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 – F. : +32 (0)2 234 65 11
Email : ccbe@ccbe.eu – www.ccbe.eu

Étude comparative du CCBE sur la surveillance gouvernementale des données des avocats hébergées dans le nuage

4 avril 2014

Sommaire

1. Introduction :

Notre liberté repose sur l'État de droit. Si celui-ci n'est pas respecté, la tyrannie, la corruption et l'exercice arbitraire du pouvoir s'installent : les forts prospèrent, les faibles souffrent et la justice se révèle inexistante.

Afin que l'État de droit fonctionne convenablement, certaines conditions s'avèrent nécessaires, notamment une profession d'avocat solide et indépendante. Les communications entre les avocats et leurs clients doivent demeurer confidentielles, de sorte que les avocats défendent les droits de leurs clients de manière efficace. Certaines juridictions en Europe répondent à cette exigence en protégeant ces communications à l'aide du secret professionnel de la profession d'avocat, d'autres en les considérant comme confidentielles. Bien que ces deux approches diffèrent sur le plan conceptuel et que les résultats pratiques précis qui en découlent divergent eux aussi, la finalité reste identique : la protection des informations communiquées dans le cadre des relations entre un avocat et son client. En l'absence d'une telle protection, le fonctionnement même de l'État de droit se trouve entravé.

Il fut un temps où ces commentaires auraient semblé bien ordinaires dans une société européenne respectant l'État de droit. La pierre angulaire de la liberté se trouve cependant menacée en raison de l'utilisation accrue de moyens de communication électroniques et, plus récemment, de l'informatique en nuage.

Lors de la guerre froide, chaque camp connaissait ses ennemis qui, eux aussi, se constituaient de gouvernements et d'États-nations. Cette conception est depuis longtemps révolue. Depuis les attentats contre le *World Trade Center*, les ennemis peuvent très bien se révéler être des groupements libres d'individus qui ne prêtent allégeance qu'à des doctrines extrêmes et se montrer impitoyables dans la poursuite de celles-ci, allant même jusqu'à souhaiter leur propre mort. Les sociétés éprouvent un besoin manifeste et légitime de se protéger contre une attaque terroriste, et le seul moyen d'y parvenir est de recueillir des renseignements.

La difficulté réside dans l'équilibre à atteindre entre le besoin de renseignements et le respect de la liberté et de l'État de droit. À l'une des extrémités siège la vision selon laquelle le meilleur moyen de préserver nos libertés ancestrales est de les détruire : par exemple, personne ne devrait plus s'attendre à ce que sa correspondance reste privée ; l'autre extrémité abrite la vision selon laquelle une société libre ne peut laisser place à aucune forme de surveillance que ce soit.

Cette étude ne porte en principe pas sur ce vaste débat (même si elle part notamment du principe que l'État de droit doit être préservé et que les gouvernements effectuent des opérations de surveillance). Elle traite avant tout de la manière dont les nations européennes établissent cet équilibre.

Ce débat s'avère bien plus que purement théorique aux yeux du CCBE car les informations confidentielles ou relevant du secret professionnel détenues par les avocats et leurs clients dans le cadre de leurs relations se trouvent de plus en plus exposées à la menace de la surveillance. Les informations qui jadis auraient été conservées au cabinet de l'avocat et littéralement mises sous clé sont aujourd'hui échangées entre l'avocat et son client par le biais de moyens électroniques sur internet et de plus en plus hébergées dans le nuage. Ces informations se retrouvent sur l'espace public avec pour seule protection une protection technique et juridique telle que l'encodage. Envoyées par courriels ou stockées, les données électroniques (ainsi que nous pouvons désormais les considérer) pourraient se trouver littéralement n'importe où dans le monde. Elles sont également susceptibles d'être interceptées et consultées non seulement par les agences de sécurité de l'État d'origine mais aussi par des puissances étrangères, que les rapports avec celles-ci soient « amicaux » ou non. Les données se trouvent dès lors plus à découvert que jamais.

Si plus rien ne garantit la confidentialité ou le secret des communications entre les avocats et leurs clients, l'État de droit se trouve lui-même sous la menace de cette surveillance qui vise peut-être pourtant à le protéger.

2. Portée du rapport

La question de la surveillance a récemment suscité de vives inquiétudes de la part de l'opinion publique à la suite des révélations apportées au lendemain de la fuite d'informations d'Edward Snowden concernant les activités des services de renseignements américains. Ces révélations

d'autant plus étonnantes que cet espionnage a été pratiqué sans le moindre fondement juridique approprié dans aucune des juridictions concernées. Si même les conversations téléphoniques confidentielles de la chancelière allemande sont mises sur écoute illégalement, comment pouvons-nous supposer que les communications entre les avocats et leurs clients bénéficieront d'une protection plus grande contre une telle activité illicite ?

Il est néanmoins dans la nature de ces activités (quiconque les ait entreprises) d'être réalisées en dehors de tout cadre juridique et, en général, d'échapper au contrôle de la population. C'est pour cette raison que ces activités ne sont pas soumises à une étude comparative systématique de la législation en matière d'accès aux données des avocats. Bien qu'elles soient mentionnées, elles ne font donc pas l'objet du présent rapport.

Le présent rapport porte plus précisément sur la mesure dans laquelle, dans les différentes juridictions européennes, les données électroniques des avocats sont soumises à un accès gouvernemental ainsi que les règles et les conditions de cet accès.

Avant d'entamer l'étude comparative, certaines précisions s'avèrent nécessaires :

Premièrement, bien que le rapport se réfère à « l'accès gouvernemental », il s'agit d'un terme vague et imprécis, étant donné que, selon la juridiction, l'accès est accordé au gouvernement national lui-même, aux différents niveaux du gouvernement (fédéral, national ou local), aux agences gouvernementales, aux autorités fiscales, aux agences indépendantes qui assurent des fonctions de droit public, à la police, aux procureurs, aux services secrets et à d'autres organismes. Le rapport traite de l'accès de l'État sous toutes ses formes et représentations aux données des avocats.

Deuxièmement, le rapport se concentre sur les données en format électronique et non en format papier. Toutefois, en raison de la nature de la réglementation de l'accès gouvernemental, la plupart des règles régissant l'accès gouvernemental ont été établies pour les documents papier. Il existe très peu de règles spécifiques aux données électroniques.

Troisièmement, le rapport traite des données détenues par les avocats et protégées par le secret professionnel : il ne porte pas simplement sur les données *concernant* les avocats.

La question du secret professionnel et de la confidentialité fut abordée dès 1975 dans un contexte technique et sécuritaire très différent, lorsque la Commission Consultative des Barreaux de la Communauté Européenne (ainsi qu'elle était désignée à l'époque) adopta une résolution intitulée *The Professional Secret: Confidentiality and Legal Professional Privilege in the Nine Member States of the European Community1* (ci-après le « rapport Edward »). Le présent rapport n'a nullement la prétention de mettre à jour ou de suppléer cet excellent travail, que ce soit en profondeur ou en portée. Les conclusions du rapport Edward2 ont toutefois servi de point de départ à l'étude du CCBE.

3. Structures de la réglementation et ossature du rapport

La plupart des juridictions disposent d'un cadre juridique général qui régit l'accès de l'État aux données électroniques. Le régime de réglementation général s'applique dans tous les pays avec des exceptions ou des protections prévues pour les avocats (soit exclusivement soit partiellement en commun avec d'autres professionnels). Celles-ci peuvent être d'origine législative/réglementaire ou découler de la jurisprudence ou du droit commun, par exemple en affirmant que le secret professionnel s'applique aux communications entre les avocats et leurs clients.

Le rapport fournit tout d'abord un bref aperçu de la réglementation dans les différentes

1 Élaborée par D.A.O. Edward, C.R., trésorier de la Faculté des avocats d'Écosse, rapporteur-général, disponible sur le site http://www.europarl.europa.eu/document/activities/cont/201312/20131204ATT75510/20131204ATT75510EN.pdf (consulté le 15 février 2013). Dernière mise à jour réalisée dans une certaine mesure par le CCBE en 2003, disponible sur le site http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/ccbeedward_report_update_/ccbeedward_report_update_en.pdf (consulté le 15 février 2013).

2 En particulier celles en matière de « protection des documents contre les perquisitions et les saisies » (C. 13-19) et « d'interception de courriels et d'écoutes téléphoniques » (C. 27 and C.40). Nous devons garder à l'esprit que le rapport Edward concernait neuf (9) États membres des Communautés européennes. Aujourd'hui, l'UE en compte 28.

juridictions. Cet aperçu repose dans la mesure du possible sur une structure analytique commune, elle-même fondée sur une structure similaire. Cette analyse nationale est suivie d'un récapitulatif succinct des similitudes les plus flagrantes entre les régulations. Le rapport présente finalement des recommandations de mesures communes.

L'analyse des différentes juridictions se fonde partiellement sur la connaissance personnelle des auteurs (pour l'Allemagne, l'Autriche, la Hongrie, la France, la République tchèque et le Royaume-Uni) et sur la multitude de réponses fournies à un questionnaire soumis aux membres du CCBE. Ne disposant pas de réponse à tous les aspects concernés, il a donc fallu omettre de l'analyse générale l'analyse de ces aspects dans ces juridictions.

L'objectif de ce rapport étant de fournir une synthèse comparative, l'analyse demeure nécessairement générale et n'a pas vocation à constituer un traité approfondi reprenant les détails des garanties et des voies de recours de chaque pays. Il se peut que cette simplification peut-être excessive omette certains éléments mais elle offre une analyse comparative claire. Force est toutefois de reconnaître qu'en raison de la diversité des systèmes, les termes anglais utilisés peuvent cacher des équivalents approximatifs. Par ailleurs, le présent rapport n'entend pas aborder la pratique en vigueur en matière d'exécution des lois. Les règles peuvent être appliquées de diverses manières dans les différentes juridictions. Nous ne devons donc jamais perdre de vue la possibilité que, même si les garanties juridiques semblent plus solides par écrit dans une juridiction donnée, le faible degré d'application des lois peut résulter en un niveau effectif réel de protection juridique plus bas que celui d'un pays disposant de règles plus faibles sur papier mais appliquées avec davantage de vigilance.

En outre, le rapport traite uniquement des documents relatifs aux clients ainsi que des autres données concernant les clients. Il ne concerne pas les métadonnées créées par le fournisseur de services à partir des données relatives aux clients qu'il stocke.

4. Analyse des juridictions

4.1. Introduction à la structure de l'analyse

La structure ordinaire générale de l'analyse d'une juridiction débute par une question concernant l'accès aux documents relatifs aux clients et détenus par un avocat lors d'enquêtes judiciaires effectuées dans le cabinet de l'avocat, y compris les possibilités de réaliser en secret des perquisitions et des saisies.

Vient ensuite une question au sujet des différences pouvant survenir dans l'éventualité où l'avocat conserverait des données relatives à ses clients ailleurs que dans son cabinet, suivie d'une autre sur les différences que présente un tel accès lorsque la perquisition se déroule selon des règles de sécurité nationale et aussi lorsqu'elle se déroule selon des procédures non pénales (si une telle perquisition s'avère possible en fonction de la branche du droit en question) y compris de droit administratif et de droit civil. Sont ensuite abordées les règles en matière d'interception des donnés des avocats qui ont été transmises (par téléphone, courriel ou via d'autres méthodes).

Le rapport aborde également les différences dans les cas où l'accès à un document est demandé au moyen du témoignage d'un tiers et, si de telles dispositions existent dans le droit national, au moyen d'enquêtes de données générales organisées par les forces de l'ordre sur des tiers en possession de données d'un avocat lorsque cette méthode n'est pas prévue par l'une des règles susmentionnées.

Le rapport présente les questions individuelles dans le même format pour chaque juridiction, avec une brève question en introduction, de sorte qu'elles soient aisées à comprendre. La recherche fournit tout d'abord des précisions aux questions elles-mêmes afin de mieux les comprendre :

Question brève	Précisions
Règles de droit pénal en matière de perquisition et de saisie des données relatives aux clients d'un avocat dans son cabinet	Quelles règles en matière de perquisition et de saisie s'appliquent aux cabinets d'avocats ? Y a-t-il des restrictions si l'avocat soumis à la perquisition agit en qualité d'avocat de la défense ? Des personnes extérieures à l'autorité chargée de l'enquête doivent-elles donner une *autorisation* préalable ? Si oui, quelles sont-elles ? (Par autorisation, nous entendons qu'elles ont le droit de refuser l'accès.) Un tribunal/un juge ? Un procureur ? Des personnes extérieures à l'autorité chargée de l'enquête doivent-elles être *notifiées* préalablement (les barreaux par exemple) ? Si oui, qui doit recevoir une notification ? Est-il possible de réaliser en secret une perquisition et une saisie dans le cabinet d'un avocat ?
Quelle différence y a-t-il si les données relatives aux clients sont conservées ailleurs que dans le cabinet de l'avocat ?	Si les avocats bénéficient d'une protection spéciale relative aux perquisitions et saisies effectuées à leurs cabinets, ces règles s'appliquent-elles également aux données que l'avocat a conservées ailleurs que dans son cabinet, notamment à l'aide d'un fournisseur de services informatiques (fournisseurs de services d'informatique en nuage par exemple) ? Les fournisseurs de services informatiques des avocats qui conservent des données relatives aux clients bénéficient-ils d'une protection spéciale identique à celle des avocats ?
Les règles en matière de perquisition sont-elles différentes en vertu d'un régime de sécurité nationale applicable ?	Les agences de sécurité nationale ont-elles la possibilité d'accéder aux données relatives aux clients ? Existe-t-il un régime juridique particulier ? À quel point est-ce détaillé comparé à la réglementation pénale ? Les avocats sont-ils protégés de la même manière qu'en droit pénal ?
Protection des avocats en matière de règles d'écoutes téléphoniques	Les règles applicables à l'interception de communications reconnaissent-elles le statut spécial des avocats et existe-t-il des mesures de protection particulières ? Les mêmes protections dont les avocats bénéficient en cas de perquisition et de saisie s'appliquent-elles dans le cadre de l'interception de communications ? L'autorité chargée de l'enquête doit-elle se conformer à un régime de protection spécial destiné aux avocats ou le fournisseur de services doit-il également s'en charger ?
Règles régissant l'accès aux données détenues par les fournisseurs de services au moyen d'un témoignage	Est-il possible de se soustraire aux règles et aux restrictions strictes (de droit pénal par exemple) en matière d'accès aux données relatives aux clients en demandant à un fournisseur de services informatiques de déposer en qualité de témoin ?
Accès à des données en fonction de demandes de données générales et d'autres réglementations non pénales	Veuillez vérifier si les garanties prévues par le droit pénal et détaillées ci-dessus peuvent être contournées ou non, notamment dans d'autres domaines du droit (le droit fiscal par exemple) ou en soumettant une demande officielle ou officieuse directement aux fournisseurs de services (en demandant leur aide dans le cadre d'une enquête).

