exerce ou a exercé la mission de CIL dans les procédures mettant en cause le responsable des traitements, afin d'éviter toute situation de conflit d'intérêts ou de violation du secret professionnel.

Par ailleurs, l'article 6.4 « Déclarations à l'Ordre » du RIN dispose :

*« **L'avocat qui entend exercer l'activité de** mandataire en transaction immobilière, en gestion de portefeuille ou d'immeubles, de mandataire sportif, de mandataire d'artistes et d'auteurs, d'intermédiaire en assurances, de lobbyiste, de syndics de copropriété et de **Correspondant à la protection des données à caractère personnel – Correspondant Informatique et libertés (CIL) doit en faire la déclaration à l'Ordre, par lettre ou courriel adressée au Bâtonnier.** »*

A compter du 25 mai 2018, dans l'article 6.4, les mots *« Correspondant à la protection des données à caractère personnel Correspondant Informatique et libertés (CIL) »* sont remplacés par les mots *« Délégué à la Protection des Données ».*

Il s'agit d'une simple obligation de déclaration, sans contrainte formelle. Ainsi, cette déclaration vise d'une part à permettre une meilleure formation des avocats souhaitant les exercer, et d'autre part à permettre aux Ordres de communiquer sur les avocats exerçant ces misions dans leur ressort.

22 rue de Londres 75009 Paris ● Tél 01 53 30 85 60 ● Fax 01 53 30 85 61 ● cnb@cnb.avocat.fr ● www.cnb.avocat.fr

POUR EN SAVOIR PLUS

- **Lignes directrices du G29** :
  https://www.cnil.fr/fr/reglement-europeen/lignes-directrices
  - Délégué à la protection des données (5/05/2017)
  - Analyse d'impact relative à la protection des données (DPIA) (4/10/2017)
  - Portabilité (5/05/2017)
  - Désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant (5/05/2017)

- **Lignes directrices du Conseil des barreaux européens (CCBE[4]) sur les principales nouvelles mesures de conformité des avocats au RGPD (19/05/2017)** :
  http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/FR_ITL_20170519_CCBE-Guidance-on-main-new-compliance-measures-for-lawyers-regarding-GDPR.pdf

AUTRE TEXTE EN VIGUEUR

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil :
http://eurlex.europa.eu/legalcontent/FR/AUTO/?uri=uriserv:OJ.L_.2016.119.01.0089.01.FRA&toc=OJ:L:2016:119:TOC

[4] Le Conseil des barreaux européens représente les barreaux de 32 pays membres et 13 pays associés et observateurs, soit plus d'un million d'avocats européens.

22 rue de Londres 75009 Paris ● Tél 01 53 30 85 60 ● Fax 01 53 30 85 61 ● cnb@cnb.avocat.fr ● www.cnb.avocat.fr