Conseil des barreaux européens
Council of Bars and Law Societies of Europe
Association internationale sans but lucratif
Rue Joseph II, 40 /8 – 1000 Bruxelles
T. : +32 (0)2 234 65 10
Email : ccbe@ccbe.eu – www.ccbe.eu

Lignes directrices du CCBE sur les principales nouvelles mesures de conformité des avocats au règlement général sur la protection des données (RGPD)

19/05/2017

Le Conseil des barreaux européens (CCBE)[1] souhaite à l'aide du présent document offrir un aperçu des principales nouvelles mesures de conformité qu'il serait bon que les barreaux recommandent en vue de garantir la conformité aux exigences du RGPD.

Les parties suivantes soulignent les aspects du RGPD qui créent ou accroissent les responsabilités en matière de conformité, en particulier pour les avocats et les cabinets d'avocats. L'objectif de la mise en évidence de ces aspects et de permettre aux cabinets d'avocats d'identifier les problèmes qui devraient être prioritaires. Étant donné que la grande majorité des cabinets d'avocats européens comptent moins de 250 employés, les problèmes abordés ci-dessous ne concernent pas les dispositions qui s'appliquent uniquement aux cabinets de plus grande taille (par exemple, l'obligation d'avoir un délégué à la protection des données). Il convient également de préciser que de nombreux cabinets d'avocats traitent des données à caractère personnel considérées comme des « catégories particulières de données à caractère personnel ».

A. Notification d'une violation de la sécurité

En vertu de l'article 33, 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).

Dans le cas où le cabinet d'avocats agit en tant que sous-traitant, il doit le notifier au responsable du traitement dans les meilleurs délais après avoir pris conscience de la violation des données à caractère personnel.

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.

[1] 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.

En outre, le responsable du traitement doit documenter ces violations de manière suffisamment détaillée pour que l'autorité de contrôle puisse vérifier qu'elles sont conformes à la notification de violation. 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 (article 34), bien qu'il y ait des exemptions particulières.

Manifestement, le format de notification, la définition de « meilleurs délais » et les exigences relatives au contenu de la documentation et de l'interprétation de l'autorité de contrôle concernant les seuils et les exemptions peuvent varier considérablement d'un État membre à l'autre.

Par conséquent, les cabinets d'avocats doivent être informés de toute ligne directrice nationale existante ou à venir à cet égard.

Bien que certains États membres aient déjà mis en œuvre dans leur droit national les conditions relatives à l'obligation de communication de violations de données, la directive 95/46/CE n'obligeait pas les responsables du traitement à communiquer les violations de données à l'autorité de contrôle. Néanmoins, ce type d'exigence existe déjà dans le secteur des télécommunications (voir la directive 2002/58/CE et le règlement de la Commission (UE) 611/2013, qui s'appliquent aux fournisseurs de services de communications électroniques). Ce dernier règlement de mise en œuvre a été défini indépendamment du secteur et, dans certains États membres, les autorités de contrôle de protection des données ou des télécommunications ont parfois publié des lignes directrices plus approfondies. De plus, en vertu de cette législation, le groupe de travail « Article 29 » des autorités de contrôle de la protection des données de l'Union européenne a également émis des lignes directrices détaillées concernant la mise en œuvre du règlement sur la violation des données (Avis 03/2014 WP 213 sur la notification des violations de données à caractère personnel du 25 mars 2014[2]), qui présente une série de bonnes pratiques à l'intention de tous les responsables du traitement des données.

Quant aux règlements à venir en la matière, 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) établir les 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.

B. Droit à l'oubli

L'article 17 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. Cet article 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[3], 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

[2] Accessible via http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_fr.pdf.

[3] http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d57637cb18820e4ceb913ecf71af33028d.e34KaxiLc3qMb40Rch0SaxuTahn0?text=&docid=152065&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=1115616.

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 de conservation de données au niveau local pendant une certaine période, par exemple pour des raisons de conformité aux obligations fiscales.

C. Délégué à la protection des données (DPD)

Obligation des cabinets d'avocats de désigner un DPD

L'un des nouveaux aspects est l'exigence de la désignation d'un DPD dans le cas où les activités de traitement des données d'une organisation impliquent un suivi régulier et systématique à grande échelle des personnes concernées ou le traitement à grande échelle de catégories particulières de données (article 37). Le groupe de travail « Article 29 » (WP29), composé de représentants des autorités de protection des données des États membres de l'UE, a publié des lignes directrices sur le rôle des DPD et a fourni des recommandations concernant les bonnes pratiques.

Si un DPD est désigné, l'organisation est tenue de publier les détails du DPD et de les communiquer à l'autorité de contrôle compétente.