4.2. Answers by each jurisdiction

Austria	
Short question	**Answer**
Criminal law rules on search and seizure of client data of lawyer at the lawyer's premises	As a rule prior permission is required from the Prosecutor General. The criminal investigation department may conduct a search and seizure without a prior warrant in urgent cases. There is a prior notification of the regional bar which the lawyer belongs to. Representatives of the bar (usually two commissioners of the bar) have to be present throughout the whole search and seizure. There is no legal basis for secret search and seizure at the lawyer's premises.
What is different if client data is stored outside the lawyer's premises?	If there are any third parties involved by the lawyer for data storage they may receive the same special protection that lawyers receive as described in the above answer. Especially the data has to be copied and sealed. The unsealing has to be supervised by the court. The data stored has to be identified as being subject to professional privilege. It is advisable to have some contractual obligation with the third party. It is mandatory by law that a lawyer being a customer of such a third party has to be notified by the investigating authority.
Are the search rules different under national security regime?	There are no exceptions regarding National Security.
Protection of lawyers in wiretapping rules	The interception rules are specific to criminal law due to the fact that the lawyer-client privilege in search and seizure cases applies only to the lawyer acting as a defence counsel.
Rules for access to data held by service providers by way of witness testimony	If third parties are prevented from disclosure/gathering of data according to any of the above rules, there is no possibility to circumvent that restriction by requesting their testimony as witness.
Access to data based on general data requests and other non-criminal law regulations	

Czech Republic	
Short question	**Answer**
Criminal law rules on search and seizure of client data of lawyer at the lawyer's premises	As a rule prior permission is required from the Court. There is a prior notification of the bar for search and seizure. Representatives of the bar have to be present.
What is different if client data is stored outside the lawyer's premises?	If there are any third parties involved by the lawyer for data storage they may receive the same special protection that lawyers receive as described in the above answer, however, according to the first answer to the Questionnaire, this question remains undecided.
Are the search rules different under national security regime?	There are exceptions regarding National Security (Security Information Service and Army Intelligence). The professional secrecy between lawyer and its client should however be respected.
Protection of lawyers in wiretapping rules	The interception rules are specific to criminal law due to the fact that the lawyer-client privilege in search and seizure cases applies only to the lawyer acting as a defence counsel.
Rules for access to data held by service providers by way of witness testimony	If third parties are prevented from disclosure/gathering of data according to any of the above rules, there is no possibility to circumvent that restriction by requesting their testimony as witness.
Access to data based on general data requests and other non-criminal law regulations	

Denmark	
Short question	**Answer**
Criminal law rules on search and seizure of client data of lawyer at the lawyer's premises	The authorities (i.e. the prosecution and the police) can seek access to lawyers' data based on suspicions regarding a particular client or the lawyer him/herself. This would require a court order. Communications between a criminal defence lawyer and his/her client remains in any case confidential. The conditions that need to be fulfilled by the police in order to conduct a search can be found in chapter 73 of the Administration of Justice Act (AJA). The rules governing seizure and disclosure can be found in chapter 74 of the AJA. If the lawyer isn't a suspect him/herself, searches of dwellings, other premises or objects (including documents) may only take place if the investigation concerns an offence which under the law can result in imprisonment and there are specific reasons to presume that evidence in the case or objects, which can be seized, can be found by the search. A prior Court order is required for a search and seizure. As a general rule the lawyer is informed about the search or seizure except when the lawyer him/herself is the suspect. The client is expected to be informed through the lawyer. The Danish law envisage the possibility to search data without a court order, if there is a risk the data will otherwise disappear – but it happens rarely and a court order with retroactive effect must be obtained immediately thereafter. In situations where it is deemed necessary that searches are conducted in secrecy, and then neither the lawyer nor the client is (naturally) informed immediately.
What is different if client data is stored outside the lawyer's premises?	As a general rule, possessions of persons, who are excluded from giving testimony as witnesses in the case (incl. lawyers), written messages and similar communication between the suspect and the lawyer, as well as notes, are not subject to search. The server and/or cloud is regarded an "extended office" of the lawyer, and the lawyer has the same obligations to ensure that data stored online/server/cloud is duly stored, as with data/case files kept physically at the lawyers' office. This is provided that the server is on Danish soil. As a consequence, cloud services providers can be required to disclose lawyers' data in the course of a Government investigation, provided that there is a prior court order. In addition, communications between criminal defence lawyers and their clients remain protected and cannot be disclosed. The lawyer shall be notified by the Cloud Services provider only if the disclosure of the relevant data can be considered as an interception.
Are the search rules different under national security regime?	
Protection of lawyers in wiretapping rules	
Rules for access to data held by service providers by way of witness testimony	
Access to data based on general data requests and other non-criminal law regulations	Cloud provider can disclose data voluntarily to the government in response to an informal request.

Germany	
Short question	**Answer**
Criminal law rules on search and seizure of client data of lawyer at the lawyer's premises	If criminal law investigations take place at the lawyer's premises §§ 94-110 StPO (Code of Criminal Procedure, Strafprozessordnung) shall apply. A prior permission is required, which is usually issued by the local court (Amtsgericht) that has jurisdiction in the court district where the lawyer's premises are located. As an exception to this rule, the Public Prosecutor and police may act without a judge's permission in exigent circumstances („Gefahr im Verzug") § 98 (1) StPO. If a seizure takes place without a court order, the permission has to be obtained within 3 days, if the lawyer concerned was not present during the seizure or objected to it. The lawyer concerned may at any time apply for a court decision. No, prior notification is not required. No third party required to be notified after the search and seizure. Secret search and seizure are not possible. Secret investigative measures such as telephone tapping are only possible where certain facts provide sufficient grounds for suspicion that the lawyer is involved in an offence or in aiding the perpetration of an offence, in the obstruction of justice or in the offence of receiving and handling stolen goods. Secret search and seizure are not possible. Secret investigative measures such as telephone tapping are only possible where certain facts provide sufficient grounds for suspicion that the lawyer is involved in an offence or in aiding the perpetration of an offence, in the obstruction of justice or in the offence of receiving and handling stolen goods. Telephone tapping requires a permission by the court. There is no prior notification of the lawyer concerned or of other persons. The lawyer concerned has to be notified following the end of the telephone tapping (§ 101 StPO).
What is different if client data is stored outside the lawyer's premises?	This is not permitted if the measures concern client data and the lawyer is not suspected of having committed the offence. No, since the protection is derived from the duty of confidentiality, the right to refuse to give evidence and the resulting exemption from confiscation. Notification of the lawyer or any other customer of the third party by the third party after having granted access results from § 101 StPO. If the notification constitutes an obstruction of justice, it is prohibited.
Are the search rules different under national security regime?	With a view to averting danger, covert police interventions at the federal level are permitted on the basis of § 20 BKA (Act governing the activities of the German Federal Police Office), for example. At Länder level, covert online searches by the police are in part authorized by the laws of the respective Land (e.g. in Bavaria, Art. 34 (d) of the Act on Police Functions, Polizei-aufgabengesetz). As far as intelligence-led access is concerned, such access is based on special legal foundations (e.g. § 8 (2) of the Act on the Protection of the Constitution, Bundes-verfassungsschutzgesetz).
Protection of lawyers in wiretapping rules	The Directive has not yet been implemented in Germany.
Rules for access to data held by service providers by way of witness testimony	No. If access to data is restricted, this restriction cannot be avoided by requesting the concerned third party, the protection of which is sought, for testimony as witness.
Access to data based on general data requests and other non-criminal law regulations	No. Pursuant to § 100 (g) StPO, telecommunications traffic data (traffic data stored for billing purposes) may be obtained also without the knowledge of the person concerned in accordance with § 96 TKG, (Telecommunications Act, Telekommunikationsgesetz) to the extent

	that this is necessary to establish the facts or determine the accused's whereabouts.

Finland	
Short question	**Answer**
Criminal law rules on search and seizure of client data of lawyer at the lawyer's premises	According to the Coercive Measures Act (806/2011) a special search of a domicile refers to a search of premises in which it can be assumed that the object of the search would reveal information in respect of which a person [referred to in the Code of Judicial Procedure Chapter 17, section 23, subsection 1 (presently under renewal)] may not testify in court proceedings; and in respect of which no confiscation or copying of a document may be directed. Such a person is for example a lawyer, who has attorney-client privilege. A lawyer, except the counsel of the defendant, may be ordered to testify in the case if the public prosecutor has brought a charge for an offence punishable by imprisonment for six years or more, or for an attempt of or participation in such an offence. A document may be confiscated under similar provisions. The provisions regarding a document apply also to a document that is in the form of data i.e. information that is contained in a technical device or in another corresponding information system or in its recording platform. A document may not be confiscated or copied to be used as evidence if it can be assumed to contain material on which a person may not testify in court proceedings and the document is in the possession of such person or in the possession of a person in whose benefit the obligation or the right to remain silent has been provided. Notwithstanding a document may be confiscated or copied if the person may be required to testify. A special search of premises may be conducted if there is reason to suspect that an offence has been committed and the most severe punishment provided for the offence is imprisonment for at least six months, or if the matter being investigated is circumstances connected to the imposition of a corporate fine, and it can be assumed that the search will uncover an object, property, document or information to be confiscated; a document that may be copied; property which may be confiscated for security; or a circumstance that may be of significance in the investigation of the offence. A search of premises may be conducted in a place that is not occupied by the suspect (for example the lawyer's office) only if the offence had been committed there or the suspect had been apprehended there or if otherwise it can be assumed on very justifiable grounds that an object, property, document, information or circumstance shall be found in the search. A search representative shall be appointed for a special search of a domicile in order to ensure that confiscation or copying is not directed at information under secrecy/seizure ban. Covert coercive means are not possible concerning a search of the premises. On the contrary the person in whose domicile the search is conducted or, in his or her absence, a person residing, working or otherwise authorised to be present there, shall be reserved an opportunity to be present during the search and to summon a witness. The decision on a special search of a domicile is made by the district

	court. An official with the power of arrest submits the request (the head of investigations or the prosecutor). The decision can be appealed. A search of data contained in a device refers to a search that is directed at the data contained at the time of the search in a computer, a terminal end device or in another corresponding technical device or information system. The decision on the conduct of a search of the premises may be extended to cover also a technical device or information system in said premises, if the search in question is not one intended to find a person. When a search of data contained in a device is conducted in connection with a search of the premises, the abovementioned provisions on search apply.
What is different if client data is stored outside the lawyer's premises?	There is no difference. The same provisions apply. The data of a defence counsel is privileged also on a cloud server.
Are the search rules different under national security regime?	There are no exceptions concerning national security.
Protection of lawyers in wiretapping rules	Telecommunications interception may be directed only at a message that originates from or is intended for a suspect in an offence. A criminal investigation authority may receive a permission from a court for telecommunications interception directed at a network address or terminal end device in the possession of or otherwise presumably used by a suspect in an offence, when there are grounds to suspect a person of a certain specific aggravated crime listed in the law. Telecommunications interception may not be directed at a message between the suspect and his or her defence counsel. If during the telecommunications interception it becomes evident that the message involved is one in respect of which on-site interception and observation is prohibited, the measure shall be interrupted and the recording made thereof as well as the notes made in respect thereof shall be destroyed immediately. The prohibitions of on-site interception and observation do not, however, apply to cases in which the person referred to is suspected in the same offence as the person suspected in the offence or of a directly connected offence, and also in respect of him or her a decision has been made on telecommunications interception, the obtaining of data other than through telecommunications interception, on-site interception or technical observation. Written notice shall be given without delay to the suspect concerning telecommunications interception directed at him or her, after the matter has been submitted to the consideration of the prosecutor or the criminal investigation has otherwise been terminated or interrupted. However, the suspect shall be informed at the latest within one year of the termination of the use of a coercive measure.
Rules for access to data held by service providers by way of witness testimony	If access to data is prohibited, it is not possible to circumvent this restriction by requesting the concerned third party to testify as a witness.
Access to data based on general data requests and other non-criminal law regulations	Under general data access request, no court order is needed to ask for disclosure of data from cloud provider. Also the head of investigation can request such data to be given voluntarily. Nevertheless the cloud provider should not give the data. In all instances, criminal or civil, professional secrecy should apply.

France	
Short question	**Answer**
Criminal law rules on search and seizure of client data of lawyer at the lawyer's premises	A search and seizure is granted by a court order describing suspicions related to the lawyer. It shall concern only information that is directly linked to the decision of seizure. Professional secrecy applies for the lawyers data. There is a prior notification of the Bâtonnier (President of the Bar where the lawyer is registered). The Bâtonnier (or a Bar representative) and the lawyer have to be present throughout the whole search and seizure. The lawyer can ask a counsel to be present. The Bâtonnier checks if the seized information is directly linked to the court order, and can ask that some information covered by professional secrecy cannot be used as evidence. A judge will decide if the court order covered this information and if it can be used as evidence.
What is different if client data is stored outside the lawyer's premises?	The seizure of data without the Bâtonnier being present would be a fraud of the lawyer's rights. The lawyer has to be notified as soon as possible. Article 226-13 of the french Criminal Code prohibits the disclosure of secret information by a person who is its depositary by status or profession, or because of a temporary function or mission. It is unclear if a cloud data service provider can be included in this definition, even if the law requires the person in charge of a computerized processing of personal data to ensure the confidentiality of the stored data.
Are the search rules different under national security regime?	Wiretapping can be granted under the responsability of the Prime Minister, especially in cases relating to terrorism, threats to national security or prevention of criminality and organized crime. The opportunity of the wiretapping is controlled by an independent commission. In cases relating to the prevention of terrorism, professional secrecy does not apply but lawyers have to give their consent to the data seizure.
Protection of lawyers in wiretapping rules	Specific rules apply to wiretapping in the lawyer's premises. Communications of the lawyer can be monitored only if there are suspicions of his/her involvement in an offense. A judge that autorizes, because there is evidence of involvement of the lawyer in an offense, the tapping of the law firm must inform the Bâtonnier and ensure that professional secrecy is protected and this tapping will not compromise the professional activity of the lawyer. Similar rules should be applied to protect the data stored at a cloud data service provider.
Rules for access to data held by service providers by way of witness testimony	Professional secrecy prohibits any person to share any information which is covered by it.
Access to data based on general data requests and other non-criminal law regulations	Professional secrecy applies in every regulations. In tax matters, each visit must be granted by a judge. The presence of the Bâtonnier or his representative is not required by law but it is customary. A police officer monitors compliance with professional secrecy and the rights of the defense. The court order granting the seizure can be contested. The data of the lawyers' files can only be disclosed to authorized persons because of their functions. Specific rules and professional secrecy must apply. The Commission nationale de l'informatique et des libertés can carry out a review of a data processing provider, by decision of its President. The decision shall be notified to the person responsible of

	the places where the reviewed data processing are located. The prosecutor is also informed of the date, time and purpose of the review before it takes place. If the review concerns a client of a lawyer, the latter may be present during the inspection. Professional secrecy may be opposed to the CNIL during the review, it is then reflected in the minutes.

Hungary	
Short question	**Answer**
Criminal law rules on search and seizure of client data of lawyer at the lawyer's premises	Only a court may order a search in a lawyer's office if the search is directed to client data. Presence of the public prosecutor is required during the search. A court order is also needed to seize documents containing client data found during such searches. No written communication between a criminal defence lawyer and the accused may be seized. No memos of the defence lawyer for a given case may be seized. (Even with the client's approval.) Unless the client has given his approval to do so (i.e. releases the lawyer from his duty) or the client is obliged by law to give such an approval, no client documents may be seized from the lawyer if they are at the official premises of the lawyer. No such restriction applies if the lawyer is an accomplice or the document is an instrument of a crime. No prior or following notification is needed (only simultaneous). There is a possibility for secret search and seizure (in connection with more serious crimes). The lawyer has to be informed of the search/seizure following it has been carried out if that is not a risk to the success of the criminal procedure. A separate court decision is needed with stricter procedural rules than for simple search and seizure, a special agency carries out the search and seizure, and the seized original document will be handled as classified information, and appear in the criminal procedure only in the form of a report. Defence lawyer protection applies the same way.
What is different if client data is stored outside the lawyer's premises?	The defence lawyer protection applies regardless of the person of the third party. Otherwise, no such protection will practically apply. As long as client data is kept at a third party who carries out a profession "due to which profession they are required to keep a secret" (a term difficult to translate, we could call it "professional secrecy"), the protection related to seizure might apply, but such professionals do not currently include e.g. cloud data service providers (this covers priests, medical professionals, public notaries etc.) Communications addressed to any person (including a lawyer) and not yet delivered may only be seized by order of the public prosecutor (or the court). "no written communication between a criminal defence lawyer and the accused may be seized" & "no memos of the defence lawyer for a given case may be seized." So e.g. no court order is required. It is not mandatory by law to notify the lawyer of such access before or after granting access to an authority.
Are the search rules different under national security regime?	Although it is not called search and seizure, the specific national security service agency may carry out a search in secret, with the approval of either a criminal court judge or the minister of justice (the highest level of the administrative branch dealing with justice matters), depending on the national security task involved. There is no special protection of any kind regarding client documents of lawyers.
Protection of lawyers in wiretapping rules	Such interception is only allowed under criminal procedure law, under national security rules, and under special powers of criminal investigative bodies e.g. police (regardless of whether a criminal procedure has been formally started). Under criminal law and other police powers, interception of

	communications forwarded by electronic communication service providers or data forwarded by computers requires prior approval from a judge. This can only be used for more serious crimes. No such interception may be carried out in the home or office of a lawyer acting in the given criminal procedure as a defence lawyer, including wiretapping any phone in possession of the lawyer, searching any computers in possession of the lawyer. The only exception is that the lawyer himself is under criminal investigation in relation to the ongoing criminal procedure. Under national security rules, the legal rules are the same as written above. The electronic communications service provider and similar third parties never prefilter communications on the basis of protection set out above, it is always the police (the public prosecutor, the national security service) that has to comply with the rules of special protection. (The same technical means are used for recording all communications.)
Rules for access to data held by service providers by way of witness testimony	Lawyers may not testify unless the client has given his approval to do so about the client data (i.e. releases the lawyer from his duty) or the client is obliged by law to give such an approval. Similar protection is granted to all those acting under obligations of professional secrecy, which does not protect IT and telecom providers merely handling business secrets. There is no possibility for witness testimony by defence lawyer regarding their criminal law clients.
Access to data based on general data requests and other non-criminal law regulations	There are generic rules for seizure under administrative law. There are certain procedures under administrative law that may be used partly for the same purpose as the search under criminal procedure ("inspection"). No documents containing client data may be seized from lawyers. Third parties may also claim such protection by claiming that the data they are in possession is "business secret" of a third person. Under generic rules of inspection, a lawyer may be required to a) let the authority in to a location which contains client data, or b) to show the object of inspection to the authority (there is no specific protection for neither lawyer data, nor business secret here). This includes provision of access to an IT system. However, above rules on seizure will effectively prohibit the authority from taking the documents, but this will not necessarily prohibit the authority from recording electronic data (which may not be considered to be seizure). Outside the generic rules of administrative law, there are numerous specific rules of administrative law. E.g. under tax law, there is a specific protection requiring prior approval of the public prosecutor prior to searching the office of lawyers (and tax consultants, accountants, auditors.) This latter protection does not apply to other third party service provider or to client data outside the office of a lawyer. There is a possibility for the police (either during a criminal procedure in progress or under special secret investigatory powers) to request data by way of such "data requests" (outside search and seizure procedures) from telecommunications service providers and any handlers of business secrets. These data requests do not cover data forwarded by electronic communications services or computers or stored by computers (that is, content data – such data is protected by a stricter regime, see 4. above). They may not request any information on this basis from lawyers. There is similar possibility under administrative law, but unlike under criminal law, business data is also protected from having to disclose (unless a specific act on a given branch of administration provides otherwise for certain type of data).

Ireland

Short question	Answer
Criminal law rules on search and seizure of client data of lawyer at the lawyer's premises	There are no specific rules relating to search and seizure in law offices. Generally, the police have authority to search a premises under warrant issued by the courts and in certain circumstances they have power to search without warrant. Certain other bodies, notably the Revenue Commissioners, have powers of search and seizure. Material that is subject to legal professional privilege would be protected from search and seizure and even if seized could not be used in evidence. Generally a warrant would be issued by the courts under a statutory provision but in certain circumstances the police have powers of search and seizure without a warrant. No prior notification would have to be given to any person such as a bar association. A secret search and seizure - without notice and without warrant or consent would be illegal.
What is different if client data is stored outside the lawyer's premises?	In relation to a lawyer's client data stored externally, the position would be the same as in 1 above.
Are the search rules different under any applicable national security regime?	A number of national security measures provide for particular search and seizure mechanisms in respect of anti-terrorism activity and prevention of serious criminal offences. These are subject to the issue of a warrant by the Courts or by a senior police officer.
Protection of lawyers in wiretapping rules	There are no specific protections for lawyers in respect of 'wiretapping' or surveillance measures. However, legal professional privilege could apply to intercepted material or data.
Rules for access to data held by service providers by way of witness testimony	Evidential rules would not allow for the replacement of data or material as evidence with witness testimony
Access to data based on general data requests and other non-criminal law regulations	If access to data is not available under criminal procedures, it is unlikely that it could otherwise be obtained without consent whether through data requests or non-criminal law regulations. In all instances, criminal and civil, legal professional privilege would apply.

Italy	
Short question	**Answer**
Criminal law rules on search and seizure of client data of lawyer at the lawyer's premises	In general: Art. 247 and following of Code of Criminal Procedure: Article 247. Cases and forms of searches. 1. When there is reason to believe that anybody concealed on the person's body or a crime relating to the offense, is arrange body search. When there is reason to believe that these things are in a certain place or that it can be performed in the arrest of the accused or of the convict, is arrange local search. 1-bis. When there is reason to believe that the data, information, computer programs or tracks, however, relevant to the offense are in a computer system or computer, even if protected by security measures, nor will the search, by adopting technical measures aimed at ensuring the conservation of the original data and to prevent tampering. 2. The search is prepared by reasoned decree. 3. The court may proceed in person or provide that the act is committed by police officers delegated with the same decree. The following articles concern way of searches and seizures.

	In particular: Art. 103 of Code of Criminal Procedure: Article 103: guarantees of freedom for the defence attorney 1. The inspections and searches in the offices of the defence attorneys are allowed only: a) when they or others who are in a stable activity in the same office are recognized for the limited purpose of establishing the offense attributed to them; b) to detect traces or other material effects of the crime or to search for people or things specifically predetermined. 2. At the defence attorneys and private investigators in relation to the proceedings, as well as at the technical advisers cannot proceed to the seizure of papers or documents relating to the object of the defence, unless they constitute the body of the crime. 3. As you prepare to perform an inspection, a search or seizure in the office of a lawyer, the court, on pain of nullity informs the council of the Bar of the place because the president or a counselor from him delegated can be present during. Similarly, if you intervene and request it, is given a copy of the measure. 4. Inspections, searches and seizures at the offices of defence attorneys shall be done personally by the Judge, or in the course of the preliminary investigation the prosecutor, on the basis of reasoned consent decree of the court. 5. It is not permitted to intercept conversations or communications relating to the defence attorneys, the private investigators in relation to the proceedings, technical advisers and their assistants, or those between them and the people they assisted. 6. It is prohibited any form of seizure and control of the correspondence between the accused and the defence counsel as prescribed by the recognizable signs, unless the court has reason to believe that this is the body of the crime. 7. Except as provided in paragraph 3 and Article 271, the results of the inspections, searches, seizures and interceptions of conversations or communications, carried out in breach of the foregoing provisions, cannot be used. Confidentiality between lawyer and client do not permit access from any person outside the investigating authority. Prior notification of the President of the Bar in which the lawyer is registered in cases under art. 103 of procedural criminal code. There is no possibility for secret search and seizure at the lawyer's premises.
What is different if client data is stored outside the lawyer’s premises?	The „strong duty” is reserved for search in the premises of the lawyer, but in case of seizure all spaces referred to lawyer in theory are covered by privilege. It is difficult before S&S distinguish between data owned by common people and data referred to a client-attorney partnership and there is no way to force a provider to separate attorney data from other of common people. Usually the communication is at the same time of the access for people that are present, but in absentia of them as soon as possible (if it is outside the lawyer office). There is no legal requirements that prohibit the third party from notification of its customers on
Are the search rules different under national security regime?	All data and communication between lawyer and customer are covered by legal privilege. If a lawyer or a customer is involved in a crime, search and seizure are possible, but when data or documents are to search at the lawyer's premises, it is necessary to respect guarantees of freedom under art. 103 Code of Criminal Procedure

	(see first answer).
Protection of lawyers in wiretapping rules	Interception are provided only in criminal law and they are regulated under articles 247 and following of Code of Criminal Procedure (art. 103 guarantees of freedom for the defence attorney) (see first answer). There is not a special obligation for electronic communication service provider/network provider (except in comply with data protection regulation). The investigation authority must respect the law.
Rules for access to data held by service providers by way of witness testimony	Third parties may be witness and refer to fact or speech, but only when they are not covered by secret (lawyers, investigators, advisors, etc.)
Access to data based on general data requests and other non-criminal law regulations	All data and communication between lawyer and customer are covered by legal privilege, but tax authority can access to tax documents (also of the Client) if they are recovered at the lawyer. "Soft" inspection of investigators is possible (art. 246 Code of Criminal Procedure) and the lawyer that represents clients in criminal proceedings can carry out defensive investigations.

Slovak Republic	
Short question	**Answer**
Criminal law rules on search and seizure of client data of lawyer at the lawyer's premises	For the purposes of a Criminal investigation, any person holding data may be required, by Court Order, to (a) store and (b) hand over data. An order from the Court or the Prosecutor is required. There are no special rules regarding lawyer's offices. No prior notification is given. Data falling under the criminal defence counsel relationship with the client is protected, and, if recovered, cannot be used and must be destroyed. In civil and administrative proceedings a prior warrant issued by a judge or the administrative body concerned requires to be obtained
What is different if client data is stored outside the lawyer's premises?	The rules are the same.
Are the search rules different under national security regime?	In exceptional circumstances, *the Constitutional Act on the security of the state in time of war, warfare, exceptional or state of emergency* provides the possibility of limiting the privacy of letters and secrecy of mailed messages.
Protection of lawyers in wiretapping rules	The general regime allows for wiretapping in the case of certain specified serious crimes. A warrant requires to be obtained from a judge or prosecutor (subject to confirmation by a judge). There are no special rules relating to lawyers, though privileged data is protected by defence counsel privilege. If the data is recovered from a service provider (not a lawyer) the data requires to be handed over.
Rules for access to data held by service providers by way of witness testimony	Professional secrecy applies.
Access to data based on general data requests and other non-criminal law regulations	Professional secrecy applies.

Slovenia	
Short question	**Answer**
Criminal law rules on search and seizure of client data of lawyer at the lawyer's premises	Only by an ordinance from the court and only for the records and objects stated therein. A bar representative has to be present.
What is different if client data is stored outside the lawyer's premises?	The protection of data under search and seizure rules would be the same as for data stored at the lawyer's office. [This is just my deduction from their answer to their answer number A8 to the second

	questionnaire, this should be confirmed! ["A8 Would the answer to any of the foregoing questions differ depending on whether the data is stored in a lawyers' office or with an IT Service Provider?"] If third parties involved by the lawyer do not receive special protection or that protection is materially different from that of a lawyer.
Are the search rules different under national security regime?	No.
Protection of lawyers in wiretapping rules	Criminal law governs this. Upon the request of the public prosecutor, an investigating judge may order the operator to provide the judge with metadata about the communications, or to monitor the communication itself. Wiretapping can be ordered only if that the person involved has committed serious crime and that the communication is in connection with the crime (or be used for committing it), and other means can be expected not to be sufficient or such other measures would risk life/health of people. The rules are not lawyer specific.
Rules for access to data held by service providers by way of witness testimony	Under Criminal Law rules.
Access to data based on general data requests and other non-criminal law regulations	No.