L'article 9 du RGPD définit des catégories particulières de données à caractère personnel[4], dont le traitement est interdit, à quelques exceptions près : 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 DPD, 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 ».

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-dessous le point D relatif à l'analyse d'impact).

Obligations et missions du DPD

Le RGPD impose des obligations importantes aux DPD, telles que l'exigence de contrôle du respect du règlement, d'autres dispositions du droit de l'Union ou du droit des États membres en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition

[4] 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 […] ».

des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant. Les DPD font également office de point de contact pour les autorités de protection des données.

Le DPD désigné, qu'il soit employé ou non au sein d'un cabinet d'avocats, doit avoir des connaissances spécialisées du droit en matière de protection des données et être capable d'accomplir les missions visées à l'article 39 du RGPD, telles que le maintien des documents relatifs aux opérations de traitement, le suivi de leur mise en œuvre, la formation du personnel, la réalisation d'audits, etc. En conséquence, une personne qui agit en tant que DPD endossera de lourdes et importantes responsabilités.

Avocats agissant en tant que DPD

Un avocat pourrait être considéré comme la personne la plus à même d'être désignée DPD, mais il convient de garder à l'esprit qu'étant donné la diversité des devoirs qu'exige le règlement, une personne devant être désignée DPD ne devra pas uniquement témoigner de connaissances spécialisées.

L'assimilation de ces deux fonctions (avocat et DPD) et le risque de confusion entre celles-ci constituent un élément clé pour l'avocat susceptible d'être désigné DPD à la demande d'un client. Un avocat qui se retrouve dans cette situation devra vraisemblablement alterner entre la fonction de DPD et celle d'avocat exerçant une profession réglementée. Un avocat agissant en qualité de DPD sera tenu de garantir l'indépendance et d'éviter les conflits d'intérêts, en particulier ceux qui peuvent découler de la double fonction simultanée de personne de contact et d'autorité de protection des données. Ce rôle implique des obligations de communication à l'autorité même dans les cas où cela va à l'encontre de l'intérêt du responsable du traitement ou du sous-traitant. L'avocat qui assumera une telle fonction sera par ailleurs tenu de représenter les intérêts de son client dans la mesure où la loi le permet. Compte tenu de l'éventualité d'un conflit d'intérêts, il serait bon que les barreaux recommandent aux avocats d'endosser la responsabilité d'un DPD pour un client extérieur uniquement s'ils n'ont pas n'ont pas agi en tant qu'avocats dans des matières qui relèvent de la responsabilité du DPD ou si, au cours de leur mandat de DPD, ils n'agiront pas en tant qu'avocat dans des matières dans lesquelles ils étaient ou sont impliqués comme DPD.

D. Analyses d'impact

En vertu de l'article 35, 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 données spécialisées, le responsable du traitement doit effectuer, avant le traitement, une analyse d'impact (en particulier en cas de recours aux nouvelles technologies, dans l'examen des finalités du traitement, etc.).

Il est important de noter que le considérant 91 explique que le traitement de données à caractère personnel ne devrait pas être considéré comme étant à grande échelle si le traitement concerne les données à caractère personnel de clients par un avocat exerçant à titre individuel. 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.

Le problème est que selon les normes (non spécifiques à un secteur) relatives aux cadres d'analyse d'impact concernant la protection des données actuellement en vigueur, ce type d'analyses d'impact pourrait être interdit aux petits cabinets d'avocats. Par exemple, même une simple exigence que les responsables du traitement des données identifient des biens logiciels et du matériel informatique, dont des données à caractère personnel pourraient dépendre, pourrait être interprétée par certaines autorités comme une exigence visant à mettre en œuvre une configuration et à changer le système de

gestion. De manière générale, les petits cabinets d'avocats qui possèdent peu d'employés (mais qui dépassent le seuil de « l'avocat exerçant à titre individuel ») ne sont pas en mesure de respecter ces exigences au sens strict dans tous les cas. Un changement du système de gestion exigerait un mode de fonctionnement réfléchi et contrôlé de leur système informatique, ce qui n'est en général pas le cas des cabinets de cette taille (il y a une grande différence entre le fait d'avoir une vue d'ensemble des composants informatiques d'un cabinet d'avocats et le fait disposer d'une configuration contrôlée et opérationnelle et d'une gestion du changement).