Spain	
Short question	**Answer**
Criminal law rules on search and seizure of client data of lawyer at the lawyer's premises	Legal basis: Title VIII of Criminal Procedure Law – Ley de Enjuciamiento Criminal Prior permission from a judicial authority is required in criminal investigations. If the access sought is to a lawyer's data as the subject of the investigation, the provider shall provide those data given that the conditions stated above are met. If the access is to data of the lawyer's client, then the lawyer's code of professional secrecy does apply. The local Bar where the lawyer sits may be notified by the judicial power competent for the register in a lawyer's office. In this situation the President of the Local Bar or a person replacing him should appears in person in the lawyer's premises in order to safeguard legal professional privilege. There is no legal basis for secret search and seizure at lawyers' premises in criminal investigations.
What is different if client data is stored outside the lawyer's premises?	Lawyers' providers may only disclose the lawyers' data if guarantees and conditions of art 579 of the Criminal Procedure Law are met (reasoned judicial authorization). Otherwise, such access would infringe fundamental rights and therefore would be illicit or illegal. Allowing access to lawyers' data through a service provider without the required guarantees would mean circumventing constitutional (art 18.3 and 24.2 Spanish Constitution) and legal protections such as the secrecy of communications, legal guarantees and the right and duty of professionals (Organic Law of the Judiciary Power and General By-Law of the Spanish Lawyers). If the request involves personal data in cases according to article 22(2) of Organic Law 15/1999, considering that such communication of personal data to the law enforcement authority fulfils the requirements provided in such article or there is a judicial request, notification to the lawyer would not be needed, but only if lawyer himself is subject to the investigation. In other cases or specific circumstances, the cloud provider might have to maintain secrecy in

	order to avoid interfering with a criminal investigation if this is referred to the lawyer.
Are the search rules different under national security regime?	With regard to National Security Agency investigations, Organic Law 2/2002 regulates the terms and conditions under which the National Intelligence Agency may intercept communications. Any interception of communications, as this affects a fundamental right, would require the authorization of the designated Magistrate of the Supreme Court (which corresponds to a Higher Judge in Spain).
Protection of lawyers in wiretapping rules	Directive 200/24/EC has been transposed into national law by Law 25/2007. In the context of criminal investigation, access to retained data requires prior permission from a judicial authority. Profesional secrecy is protected by the Spanish Contititution (art. 24.2) and the Organic Law of Judicial Power (art. 542.3).
Rules for access to data held by service providers by way of witness testimony	
Access to data based on general data requests and other non-criminal law regulations	A law enforcement investigation for administrative purposes may differ from a criminal investigation. The key point is that access without consent for police purposes is only possible when the data are needed to prevent a genuine threat to public safety or for the suppression of crime, and the Spanish Data Protection Authority has provided a narrow interpretation of such cases. The investigation must relate to a concrete and/or real threat, not a potential or possible one (article 22(1 and 2) of the Organic Law 15/1999). Therefore, in the context of a police investigation, in principle, the data subject´s consent is not required, but what is required is a real threat to public safety or the likelihood of suppressing crime. Police investigations (law enforcement request for administrative purposes): Article 22 of the Organic Law 15/1999 on Data Protection applies. In police investigations, authorization by judicial order is not required if the access is to a lawyer's data exclusively, not to clients' data, and additionally: 1. It is in the context of an investigation where the subject of this investigation is the lawyer itself and 2. there is a real threat to public safety or it is likely that accessing the data will support suppression of crime. These cases have been narrowly interpreted by the Spanish Data Protection Agency (DPA).

Sweden	
Short question	**Answer**
Criminal law rules on search and seizure of client data of lawyer at the lawyer's premises	Prosecuting authorities and the police can seek access, either because of suspicions related to a certain client or suspicions related to the lawyer him/herself. Access can only be granted by a court under very special circumstances and it shall only concern information which is directly linked to the decision of seizure (i.e. directly connected with the suspicions). Surplus information may not be accessed and cannot be used as evidence. In principle the access is subject to a prior court order (decision for seizure and sometimes for research of premises) authorising access to certain documents. According to the Swedish rules the lawyer shall be informed before except in the very rare situation where the lawyer him/herself is suspected of a crime.
What is different if client data is stored outside the lawyer's premises?	According to the Swedish rules the information still belongs to the lawyer, therefore it is still confidential, even if it is stored with an external IT provider. The lawyer/law firm considered to be the owner of the data stored at

	an (external) IT service provider. As a consequence, any „external" request for disclosure shall be forwarded to the advocate who is responsible for the mandate in which the information is stored.
Are the search rules different under national security regime?	
Protection of lawyers in wiretapping rules	
Rules for access to data held by service providers by way of witness testimony	
Access to data based on general data requests and other non-criminal law regulations	

United Kingdom of Great Britain and Northern Ireland	
Short question	**Answer**
Criminal law rules on search and seizure of client data of lawyer at the lawyer's premises	There are three separate jurisdictions in the United Kingdom, and the precise rules differ as amongst the jurisdictions. (on the whole the rules are largely statutory in England & Wales and Northern Ireland and lean more heavily on common law in Scotland). Broadly speaking, in all three jurisdictions, the police require a warrant obtained from a judge to authorise the search of any premises and seizure of evidence, including data. Under part 3 of the Regulation of Investigatory Powers Act 2000, the police can demand the decryption of encrypted material. In exceptional cases (such as hot pursuit) evidence may be recovered without a warrant. Police powers do not extend to the seizure of evidence protected by legal professional privilege, nor can a warrant authorise such seizure. This applies to all documents and other evidence and (apart from the power to request decryption), there are no special rules relating to data in electronic form. The rules are of general application and (apart from the protection afforded to legal professional privilege) there is no special regime for lawyers.
What is different if client data is stored outside the lawyer's premises?	The same rules apply, and evidence covered by legal professional privilege remains protected.
Are the search rules different under national security regime?	Yes. Surveillance is governed by the Regulation of Investigatory Powers Act 2000 supplemented in Scotland by the Regulation of Investigatory Powers (Scotland) Act 2000, which governs investigations by the security services, police and certain other agencies, and which (amongst other matters) requires those authorities to obtain from a senior government minister a warrant authorising interception of private communications carried over a "public telecommunications system" which may include Cloud computing services and certainly includes the transmission of data to, from or between the storage and processing systems operated by Cloud service providers. The warrant is obtained from a minister, not a judge. Separately, the Intelligence Services Act 1994 provides the security and intelligence services with power to obtain a Government warrant authorising an interference with property or with wireless telegraphy. It is possible that these powers could be used to obtain access to data stored or processed in the Cloud. Where data have been accessed under RIPA or the Intelligence Services Act, a subsequent review may be undertaken by a specialist tribunal, the Investigatory Powers Tribunal ("IPT"). The IPT includes members of the senior judiciary but conducts its investigation into the facts in secret. Because the authorities do not give notice of the exercise of their powers, even after the event, the right to complain is of very limited value.

Protection of lawyers in wiretapping rules	Under the RIPA regime, and the ISA, there is no exception for communications to or from lawyers, even where those communications are, or are reasonably believed to be, privileged. However, the Interception Code of Practice issued under RIPA advises that "consideration should be given to any infringement of the privacy of individuals who are not the subject of the intended interception, especially where communications relating to religious, medical, journalistic or legally privileged material may be involved." This has no legal force, and does not of itself prevent the interception of material subject to legal professional privilege. That said, the process of granting warrants is overseen by the Interception Commissioner (a High Court judge) who sets a very high bar, rendering extremely unlikely that there would be interception of legally privileged material. A further opportunity for protection would arise in any subsequent court proceedings where the prosecution might seek to lead evidence of legally privileged information which had been recovered under a RIPA warrant. This could be objected to under the general rules of evidence, (in England & Wales and Northern Ireland under the Police and Criminal Evidence Act 1984, or, in Scotland, under common law).
Rules for access to data held by service providers by way of witness testimony	The rules discussed above relate to documentary evidence (whether or not in the form of electronic data). There is no power to compel anyone to give parole evidence of the content of documents which have not been (or could not be) lawfully recovered, and if the documents have been lawfully recovered, parole evidence as to their contents would not be permitted as it would be the documents themselves which would constitute the best evidence. A lawyer could not voluntarily give parole evidence relating to matters protected by legal professional privilege unless the client specifically waived that privilege.
Access to data based on general data requests and other non-criminal law regulations	Recovery of evidence under civil law (which includes matters falling under what in continental jurisdictions might be classed as administrative law) are subject to controls by the Court. The precise rules differ amongst the three jurisdictions, but, in general, the recovery of, or the leading of evidence protected by legal professional privilege (including lawyers' data discussed in this Report) is not permitted. However, a distinction lies between what may be compelled and what might be done voluntarily. There is no specific legislative provision expressly forbidding such disclosure. The subject of the lawyer's data (typically, the client, though the lawyer could also fall into this category) benefits from national implementation of the EU data protection regime in the ordinary way, but this is considered to provide limited protection, particularly where the request is made for law enforcement purposes falling within the DP Framework Decision rather than the DP Directive. In relation to communications data retained by a provider pursuant to Directive 2006/24/EC, the agency concerned would normally be expected to obtain an authorisation under RIPA

5. Conclusions communes de l'analyse nationale

5.1. Tableau récapitulatif des réponses

L'objectif de ce tableau est d'offrir un aperçu des similitudes et des différences principales. Il ne vise nullement à examiner la question en détails ni à traiter des cas spéciaux tels que la récupération de données lors de « situations d'urgence » ou lorsqu'un mandat judiciaire doit être obtenu seulement après la perquisition en cas d'urgence et d'autres aspects semblables.

	Exceptions en matière de perquisition et de saisie pour l'avocat de la défense	Garanties en matière de perquisition et de saisie qui s'appliquent aux données des avocats relatives à leurs clients en général	Participation du barreau en matière de perquisition et de saisie	Interception de communications (écoutes téléphoniques), à l'exception des métadonnées	Protection des données relatives aux clients conservées en dehors du cabinet ? (dans le nuage par exemple)	Règles de sécurité nationale régissant l'accès aux données	Accès aux données relatives aux clients au moyen d'un témoignage	Contournement des mesures de protection par le biais de demandes génériques de données ?
Allemagne		Autorisation judiciaire préalable. Les données relatives aux clients sont insaisissables.	Non.	Uniquement dans des cas très limités. Notification à l'avocat *a posteriori*.	Protection identique à celle des données conservées dans le cabinet.	C'est légal. Elles sont réglementées mais de manière générale. Pas de protection particulière pour les avocats prévue par la législation.	Non. Protection identique.	Non.
Autriche	Oui. [protection particulière dans ce cas-ci ? Identique à ce qui est indiqué ci-dessus ?]	Autorisation préalable du procureur général.	Notification préalable au barreau et présence de deux représentants du barreau autorisée.		Peuvent bénéficier d'une protection identique. Les informations doivent être identifiées	Pas de règles spéciales en matière d'accès en vertu de la sécurité nationale		Non.

					comme étant des données relatives aux clients. L'autorité notifie le client *a posteriori*.			
Danemark	Oui. La communication avec le client est exemptée.	Autorisation judiciaire préalable. La perquisition peut ne pas concerner les informations qui seraient exemptées d'un témoignage.	Non.	Uniquement pour les infractions graves. L'avocat doit en être notifié après l'interception.	Oui si le serveur est localisé au Danemark. Perquisition possible grâce à une décision judiciaire préalable.			Risques de demandes officieuses.
Espagne		Autorisation préalable d'une autorité judiciaire requise.	Notification préalable au barreau local auquel l'avocat est inscrit. Présence requise d'un représentant du barreau afin de garantir le secret professionnel.	L'accès aux données conservées nécessite une autorisation préalable de la part d'une autorité judiciaire.	Protection identique. Nécessité de respecter les garanties et les conditions prévues à l'article 579 du code de procédure pénale (c.-à-d. autorisation judiciaire motivée préalable).	L'agence nationale de renseignements peut intercepter les communications. L'interception nécessite une autorisation du magistrat désigné de la Cour suprême.		L'accès sans consentement à des fins policières n'est possible que lorsqu'il s'avère nécessaire afin d'empêcher une véritable menace pour la sécurité publique ou de réprimer une infraction. L'Autorité espagnole de protection des données donne une interprétation très étroite de ces conditions.

Finlande		(Par le responsable de l'autorité uniquement)		Notification *a posteriori*.	Identique à la protection des données conservées dans le cabinet.			Dans le cas des demandes génériques de données, aucune décision judiciaire n'est nécessaire pour demander la divulgation de données de la part du fournisseur de services d'informatique en nuage. La personne responsable de l'enquête peut demander ce type de données.
France	Seules les informations qui font l'objet de la décision judiciaire peuvent être utilisées comme éléments de preuve. Les autres informations sont protégées par le secret professionnel.	Autorisation judiciaire préalable. Les données relatives aux clients qui ne font pas l'objet de la décision judiciaire sont insaisissables.	Notification préalable et présence du bâtonnier et de l'avocat.	Décision judiciaire et notification préalables au bâtonnier.	Une protection identique peut être appliquée mais c'est incertain.	Légales et réglementées.	Protection identique, le secret professionnel s'applique.	Le secret professionnel s'applique.
Hongrie	Oui, aucune note de l'avocat de la défense dans	Autorisation judiciaire préalable (spécifique à	Non.	Uniquement pour les infractions graves. Les	Seule la protection destinée à l'avocat de	C'est légal. Elles sont réglementées mais de	Les fournisseurs d'informatique en nuage	Oui, se référer au stockage de données dans le nuage.

	l'affaire ni aucune communication entre l'avocat de la défense et l'accusé ne peut être saisie.	l'avocat). Présence requise du procureur général. Les documents relatifs aux clients sont insaisissables s'ils sont conservés dans le cabinet de l'avocat à moins qu'il s'agisse de documents qui aient servi à commettre une infraction.		communications adressées à quiconque qui ne sont pas encore transmises ne peuvent être saisies que sur ordre du procureur général ou de la cour. Protection spéciales destinées à l'avocat de la défense.	la défense s'applique, pas les données générales relatives aux clients. Pas de protection spéciale prévue par la loi, parfois utilisée par la police afin de se soustraire à une exemption spécifique destinée aux avocats.	manière moins détaillée que dans le droit pénal. Pas de protection spéciale prévue pour les avocats.	peuvent témoigner dans des enquêtes pénales.	
Irlande	Non, pas de règles spécifiques en matière de perquisition et de saisie dans les cabinets d'avocats.	Les documents qui relèvent du secret professionnel sont protégés contre la perquisition et la saisie. S'ils sont tout de même saisis, ils ne peuvent pas être utilisés en tant qu'éléments de preuve. Tout accès aux données d'un avocat nécessite l'autorisation de l'avocat et/ou	Non.	Aucune protection particulière n'est en place pour les avocats en matière « d'écoutes téléphoniques » ou de mesures de surveillance. Le secret professionnel pourrait néanmoins s'appliquer aux données ou aux documents interceptés.	La doctrine relative au secret professionnel est primordiale dans le droit irlandais et limite considérablement l'accès du gouvernement aux données des avocats.	Sont soumises à l'émission d'un mandat par la cour ou par un haut fonctionnaire de la police.	Les règles de preuve n'autorisent pas le remplacement de données ou de documents en tant qu'éléments de preuve par un témoignage.	Non.

		de son client en l'absence d'obligations d'accès légal très restreintes ou d'une décision judiciaire.						
Italie	Oui, aucune note de l'avocat de la défense dans l'affaire ne peut être saisie, à moins qu'il s'agisse d'éléments de preuve d'une infraction.	Une autorisation judiciaire préalable est requise. Le procureur ou le juge doit mener la perquisition et la saisie.	Notification préalable au barreau et présence d'un représentant du barreau.	Possible uniquement au pénal. Notification à l'avocat *a posteriori*.	La protection est incertaine mais pourrait s'appliquer en théorie (les conseillers techniques des avocats bénéficient également d'une protection). Problèmes techniques concernant l'identification des données de l'avocat relatives à ses clients.	Une protection identique s'applique.	Non. Protection identique.	Les autorités fiscales peuvent avoir accès aux documents fiscaux du client si l'avocat les détient.
République slovaque	Oui.	Le secret professionnel s'applique.	Non.	Uniquement pour les infractions graves. Pas d'obligation d'informer qui que ce soit. Protection particulière pour les données	Identique à la colonne précédente.	Pas de règles spéciales ; il existe néanmoins des pouvoirs spécifiques pour les cas d'urgence	Le témoignage ne peut pas être utilisé pour contourner les protections.	Non.

				confidentielles relatives aux clients.		qui annulent le droit au respect de la vie privée en temps de guerre et d'urgence nationale.		
République tchèque	Oui.	Autorisation judiciaire préalable.	Notification préalable au barreau et aux représentants du barreau pour qu'ils assistent à la perquisition.		La protection est incertaine mais est en théorie applicable.	C'est légal. Elles sont réglementées et certaines exceptions peuvent être applicables par rapport à la réglementation générale.	Non. Protection identique. Le secret professionnel s'applique.	Non. Le secret profession s'applique.
Royaume-Uni	Les éléments de preuve protégés par le secret professionnel ne peuvent généralement pas être restitués ou, si c'est le cas, ne peuvent pas être utilisés comme moyens de preuve.	Un mandat préalablement délivré par un juge est habituellement requis.	Non.	Aucune notification.	Protection identique à celle des données conservées dans le cabinet, sauf que s'il s'agit de données hébergées dans le nuage, il est peu probable qu'elles soient soumises aux règles normales de preuve en matière pénale mais	Règles de la loi RIPA et de l'institution ISA. Mandat administratif mais pas judiciaire, pas de notification, pas de protection juridique expresse pour les données des avocats protégées par le secret professionne	Normalement pas possible.	Possible.

					bien au régime de la loi RIPA (voir colonne suivante).	l, à part une certaine protection en vertu du code de déontologie. L'usage du contrôle de l'*Investigatory Powers Tribunal* (IPT) est limité étant donné que le tribunal est secret et une personne/un avocat concerné peut ignorer (en raison d'une absence de notification) que ses données confidentielles ont été consultées et qu'il peut éventuellement porter plainte.		
Slovénie	En vertu du secret professionnel.	Décision judiciaire préalable requise.	Notification préalable et un représentant du barreau doit assister à la perquisition.	Uniquement pour les infractions graves. Les autres moyens seront sans doute insuffisants.	Protection identique à celle des données conservées dans le cabinet.	Une protection identique s'applique.	En vertu des règles en matière de droit pénal.	Risques de demandes informelles.

Suède		Décision judiciaire préalable requise (pour par ailleurs pour des motifs restreints). Notification préalable à l'avocat requise à moins que ce dernier ne soit la personne soupçonnée.			Protection identique à celle des données conservées dans le cabinet. Les demandes de données externes doivent être transmises à l'avocat (client du fournisseur de services).			

5.2. Aperçu des similitudes, des différences, des insuffisances et des sujets de préoccupation

5.2.1. Il existe de fortes similitudes manifestes quant à la manière dont les juridictions nationales tiennent compte du secret professionnel dans leurs régimes de réglementation. L'analyse du CCBE semble indiquer que les différences entre les États membres (qui se marquent dans leur droit matériel) ne se sont pas considérablement accrues si l'on se réfère aux résultats du rapport Edward. Ce bilan semble plutôt rassurant si l'on considère que la portée internationale de l'Union européenne est aujourd'hui bien plus large et que l'UE dispose d'une plus grande diversité culturelle.

5.2.2. La majorité des pays reconnaît la valeur universelle de la protection des données détenues par les avocats. Certaines juridictions la considèrent néanmoins comme un privilège accordé à l'avocat de la défense. Ces pays prévoient également des règles générales destinées aux avocats qui n'exercent pas en qualité d'avocats de la défense. Ces règles se fondent sur le droit au respect de la vie privée. Par ailleurs, la plupart des pays prévoient une protection juridique particulière pour les secrets professionnels de manière plus large qui sert également à protéger les avocats n'exerçant pas en tant qu'avocats de la défense.

D'autres juridictions possèdent comme point de départ conceptuel un principe général de secret professionnel qui s'applique à l'ensemble des communications relatives aux conseils juridiques d'un avocat envers son client. Les conseils donnés dans le cadre de la défense au pénal ou, par exemple, les conseils relatifs à une fusion d'entreprises sont alors considérés comme des cas particuliers de ce principe général.

Quel que soit le point de départ conceptuel, la protection s'étend toutefois au droit de refuser (en l'absence de l'accord du client) de rendre un témoignage sur des affaires que le principe protège. Les avocats bénéficient d'une telle protection notamment en Allemagne, au Danemark, en Espagne, en Hongrie, en Italie et dans les diverses juridictions du Royaume-Uni. Cette protection s'applique également lorsqu'il est exigé que l'avocat fournisse les pièces à propos desquelles il pourrait refuser de témoigner (y compris notamment le Danemark, la Hongrie et le Royaume-Uni).

Si l'on part de ce principe, quelques conséquences s'ensuivent. La perquisition visant à saisir des éléments de preuve pour les utiliser ensuite dans les poursuites judiciaires doit en particulier être interdite, indépendamment de la manière et de l'endroit où les données en question sont stockées, qu'elles soient conservées dans l'ordinateur personnel de l'avocat se trouvant dans son cabinet ou hébergées par un fournisseur de services informatiques tiers, en connexion directe ou dans le nuage. Cette question sera examinée plus en détail au point 5.2.4. ci-dessous.

Le CCBE attire également l'attention sur le fait que, dans les mêmes juridictions, les protections prévues par le droit pénal sont parfois plus élaborées que celles offertes par les branches spécifiques du droit administratif.

5.2.3 Un certain nombre de juridictions disposent de règles spécialement adaptées aux avocats et aux cabinets d'avocats qui sont différentes des règles d'application générale. Dans la plupart des pays, la perquisition dans un cabinet d'avocats nécessite une autorisation distincte de la part soit d'un procureur général soit d'un juge. En Autriche, une autorisation est requise de la part du procureur général. Dans d'autres États, c'est le tribunal qui doit donner une autorisation. Un mandat judiciaire n'est parfois exigé que pour les perquisitions dans les cabinets d'avocats et cette exigence diffère de celles qui s'appliquent en temps normal.

Un certain nombre de juridictions ne prévoient cependant aucune règle particulière relative aux perquisitions dans les cabinets d'avocats. Paradoxalement, les avocats peuvent encore disposer du plus haut degré de protection assuré par un mandat judiciaire, pour la seule raison toutefois que toutes les perquisitions dans l'ensemble des lieux nécessitent un mandat judiciaire préalable. (En Irlande et au Royaume-Uni notamment).

Dans certains pays où des dispositions spéciales s'appliquent dans le cadre des perquisitions dans les cabinets d'avocats, la présence d'un procureur général ou d'un juge (Hongrie, Italie) est requise lors de la perquisition au cabinet d'un avocat. Par ailleurs, en Autriche, en Belgique, en France, en Italie et en République tchèque (et, d'après le rapport Edward, au Luxembourg[3]), le

[3] Voir C.15.

barreau compétent doit être notifié de toute perquisition prévue dans les cabinets d'avocats, et un ou plusieurs représentants du barreau doivent assister à la perquisition.

À part signaler ces divergences nationales, le rapport ne recommande nullement laquelle de ces solutions, s'il en est, est la plus appropriée. Il indique cependant que, quoi que la législation nationale puisse exiger en matière de perquisition à un cabinet d'avocats en tant qu'infrastructure physique, une protection équivalente devrait être accordée aux données des avocats en format électronique quel que soit leur emplacement physique. En raison du non-respect de ce principe de protection équivalente, les autorités sont tentées (dans les juridictions qui le permettent) de trouver un moyen de contourner les conditions plus strictes relatives à l'accès aux données conservées dans le cabinet de l'avocat.

Il convient également de souligner la présence d'un problème technique : il est impossible d'identifier de manière fiable les données électroniques des avocats comme telles. Dès lors, même lorsque ces données bénéficient d'une protection effective et rigoureuse contre les saisies, elles peuvent, même par accident, être saisies et consultées.

5.2.4. Le CCBE est préoccupé par la divergence entre les règles « normales » de perquisition et de saisie des éléments de preuve et les règles souvent moins strictes, voire quasiment inexistantes, relatives à l'interception des transmissions de données. Le CCBE ne voit en principe pas pourquoi les données des avocats devraient bénéficier d'une protection moindre dans les cas de surveillance par les services de sécurité que dans les affaires de droit administratif, privé ou pénal. Selon l'étude, le secret professionnel s'avère moins protégé dans le cadre des services de sécurité que dans le celui du droit au sens plus large. Cet aspect est signalé dès le départ : le secret professionnel est au cœur même de l'État de droit.

Il est particulièrement inquiétant que le rapport ait identifié cette tendance générale. Dans de nombreuses juridictions, les données hébergées sur internet ou transmises par le biais d'un réseau de télécommunications sont soumises à la surveillance des services de sécurité sans qu'aucune disposition particulière ou effective ne protège le secret professionnel. Les pays sont nombreux à connaître des lacunes importantes dans leur réglementation à la fois de manière générale et plus spécifiquement vis-à-vis du secret professionnel. En outre, même s'il existe un cadre juridique réglementant l'accès aux informations par les services de sécurité nationale (notamment perquisitions effectuées en secret dans les lieux, les ordinateurs, les installations de stockage, etc.), ces pouvoirs sont considérables et très étendus et, généralement, aucune garantie juridique explicite ne protège de telles informations confidentielles. Si un mandat est exigé, il est rarement judiciaire. Il s'agit habituellement d'un mandat administratif et les protections judiciaires comme il en existe ont souvent un effet limité. C'est le cas de l'utilisation, au Royaume-Uni, d'un tribunal qui reçoit seulement un nombre restreint de requêtes étant donné que, en l'absence de toute notification, un individu faisant l'objet d'une surveillance (prenons un avocat pour illustrer notre rapport) ignore qu'il fait l'objet d'une surveillance et que des informations juridiquement confidentielles ont pu être compromises. Il ne sait pas qu'il pourrait déposer plainte et ne peut donc pas le faire. Si une plainte est formulée, les délibérations du tribunal sont tenues à huis clos et ses décisions spécifiques ne sont pas rendues publiques. En Irlande, bien qu'il n'y ait aucun mécanisme équivalent au texte de loi *Regulation of Investigatory Powers Act* (RIPA) du Royaume-Uni afin de régir la surveillance virtuelle par les services de sécurité, il existe en revanche une variété de mesures individuelles : certaines exigent qu'un mandat soit délivré par un juge et d'autres, de manière plus inquiétante, qu'il soit délivré par un haut fonctionnaire de police. Tout comme au Royaume-Uni, aucune protection n'est prévue pour les informations confidentielles.

Un autre domaine d'incertitude réglementaire provient du fait que, dans certains pays, la façon dont la protection des informations des avocats en question est formulée n'établit pas distinctement si les dispositions concernées s'appliquent aux informations stockées chez des fournisseurs de services externes, tels que les fournisseurs de services d'hébergement et d'informatique en nuage. Cette incertitude se révèle être un problème en Slovaquie et en Hongrie. Par ailleurs, le code pénal italien définit également la protection d'un avocat de la défense en ayant le cabinet d'avocats à l'esprit. De telles incertitudes pourraient encourager les forces de l'ordre à s'adresser directement au fournisseur de services en nuage afin d'obtenir des informations hébergées sur son ou ses serveurs (sans mandat judiciaire dans certains pays), au lieu de se rendre au cabinet de l'avocat munies d'un mandat délivré par une autorité judiciaire.

Ces problèmes sont d'autant plus intenses en l'absence de moyen technique approprié permettant soit à un fournisseur de services en nuage ou d'hébergement soit à un tiers (tel qu'un organisme

ou une puissance étatique) de déterminer si des informations sont protégées par le secret professionnel.