Malheureusement, ni les lignes directrices du groupe de travail « Article 29 » sur les délégués à la protection des données (« DPD ») adoptées le 13 décembre 2016 ni son projet de document actuellement disponible relatif aux directives sur l'analyse d'impact relative à la protection des données ne donnent de lignes directrices à cet égard. En ce qui concerne le considérant 91, la note de bas de page 14 des lignes directrices sur les DPD indique que tout ce qui se situe entre le traitement par un avocat exerçant à titre individuel et le traitement de données relatives à un pays tout entier est imprécis. Cette zone de flou mènera inévitablement à des divergences d'interprétation.[5]

Bien que cela représente une charge supplémentaire pour les cabinets d'avocats, le règlement espère leur permettre, au moyen d'analyses d'impact, d'être en mesure 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.

En comparaison avec la notification de violation de données, il n'y a aucun historique réglementaire ni ligne directrice clairs sur la manière dont les analyses d'impact doivent être menées par des cabinets d'avocats ou d'autres professions similaires.

Actuellement, les analyses d'impact relatives à la protection des données sont multiples dans leur contenu comme dans leur méthode, et sont généralement plébiscitées dans les pays de *common law*.[6] En Europe, l'Office du commissaire à l'information du Royaume-Uni a publié en 2014 un « *Privacy Impact Assessment Code of Practice* »[7] (à la suite du « *Privacy Impact Assessment Manual* » qui avait été publié en 2007), et la Commission nationale de l'informatique et des libertés (CNIL) française a publié un « *Privacy Impact Assessment Manual* » en 2015[8]. La Commission européenne a elle aussi publié une recommandation exigeant une analyse d'impact concernant les puces d'identification par radiofréquence (puces RFID)[9], qui a débouché sur un accord sectoriel conclu le 12 janvier 2011 : « *Privacy and Data Protection Impact Assessment Framework for RFID Applications* ». Ce dernier cadre a été approuvé par le groupe de travail « Article 29 » et a par ailleurs servi de modèle pour une initiative « modèle » semblable pour les systèmes intelligents de mesure.[10]

Malheureusement, ces recommandations sont spécifiques à leur sujet et ne seront virtuellement d'aucune aide en matière de lignes directrices pratiques sur l'analyse d'impact par des avocats ou des

---

5 Étant donné qu'au moment de la rédaction de ce document, le groupe de travail « Article 29 » est toujours en phase de collecte de commentaires de la part des parties intéressées concernant les lignes directrices sur l'analyse d'impact relative à la protection des données, il se peut qu'une version finale révisée soit publiée dans le courant de l'année 2017. Celle-ci contiendra peut-être des clarifications supplémentaires concernant la définition de « grande échelle » eu égard aux activités de traitement.

6 Les analyses d'impact sur l'environnement, qui proviennent des États-Unis, sont susceptibles de servir de base aux analyses d'impact sur la vie privée, voir le rapport D1 du PIAF (*Privacy Imapct Assessment Framework)* via http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf.

7 Voir https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

8 Voir https://www.cnil.fr/fr/PIA-privacy-impact-assessment.

9 Voir la recommandation 2009/387/CE de la Commission via http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:FR:PDF.

10 Voir la recommandation 2012/148/UE de la Commission et son approbation par le groupe de travail « Article 29 » via http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_fr.pdf.

professions similaires dans le cadre de la notification de violations de données. De plus amples détails devraient figurer dans lesrèglementations nationales et propres au secteur, si tant est qu'il y en aura.

Les résultats d'une étude sur les analyses d'impact financée par la Commission (*Privacy Impact Assessment Framework for data protection and privacy rights*) peut être utile aux avocats intéressés par le contexte général des analyses d'impact relatives à la vie privée.[11]

En bref, bien que le règlement lui-même aborde en détail les analyses d'impact, les exigences pratiques sont encore inconnues. Il est attendu que les autorités de contrôle ainsi que le comité mentionné ci-dessus donnent des lignes directrices supplémentaires concernant les détails manquants, comme ceux en lien avec le type d'opérations de traitement pour lesquelles ces analyses d'impact pourraient être requises.

E. 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 règlement 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.

Bien qu'il soit facile de répondre aux exigences concernant le format couramment utilisé et lisible par machine, la question d'un format « structuré » peut en revanche s'avérer particulièrement problématique. Le contenu des documents auxquels les avocats ont recours n'est généralement pas structuré (par exemple les formats Microsoft Word ou PDF). Il n'existe aucun format structuré universellement accepté pour la remise de dossiers judiciaires complets ou de dossiers.

Tous les avocats savent comment remettre des dossiers à des cabinets nouvellement désignés par leurs anciens clients, mais la question de la structure et du format exacts de cette remise constitue déjà parfois un sujet de conflits entre avocats. À l'avenir, cette question devrait probablement être davantage réglementée par les barreaux.

F. 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.

[11] http://www.piafproject.eu/About%20PIAF.html