La raison de cette différence d'approche est souvent historique. Ou bien les règles en matière de perquisition et de saisie d'éléments de preuve en format papier sont elles-mêmes considérablement anciennes et reflètent les valeurs universelles de la société desquelles elles découlent (comme la plupart des règles de *common law* en Écosse), ou bien, si elles sont plus récentes, ressortent néanmoins de normes profondément ancrées (comme en Angleterre, au pays de Galles et en Irlande du Nord). Lorsque les « nouvelles technologies » du télégramme et du téléphone sont arrivées, le moyen de communication semble toutefois avoir rendu les avocats et les tribunaux aveugles au message en soi, conduisant ainsi à l'interception non réglementée des télécommunications qui ont été considérées comme ne faisant pas partie du champ d'application des règles existantes. Bien que de nombreuses juridictions aient désormais élaboré des régimes de régulation en matière d'interception des télécommunications, ceux-ci ont abordé la réglementation du mauvais côté en la considérant comme un frein à l'accès autrefois excessif des services de sécurité. Ce phénomène est particulièrement flagrant dans les raisons de la promulgation de la loi RIPA au Royaume-Uni.

En conséquence, les télégrammes, les conversations téléphoniques, voire les documents transférés et, dans le contexte actuel, l'interception de toute forme de données transmises au moyen d'un système de télécommunications bénéficient généralement d'une protection nettement moins forte que les règles en matière de perquisition sur les lieux. Au mieux, dans les pays disposant d'un régime spécial pour les perquisitions effectuées dans les cabinets d'avocats, (qu'il concerne les avocats en général ou qu'il se limite aux avocats de la défense, tel que mentionné ci-dessus), celles-ci ne sont pas réalisées en vertu de règles en matière d'interception des télécommunications. L'avocat perd alors sa protection spéciale, s'il en bénéficiait, et se trouve à la place assujetti aux règles générales qui s'appliquent à l'ensemble des citoyens. Dans certaines de ces juridictions qui considèrent toutefois la protection des données relatives aux clients comme étant principalement une protection destinée à l'avocat de la défense (par opposition à une protection des données relatives aux clients détenues par des avocats en général), seul celui-ci peut conserver sa protection spéciale. Dans le pire des cas, (à l'instar du Royaume-Uni où, bien que l'avocat ne soit pas protégé par un régime spécial, il bénéficie de règles qui régissent dans l'ensemble les perquisitions dans des locaux), l'avocat, tout comme ses concitoyens, se verra protégé uniquement grâce à un régime de surveillance qui est nettement moins protecteur que le régime papier et qui n'offrira aucune protection juridique aux données relatives à ses clients, le laissant ainsi s'appuyer à la place sur l'application du code de pratique par le commissaire à l'interception.

Si la société estime convenablement que les données détenues par les avocats doivent bénéficier d'une protection, alors il ne peut y avoir de justification adéquate à une telle discrimination. Dans le milieu informatique actuel, pareille différenciation s'avère également peu naturelle : les utilisateurs ont recours à la même interface pour accéder aux données, les partager, les communiquer et les stocker ; sans même savoir quand les informations sont envoyées d'un ordinateur à un autre. Il en va de même pour l'avocat qui utilise son ordinateur, que les données électroniques relatives aux clients aient été envoyées en tant que pièces jointes d'un courriel ou simplement partagées avec le destinataire après l'identification de ce dernier.

L'augmentation des moyens de communication sortant du cadre traditionnel de la télécommunication est également source de préoccupations. Autrefois, les organismes spécialisés disposant de compétences spéciales (la poste publique qui pouvait décacheter vos lettres à la vapeur ou, par la suite, les entreprises de télécommunications qui pouvaient mettre vos conversations téléphoniques sur écoute) étaient chargés de procéder aux interceptions, selon des ouvrages et des formations spécifiques et à l'aide de matériel spécial.

Toutefois, le fait est que dans certaines juridictions, de telles activités étaient soumises à des régimes de réglementation spéciaux. À l'heure actuelle, même si les fournisseurs de services de communications électroniques offrent toujours l'infrastructure de base pour communiquer, ils nous sont presque invisibles et les capacités de ces fournisseurs de services de communications électroniques ne sont souvent pas suffisantes afin de procéder à une interception de communications réelles. Les fournisseurs de services ouverts (*over-the-top*, OTT) tels que Skype, qui ne sont pas soumis à de tels régimes de réglementation en matière de télécommunications, sont de plus en plus courants. Dans le cas de certains de ces services ouverts, une collaboration entre les fournisseurs de services de télécommunications devrait suffire à les décoder en tant que messages mais, dans d'autres cas, les forces de l'ordre ont besoin de l'aide des fournisseurs de

services ouverts eux-mêmes. Dans certaines juridictions, l'accès des fournisseurs de services ouverts n'est même pas soumis à un régime de réglementation spécial concernant les fournisseurs de services électroniques. Cette situation est cependant moins (ou peut-être plus) inquiétante dans d'autres juridictions où aucun régime spécial n'existait auparavant ou n'existe pas actuellement. Au Royaume-Uni par exemple, un régime de réglementation (en vertu de la loi RIPA et de l'institution ISA) régit toute forme de mise sur écoute ou d'accès aux canaux de communication qu'empruntent évidemment des services tels que Skype.

Il s'agit donc aux yeux du CCBE d'une lacune fondamentale que le régime d'interception des télécommunications soit si fondamentalement différent (et généralement plus inefficace) que les règles en matière de perquisition et de saisie des éléments de preuve dans des locaux. Bien que ce soit une critique générale, elle acquiert une résonnance particulière dans le cas des données détenues par les avocats puisqu'elle découle généralement de la perte, dans le régime de télécommunication, de toute protection garantie aux données des avocats dans le monde matériel. Le CCBE considère cette situation comme inacceptable.

6. Conclusions

Ce document se veut modeste dans sa portée et dans son ampleur, mais un exercice si limité soulève tout de même des questions très préoccupantes.

Premièrement, l'étude du CCBE considère la protection de la confidentialité des données des avocats comme un élément fondateur de l'État de droit. Les régimes de réglementation élaborés de façon indépendante par l'ensemble des juridictions que l'étude a interrogées reflètent cette norme fondamentale dans leurs règles respectives applicables dans le déroulement des perquisitions et des saisies d'éléments de preuve dans les cabinets d'avocats. Quelle que soit la diversité parmi ces systèmes (et l'on constate une importante diversité), ils partagent tous cette valeur comme tronc commun.

Les règles n'ont cependant pas toujours suivi les évolutions technologiques. C'est pourquoi, dans certaines juridictions (mais pas dans toutes), les données électroniques conservées dans les locaux d'un fournisseur informatique pour le compte d'un avocat bénéficient d'une protection moindre que les données conservées dans le propre cabinet de l'avocat. Le CCBE ne voit rien qui puisse justifier pareille distinction.

Deuxièmement, dans la mesure où les règles relatives au monde matériel d'un cabinet d'avocat offrent des dispositions spéciales prévoyant, par exemple, la présence de représentants du barreau de l'avocat lors de la perquisition à son cabinet, une disposition similaire devrait alors être prévue pour les perquisitions virtuelles. Cette mesure peut demander davantage de travaux de normalisation en informatique de la part des fournisseurs de services informatiques, y compris des fournisseurs de services d'informatique en nuage, mais le CCBE l'estime nécessaire.

Aux yeux du CCBE, le principe primordial à observer devrait établir que le monde papier et le monde électronique devraient bénéficier d'une protection identique.

Ce principe implique également qu'il soit garanti que lorsqu'un régime strict en vigueur protège les données détenues par les avocats, ce régime ne puisse pas être contourné par les autorités concernées en demandant directement de manière officielle ou officieuse aux fournisseurs de services informatiques des avocats de leur fournir des informations.

Le principe doit établir que la réglementation effective ne puisse pas être raisonnablement contournée. Nous ne devons pas revenir par défaut à une protection minimale.

De même, toutes les protections prévues dans le cadre de la perquisition et de la saisie devraient également s'appliquer si les données sont interceptées et consultées au cours de leur transfert, en tant qu'élément d'une communication, qu'importe si l'entité techniquement chargée de l'interception est un fournisseur de services de communications électroniques, un fournisseur de services informatiques ou une agence étatique agissant directement. Même si le CCBE estime qu'il s'agit d'un principe d'intérêt général et qu'il ne voit aucune raison qui justifie cette différenciation entre le monde matériel et le monde des écoutes téléphoniques et de la surveillance électronique, il convient de se montrer réaliste vis-à-vis des objectifs envisageables. Le CCBE admet que mettre le contrôle des écoutes téléphoniques au même niveau que le contrôle des perquisitions représenterait un immense travail législatif pour chacun des États membres. Même si les ressources nécessaires à l'accomplissement de cette tâche étaient disponibles, le CCBE doute que

la volonté nationale soit au rendez-vous, puisque les gouvernements protesteront certainement que la surveillance qu'ils exercent est absolument nécessaire à la protection de leur population contre les ennemis appréhendés. Quoi qu'il en soit, le CCBE estime que la protection du secret professionnel est une valeur fondamentale et une garantie primordiale du maintien de l'État de droit au point qu'il propose ce principe légèrement plus restreint :

Le principe devrait établir que, quel que soit le régime en vigueur dans un État membre en matière d'interception des communications, il devrait garantir l'inviolabilité des données et des autres éléments de preuves relevant du principe du secret professionnel.

Finalement, afin que les institutions européennes et les gouvernements des États membres mettent effectivement en œuvre les trois principes ci-dessus, le CCBE estime qu'il serait souhaitable de demander une étude plus approfondie et de plus grande envergure que le présent document. Le CCBE cherche donc à obtenir un financement de la part de la Commission afin qu'une institution universitaire appropriée réalise cette étude.

Si nous souhaitons garantir la durabilité d'une profession d'avocat indépendante et vigoureuse en tant que l'un des garants du maintien de l'État de droit à une époque où tant de personnes aspirent davantage à une sécurité illusoire qu'à la valeur éternelle qu'est la liberté, nous devons à la profession de soutenir cet appel à l'action.

ANNEX

CCBE QUESTIONNAIRE ON GOVERNMENTAL ACCESS TO LAWYERS' DATA IN THE CLOUD

Table of Contents

NATIONAL RESPONSES – COMPARATIVE TABLE

1. **Andorra**
2. **Austria**
3. **Belgium**
4. **Czech Republic**
5. **Denmark**
6. **France**
7. **Finland**
8. **Germany**
9. **Hungary**
10. **Ireland**
11. **Italy**
12. **Norway**
13. **Poland**
14. **Slovak Republic**
15. **Slovenia**
16. **Sweden**
17. **Spain**
18. **United Kingdom**

1. May the government require a Cloud provider to disclose lawyers' data in the course of a Government investigation?	
Andorra	En dehors d'un contrôle judiciaire, ce n'est pas possible.
Austria	Yes, if the object of the investigation is a criminal misconduct of the lawyer, or a court order exists for the seizure of certain client files.
Belgium	Belgium has not implemented specific rules in relation to cloud service providers; the same rules as with respect to other types of hosting services apply. Lawyers' data is subject to specific protection regimes. The general rules in relation to search and seizure orders are included in the Judicial Procedure Code (Code d'Instruction Criminelle/Wetboek van Strafvordering), including ICT specific rules, i.e. search and seizure of stored computer data, production orders and expedited preservation of stored computer data, as described under the Budapest Convention. The most directly relevant rules relate to the protection of private communication and

	telecommunication, and the authority to intercept or record such information, which is included in Article 90ter and following of the Code. These provisions allow prosecutors to order interception/recording, and to commandeer the cooperation of service providers if necessary. However, lawyers' data (including the telecommunications means used by lawyers) are protected specifically by Article 90octies of the Code: such data may only be intercepted if the lawyers themselves (and not their clients) are suspected of the enumerated crimes, or of having participated in them, or if the suspects are believed to have used their means of communication. The specific investigative measure may only be executed after the head of the competent bar association has been duly informed. Information protected by professional secrecy (client information) will be stricken from any reports drafted following the execution of the measure. The rules above apply only to interception. Separate rules are defined in relation to data seizure (including copying and sealing of IT systems) in Article 39bis of the Code. This Article states that such measures are subject to the same requirements as in relation to confiscation. Since confiscation of lawyers' data would traditionally require a search of the lawyers' offices (subject to the same requirements as elaborated above), it could be reasonably argued that the same requirements would also apply to seizures of lawyers' data on cloud systems. However, the law does not state this explicitly. We are not aware of any jurisprudence on this point. Cooperation of IT service providers can at any rate be ordered through Article 88quater of the Code; no specific rules in relation to lawyers are defined on this point. The provisions above cover general criminal investigations. National security investigations are governed by a separate law of 30 November 1998, which has been frequently revised to introduce special investigative measures. This permits intelligence and security services to use so-called exceptional measures to collect data (Article 18/2 of the Law). These measures include the observation and searching of any private places (explicitly including lawyers' offices), and to obtain any information they require within their remit, including from private service providers; this would include cloud computing providers. Interception and accessing of ICT systems is included as well, as is the breaking into such systems using 'technical means, false signals, false keys or false pretences'. Again, specific protective measures for lawyers are foreseen in the law. The head of the competent bar association must be informed in advance by the Committee that authorizes such measures, although (s)he is bound by a criminally punishable duty of secrecy with respect to these measures; thus, the lawyers themselves may not be informed. The president of the Committee will also verify whether the collected privileged data is directly linked to the investigated threat, and (s)he will need to be present when the measure is executed, either in person or via a delegated representative. Furthermore, the measures can only be used if the lawyer is 'personally and actively' involved in the threat.
Czech Republic	Yes. There is no clear law that would stipulate the matter in the Czech Republic as regards Cloud data, but, for example, the criminal proceedings authorities may require any person to cooperate in the course of the investigation. This right may not breach the confidentiality respected by the state unless previously approved by a judge, but even

	the judge may not, however, challenge the nondisclosure imposed on lawyers ("advokat"). Another example, not necessarily relevant to cloud data computing, of how the lawyer's confidentiality is protected would regard the search of lawyer's premises. This can be carried out only under a special regime with the attendance of a Czech Bar Association representative. Another example may be the protection of client – lawyer communication during wire taping. In this case the relevant authority must destroy the record and can not use it as evidence. Having said that – the Czech law provides protection to the lawyer's client data in some areas, but does not clearly provide protection in the matter of the question. The general principle described in the first part of the answer avoids the government (in the criminal proceedings) from receiving the client data from lawyer. It is however questionable if this limit covers also a cloud provider from the duty to provide data that the investigative bodies request (e.g. with judge's approval). As regards other non procedural data requests, the situation is less protective. For example, the The Security Information Service (Bezpečnostní informační služba; and also the Army intelligence) may request a public communication network or service provider to receive a gateway to the network for the purpose of wire taping or to request other communication data. The use of this intelligence is a subject to the approval by a High court judge; however this law provides no limit as to the lawyer's data.
Denmark	Yes – but only if the mentioned data is not communication between a criminal defence lawyer and his/her client and only following a court order
France[4]	Il convient d'étendre les règles applicables en matière de perquisitions des cabinets d'avocats à cette question. Ces règles sont une exception au droit commun de l'enquête selon lequel une autorité de poursuite ou d'enquête peut accéder à des données informatiques, même stockées à l'étranger[5]. Concernant les avocats, le régime de la perquisition garantit la confidentialité et le secret professionnel au bénéfice des clients : afin de protéger les droits de la défense, les perquisitions ne peuvent être faites dans les domiciles ou cabinets des avocats que par un magistrat, après décision écrite et motivée justifiant la perquisition sur la base de doutes sur la participation de l'avocat à une infraction. La perquisition se fera obligatoirement en présence du Bâtonnier ou de son délégué, et du confrère lui-même, le cas échéant assisté d'un conseil. Le bâtonnier, qui s'assure du respect du secret professionnel, vérifie que seuls les documents relatifs à l'infraction justifiant la perquisition soient saisis et peut s'opposer à une saisie (article 56-1 code de procédure pénale[6])[7].

4 For the full contribution of the French Delegation see also below - Annex I

5 Articles 56, 57-1, 60-1 et 60-2 code de procédure pénale.

6 Article 56-1 code de procédure pénale : « *Les perquisitions dans le cabinet d'un avocat ou à son domicile ne peuvent être effectuées que par un magistrat et en présence du bâtonnier ou de son délégué, à la suite* ***d'une décision écrite et motivée prise par ce magistrat****, qui indique la nature de l'infraction ou des infractions sur lesquelles portent les investigations, les raisons justifiant la perquisition et l'objet de celle-ci. Le contenu de cette décision est porté dès le début de la perquisition à la connaissance du bâtonnier ou de son délégué par le magistrat. Celui-ci et le bâtonnier ou son délégué ont seuls le droit de consulter ou de prendre connaissance des documents ou des objets se trouvant sur les lieux préalablement à leur éventuelle saisie. Aucune saisie ne peut concerner des documents ou des objets relatifs à d'autres infractions que celles mentionnées dans la décision précitée. Les dispositions du présent alinéa sont édictées à peine de nullité.*

Le magistrat qui effectue la perquisition veille à ce que les investigations conduites ne portent pas atteinte au libre exercice de la profession d'avocat. […] »

7 Voir arrêt de la Cour européenne des droits de l'homme du 24 juillet 2008 *: « La Cour estime que des perquisitions et des*

	En conclusion, les autorités ne peuvent obtenir d'un fournisseur d'informatique en nuage des données d'un avocat qu'après avoir obtenu la décision écrite et motivée d'un magistrat. La protection du secret professionnel est donc une limite au pouvoir de ces autorités.
Finland	Yes, if there is investigation of serious crime and the lawyer is either suspected of that crime or in some other role than legal defender of the suspected person. The Government can not require a Cloud provider to disclose lawyer's data if the lawyer is defending the suspected person in court or on investigation.
Germany[8]	Yes. There are several legal bases which are extremely controversial as to the question whether they legitimize access by governmental agencies. One thing that is certain, however, is that such access does occur. a) Regarding criminal proceedings, the Federal Court of Justice (Bundesgerichtshof) rejected covert online searches (in particular via recourse to § 102 Code of Criminal Procedure Strafprozessordnung, StPO) due to the lack of a legal basis (after initially having made partly different assessments) by decision of 31 January 2007 (Az. StB 18/06). (Covert online search has not and still does not only concern private PCs, but basically any EDP structure associated with an accused person in criminal proceedings). b) With a view to averting danger, covert police interventions are admitted at the federal level on the basis of § 20 k BKA Act (Act governing the activities of the German Federal Police Office), for example. c) At Länder level, such covert online searches by the police are in part authorized by the laws of the respective Land (e.g. in Bavaria, Art. 34 (d) of the Act on Police Functions (Polizeiaufgabengesetz). d) As far as intelligence-led access is concerned, such access is based on special legal foundations (e.g. § 8 (2) of the Act on the Protection of the Constitution (Bundesverfassungsschutzgesetz)). Only for a small area (namely procedural measures) - incomplete - protection flows from § 97 in conjunction with § 53 (1) sentence 1, no. 3 of the Code of Criminal Procedure. However, insofar as data are put „into the Cloud", it is doubtful whether data custody by the lawyer (which is necessary as a safeguard in criminal procedure), who is subject to professional secrecy, still exists. § 97 (2) sentence 2 StPO explicitly extends the privilege to EDP service providers of health-care professions where they use patient-related information. This provision – which does not exist for the legal profession – speaks in favour of declining safe custody with the professional who is subject to secrecy, in cases of outsourcing via the Cloud, and thus in favour of affirming the possibility of access for investigation authorities.
Hungary	Yes. There is effectively no difference between the way the government may request data

saisies chez un avocat portent incontestablement atteinte au secret professionnel, qui est la base de la relation de confiance qui existe entre l'avocat et son client. […]Partant, si le droit interne peut prévoir ***la possibilité de perquisitions ou de visites domiciliaires dans le cabinet d'un avocat, celles-ci doivent impérativement être assorties de garanties particulières*** » ; affaire André contre France, requête n° 18603/03.

8 For additional comments and remarks by the German delegation see below Annex II

	from a Cloud provider regarding non-lawyer and lawyer data. To get an overview of the regulation, the fist level is a statutory protection for personal data and business secrets, and a prohibition to either request or to provide such data without specific statutory authorization. Government bodies may request such data on multiple grounds, but the two major branches are a) requests based on specific procedural law (more specifically, criminal and administrative procedure, civil law procedures are only important as "witness testimony"); and b) "secret information gathering powers" that are granted to specific bodies, that is, national security service providers (five different authorities) and investigating authorities (police and customs authority) and are not subject to the same constraints as criminal and admin procedures.) 1. Regarding data requests based on secret information gathering powers, certain data requests require prior approval by external bodies (judges or the ministry of justice) that a) secretly record or survey the content of any communication (including computer data), b) secretly searches of apartments, c) secretly surveys the inside of apartments. These bodies may also (without such prior approval) request data provision from any person (including private persons and enterprises), and the responding persons may not reveal this to the persons affected, and may not refuse data provision based on personal data or business secret. There are no specific rules for lawyer data in this regard, but should they request a lawyer to reveal client information directly, that would violate the more regulated provisions under procedural law, so even if they do not act under the given procedural law, the lawyer itself should refuse data provision on this ground (there are no specific exemptions under this regime for "lawyers secrets", only for general business secrets.) (There has been no report on authorities trying to abuse this power.) 2. Regarding procedural laws, the following lawyer specific regulations exist (we refer to : a) "generic data requests" can be denied referring to "lawyer secrets" by the lawyer (criminal law: 1998. évi XI. törvény 8. §, Be. 71. §, Be. 178/A. §, administrative law provisions do not clearly refer to causes for declining to testify, but one can do the same under administrative law); b) a lawyer may (criminal and private procedure law) or has to (administrative law) decline to testify as a witness, for professional secrets; c) as a holder of an object to be inspected by the authority, the lawyer may refuse to hand over such object based on the same grounds as declining to testify (Be. 119. §, Ket.57/A. §, Pp. 188. §); d) search warrants (apartment search) and seizure require previous approval by judges; and no documents may be seized for which testimony may be denied and that are at the possession of the lawyer in its official premises (criminal law); no documents may be seized which contain professional secrets (under administrative law). Therefore, there are no protection for data kept by lawyers at third parties (e.g. cloud

	providers), even if the cloud provider knows that his customer is a lawyer possessing client criminal data. Outside lawyer specific regulations (e.g. cloud providers), a cloud provider has to provide data to government bodies based on the following, criminal law specific conditions: a) the content of a communication can only be recorded and handed over after having received a specific warrant from a judge for a specific crime (or a warrant from the prosecutor with an indication of "vital urgency", for 72 hours max.); b) if requested by the police or customst authority, medical data and business secrets other than those by a communications service provider and bank secrets can only be given with a prior approval from the prosecutor; c) if requested by the police or customst authority, all other business secrets may be required without prior approval of third parties. d) Any third person may be requested to testify as a witness, be subject to a search warrant, to seizure (and be obliged to cooperate in locating the information to be seized), or as a holder of an object to be inspected. Merely having an obligation to keep a business secret is not an exemption. During administrative procedures, if one is not the subject of the administrative procedure itself, may be requested to testify or to cooperate during a seizure or as a holder of an object to be inspected. Here, one may refuse to testify on grounds of having an obligation to keep a business secret, so a Cloud provider is entitled to refuse provision of data under administrative procedures. For more details see below, Annex III
Ireland	There are no specific laws concerning government access to data held by a cloud provider (“CP”). The doctrine of legal professional privilege is a key tenent of Irish law and significantly limits the extent to which the Irish government can access lawyers’ data.
Italy	In general, the government cannot require a Cloud provider to disclose lawyers’ data in the course of a Government investigation. The disclosure is possible only if the lawyer is involved in a crime, but in such cases, the lawyer is considered as a private citizen for the purpose of the law.
Norway	No Even though the client information is stored in the Cloud by an external IT supplier it is still the lawyer /law firm who is the owner of the information. Every external request for disclosure of information should be forwarded to the lawyer who is responsible for the engagement in which the information is stored. As a general rule professional privileged information is according to Norwegian law protected against external control and observation by public authorities.

Poland	**Bar Council** Yes. According to the Telecommunication Law Act dated 16 July 2004, providers of telecommunication services are obliged to keep and store the data necessary for: (i) establishing the end of the network, telecommunication end device of an end user who initializes the connection and to whom the connection is directed; (ii) establishing the date and time of connection, type of connection and localization of the end device. The providers are obliged to disclose the above data to the authorized entities (i.a. the court or the public prosecutor) on the basis of separate regulations (e.g. provisions of the Criminal Procedure Code). A separate basis for requiring electronic data is Art. 218a of the Criminal Procedure Code, pursuant to which public institutions and telecommunication entrepreneurs are obliged, upon decision of a public prosecutor or a court, to secure and deliver data stored on electronic devices or in an IT system. This obligation may be ordered for a definite period of time, not exceeding 90 days. Please note that the Telecommunication Law does not distinguish lawyers as a particular group of service users, therefore the general rules with regards to requesting data from telecommunication service providers apply to them. According to Art. 226 of the Criminal Procedure Code, however, the documents that contain information which are subject to the advocate secrecy, cannot be used as evidence in criminal proceedings.
	The National Council of Legal Advisers We understand the government as the Prosecutor, Police and other bureau with police powers. We also understand data as the Client data which is covered by the professional legal privilege. Cloud provider is not the database administrator so the government cannot require a Cloud provider to disclose lawyers' data.
Slovak Republic[9]	- <u>CRIMINAL PROCEEDINGS – Code on the Criminal Proceedings</u> **Section 90** **Storing and delivering (handing over) of computer data** (1) If storage of saved computer data including operational data saved by means of computer system is necessary in order to clarify facts significant for criminal proceedings , then presiding judge or a prosecutor within pre-trial proceedings or prior to the commencement of criminal prosecution may issue an order that needs to be justified by factual circumstances and addressed to a person in whose possession or under whose control such data are, or to a service provider of such services, with the view of: a. Storing and keeping completeness of such data b. Enabling production and keeping / possession of copies of such data c. Making access to such data impossible d. Removing such data from computer system

[9] General Remarks:
No specific regime for cloud-computing used by lawyers in Slovak Republic; general statutory regulation applies (Act no. 22/2004 Coll. on Electronic Commerce)
Authority of public bodies to require access to data stored through cloud-computing from cloud-provider emerges from certain legal acts, for instance: the Constitutional Act on the security of the state in time of war, warfare, exceptional or emergency state, the Code on Criminal Proceedings, the Code on Administrative Proceedings, the Act on the Slovak Information Service.

	e. Handing over such data for the purposes of criminal proceedings. (2) The order issued pursuant to the par. 1 must state a period of time during which data storage shall be carried out, maximum period is 90 days, and if repeated storage is necessary, new order shall be issued. (3) Where there is no longer a need to store computer data, including operational data for the purposes of criminal proceedings, the presiding judge of a panel or a prosecutor prior to the commencement of criminal prosecution or in pre-trial proceedings, respectively, shall issue an order reversing the obligation to store the data. **Sec. 118** **Comparison of data found in different computer systems** (1) Comparison of data within different information systems containing characteristic/typical or excluding features of persons, things or material for criminal proceedings may be carried out if necessary for clarification of a crime within criminal proceedings on wilful criminal act liable to a sentence of deprivation of liberty with the maximum term exceeding 3 years, on corruption or an any other wilful crime if such proceedings are to be conducted pursuant to a binding international treaty. (2) Written order to compare data in different information systems shall be issued by presiding judge or by prosecutor within proceedings prior to commencement of criminal prosecution or within pre-trial proceedings. - ADMINISTRATIVE PROCEEDINGS - the Code on Administrative Proceedings **Sec. 32** (3) Upon the administrative authority request the public authorities and the socialist organizations must communicate the facts which are relevant for the proceedings and for the decision. - ACT ON THE SLOVAK INFORMATION SERVICE **Sec. 15** **Authorization to request the provision of assistance, data, and information** (1) The Information Service shall be authorized within the scope of its functions to request from state and other bodies, legal entities and individuals, the provision of assistance, data, and information, which can contaribute to the understanding of facts critical to the fulfilment of the duties decreed by this Law. (3) No one shall be forced to provide assistance, data, or information.
Slovenia	Yes.
Sweden	No. Even though the client information is stored in the Cloud by an external IT-supplier, it is still the advocate/law-firm who is the owner of the information. Therefore it is the advocate who has entire disposal and being in control of the electronically stored information. Every external request for disclosure of information should therefore be forwarded to the advocate who is responsible for the mandate in which the information is stored. Furthermore and foremost, professional privileged information is in Sweden, as a

	general rule, protected from external control and observation and is covered by a ban of seizure and confiscation (see i.a. chap. 37, sect. 2 of the Swedish Code of Judicial Procedure) and other procedural protections (prohibition to interrogate advocates, see chap. 36, sect. 5 of the Code of Judicial Procedure). ➢ Just to make it absolutely clear; when talking about "the Government", the only possible interpretation in Sweden would be by public authorities, as for example the Public Prosecution Authority (the prosecutor's office) and other offices of the State administration – not the Government itself (it is in Sweden unthinkable to have political investigations in relation to professional secrecies of advocates).
Spain	To answer this question, it is necessary to consider the following scheme: 1º Is the request done in the context of a police investigation? In this case, in principle, the data subject´s consent is not required, but to can have access to such data the condition is that there is a real threat for the public safety or the suppression of crime. These cases have been narrowly interpreted by the Spanish Data Protection Agency (DPA). 2º To which data is the access intended? - If the access is to lawyer´s data as subject of the investigation, the cloud provider shall provide those data always that the conditions stated above are met. - If the access is to lawyer´s data clients, then the lawyer´s professional secrecy does apply. 3º In all cases the secrecy of communications is guaranteed. It is important to take into consideration that according to the Judgment of the Supreme Court of 9 February 2012 it is necessary to respect the rights of lawyers and their clients in cases in which intercept of communications is ordered. Having said that, and in order to answer to this question would be recommendable to take into consideration specific cases as a law enforcement investigation for administrative purposes (law enforcement) may differ from a criminal investigation[10]. This issue is further developed. The key point is that the access without consent for police purposes is only possible when the data are needed to prevent a genuine threat to public safety or for the suppression of crime and, as mentioned before; in such cases the Spanish Data Protection Authority has provided a narrow interpretation. The investigation must be concrete and/or real threat, not a potential or possible.. For this reason, it is necessary to provide an overview from a data

[10] In this sense, article 22(1 and 2) of the Organic Law 15/1999 states that
"*1. The files created by the security forces and containing personal data which, because they were collected for administrative purposes, must be recorded permanently, shall be subject to the general rules of this Law.*
2. Collection and processing, for police purposes, of personal data by the security forces without the consent of the data subjects shall be limited to those cases and categories of data necessary for the prevention of a genuine threat to public safety or for the suppression of crime; such data shall be stored in special files established for the purpose, which must be classified according to their degree of reliability."
Also, according to article 11(2)d consent for the communication of personal data is not required "*when the communication to be effected is destined for the Ombudsman, the Office of Public Prosecutor, judges, courts or the Court of Auditors in the exercise of the functions assigned to them. Not shall consent be required when the communication is destined to regional government authorities with functions analogous to the Ombudsman or the Court of Auditors."*
The Spanish DPA has released several legal opinions in which concludes that a controller may communicate personal data to the police always than the guarantees provided in the Organic Law 15/1999 are met.

	protection perspective, the right and duty on professional secrecy and, finally, answer the question. For additional information see also Annex IV
United Kingdom	See Below – Annex V, Continuations sheet
2. May a Cloud provider voluntarily disclose lawyers' data to the government in response to an informal request?	
Andorra	Non
Austria	That this does not happen has to be secured with a contractual obligation imposed on the Cloud provider.
Belgium	No. Even in the highly unlikely event that this would be contractually permitted and that it would not be considered a breach of general data protection rules, any professional service provider should be aware that lawyers' data is privileged and highly sensitive. Revealing such data would at the very least qualify as a tort, and could likely result in criminal prosecution, e.g. for violation of communications secrecy.
Czech Republic	No, the reasons being business and data confidentiality and prevention of damages. However, it would be a crime not to report or interrupt specified criminal activities. The duty to report would then lead to "voluntarily" disclosure.
Denmark	Yes
France	Non car la Loi Informatiques et Libertés impose au responsable d'un traitement informatisé de données à caractère personnel de garantir la confidentialité des données conservées[11]. Les prestataires de services des avocats sont susceptibles d'ignorer les implications juridiques et les exigences de protections associées au secret professionnel auquel leur client est soumis. Ils sont susceptibles d'ignorer les risques qu'ils encourent s'ils permettent l'accès à des données couvertes par le secret professionnel sans qu'aient été respectées les exigences applicables.
Finland	No. There have to be a formal request. In writing by the Cloud provider's request.
Germany	Possibly, yes. Unless precluded by contractual provisions, „voluntary disclosure" by the provider is conceivable, at least with regard to non-personal information. Where the request is made by legal persons, this may be data which are subject to lawyers' professional secrecy (but not to data protection law).
Hungary	No. Voluntary data provision is prevented by the general rule of business confidentiality provided by section 81 of Act IV of 1959 on the Civil Code ("Civil Code"). Business confidentiality, i.e. the prohibition against abusing or unlawfully disclosing confidential information, is a persistent principle even without expressly stipulating it in an agreement. However, whether Cloud Service Providers are also bound by the confidentiality of lawyers, depends on the interpretation of the Attorney Act. Section 8 para. 4 of the Attorney Act specifically stipulates that the lawyer's obligation shall apply to the entire firm and its personnel. The word "personnel" primarily refers to employees or other engaged persons of the firm.

[11] Article 34 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : « *Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.* »

	In addition, pursuant to Act CXII of 2011 on the Right of Informational Self-Determination and the Freedom of Information ("Data Protection Act"), a Cloud Service Provider is deemed to be a data processor who does not have any controlling rights over the data processed for the data controller (the lawyer), preventing it from deciding on voluntary transfer of personal data.
Ireland	Any such disclosure would likely be a breach of contract, a breach of confidentiality and in breach of legal professional privilege. Legal professional privilege belongs to a client and cannot be waived by any person other than that client or a lawyer acting with that client's authority to so waive legal professional privilege. Legal professional privilege is binding not only on lawyers but also on their servants and agents. Accordingly, to the extent that a CP is a servant or agent of a lawyer, the CP is not permitted to breach legal professional privilege save to the extent that they are authorised to do so by the lawyer acting with the express or implied authority of his client(s). A lawyer availing of services provided by a CP should procure contractual rights which enable the lawyer to assert legal professional privilege.
Italy	A Cloud provider cannot disclose data in response to an informal request. However, he shall provide data in response to a formal request, without distinctions between data coming from private persons or lawyers.
Norway	No See section 1 above. The Cloud provider cannot reveal information in the cloud to public authorities unless the lawyer has given consent to it. In order to do so the lawyer needs the consent from the client.
Poland	**Bar Council** No. According to the Telecommunication Law Act, telecommunication services providers are bound by the so-called telecommunication secrecy, which means that they cannot disclose any personal data of the users in response to informal requests.
	The National Council of Legal Advisers Cloud provider can't voluntarily disclose lawyers' data to the government in response to an informal request. It should be also regulated in the agreement signed between data administrator (law firm, professional) and Cloud provider with the contractual penalty for breaching such requirements.
Slovak Republic	Request / order has to be issued in a form prescribed by the law and it has to be issued by a competent authority.
Slovenia	Yes, except for personal data without a legal purpose.
Sweden	No. See 1 above. The issue of disposal of information is, however, often also settled in confidentiality agreements or similar agreements between the owner of the information (the advocate/law-firm) and the IT-supplier/Cloud provider. Consequently, the Cloud provider is prohibited from revealing information in the cloud to the government, unless the advocate has given consent to disclosure. In such a case the advocate must have the consent of the client.
Spain	A Cloud provider may not disclose, voluntarily or not, lawyers´ data in response to an informal request. Otherwise, the cloud provider could be held liable for infringing

	fundamental rights and legal and/or contractual obligations.
United Kingdom	There is no specific legislative provision expressly preventing this. The subject of the lawyer's data (typically, the client, though the lawyer could also fall into this category) benefits from national implementation of the EU data protection regime in the ordinary way, but this is considered to provide limited protection, particularly where the request is made for law enforcement purposes falling within the DP Framework Decision rather than the DP Directive. In relation to communications data retained by a provider pursuant to Directive 2006/24/EC, the agency concerned would normally be expected to obtain an authorisation under RIPA.
3. If a Cloud provider <u>must</u> disclose lawyer's data to the government, must the lawyer be notified?	
Andorra	Non
Austria	This has to be secured with a contractual obligation imposed on the Cloud provider.
Belgium	As noted above, there is a prior information obligation towards the head of the bar, and an obligation to strip out any privileged information, since the orders may only target the lawyer for his own alleged crimes, and not for any alleged wrongdoings of his clients. In traditional criminal investigations, the lawyer would be informed either when he is officially charged, or when the investigation is terminated, like any other suspect. In national security investigations, no notification is required.
Czech Republic	No
Denmark	Yes, but only if disclosing the mentioned data is considered to be an interception of communication
France	Une telle contrainte constituerait un contournement des règles relatives à la perquisition des cabinets d'avocat (cf réponse à la question 1). Une saisie de ces données qui ne se feraient pas sans la présence du bâtonnier serait passée en fraude des droits de l'avocat et donc il est évident que ce dernier doit en être prévenu en urgence. Il est cependant recommandé à l'avocat d'inclure dans son contrat de fourniture de services de stockage en cloud, des clauses garantissant que l'avocat pourra mettre en œuvre toutes les précautions utiles et les procédures particulières afin de protéger le secret professionnel. Les prestataires de services des avocats sont susceptibles d'ignorer le statut d'avocat de leur client et par conséquent les implications juridiques et les exigences de protections associées au secret professionnel auquel leur client est soumis. Ils sont susceptibles d'ignorer les risques qu'ils encourent s'ils permettent l'accès à des données couvertes par le secret professionnel sans qu'aient été respectées les exigences applicables.
Finland	Not at the moment of the disclosing. But afterwards the lawyer have to be notified.
Germany	No. Notification is not provided for in all cases (it is not required regarding police measures pursuant to § 20 (k) of the BKA Act, for example).
Hungary	Regarding secret information gathering powers and data gather during criminal procedure where a judges's approval is required, the Cloud provider is prohibited from doing so. Otherwise, it is up to the service provider and its agreement with its customer.

Ireland	This is primarily a matter of contract between the lawyer and the CP. It is to be expected that a lawyer will insist on a contractual requirement to notify in the event that any government seeks to gain access or actually gains access to lawyer's data. However, where laws, such as anti-money laundering regulations (which apply equally in other EU states), prohibit 'tipping-off' such contractual protections may not be of effect.
Italy	If a Cloud provider discloses personal data in accordance to a government's request, the notification to the owner of such data is not required (the rule applies also to lawyers). However, where the government is aware that the data belong to a lawyer and concerns exchanges with the client covered by confidentiality, he cannot proceed with the order.
Norway	Yes
Poland	**Bar Council** According to the Criminal Procedure Code, a decision on requesting data (as described in point 1 above) must be delivered to the "owner" of the data, however the delivery of the decision may be postponed for the period necessary for the interest of the case, no longer than until the final and valid conclusion of the case.
	The National Council of Legal Advisers As in the first question the Cloud provider cannot disclose lawyer's data.
Slovak Republic	- CRIMINAL PROCEEDINGS – Code on the Criminal Proceedings **Sec. 90** (4) An order issued pursuant to the par. 1 to 3 shall be delivered to a person in whose possession or control the data are or to a service provider of such services; both of them **may be imposed the obligation of keeping in secret the measures contained in the order**. **Sec. 93** The authority which executed the order shall immediately issue a written confirmation of taking over the computer data to the person who handed over the computer data or from whom were the computer data withdrawn or from whom were the computer data taken over. **A person whose data were seized shall be informed in written by the authority which has taken over the data.**
Slovenia	No, not by the Cloud provider.
Sweden	Yes, see 1-2 above.
Spain	As explained before, if the request involves personal data in cases according to article 22(2) of the Organic Law 15/1999, considering that such communication of personal data to the law enforcement authority fulfils the requirements provided in such article or there is a judicial request, notification to the lawyer would not be needed, but only if the own lawyer is subject to the investigation. In other cases or specific circumstances, the cloud provider might have to keep secrecy in order not interfere with a criminal investigation if this is referred to the lawyer.
United Kingdom	No. The essence of all the regimes under which access to privileged data is permitted is that no notice is given to the person whose communications are intercepted or whose communications data are accessed.
4. May the government monitor electronic communications of lawyers sent through the systems of a Cloud provider?	
Andorra	Normalement, non
Austria	Only, the object of the investigation is a criminal misconduct of the lawyer and a court

	order exists for this measure.
Belgium	Yes, this is the procedure under Article 90ter as described above; a similar measure is provided under national security law.
Czech Republic	See last part of answer n. 1.
Denmark	Yes
France	Là encore, il convient de transposer la règlementation applicable aux écoutes téléphoniques des cabinets. Les communications de l'avocat ne peuvent être surveillées que s'il existe contre lui des indices de participation à une infraction. Le juge qui autorise, de manière motivée (existence d'indices de participation de l'avocat à une infraction), la mise sur écoute du cabinet d'avocat doit en informer le Bâtonnier et s'assurer que le secret professionnel sera garanti et que cette mise sur écoute ne compromettra pas l'exercice de son activité. Le recours à des prestataires informatiques externalisés, à fortiori en mode cloud computing, présente des spécificités qui nécessiteraient de bâtir un régime de protection du secret professionnel similaire de celui qui existe en matière d'écoutes téléphonique.
Finland	If the lawyer is suspected in some serious crimes, then the goverment (police) may monitor electronic communications. The government needs a court order for monitoring.
Germany	Yes. Again, as an example, § 20 (k) of the BKA Act allows monitoring for periods of three months. At their expiry, an extension of periods of three months may be ordered. The law does not provide for a maximum number of extensions
Hungary	Yes, please see answer 1. For more details see also below, Annex III
Ireland	There are no specific laws concerning government monitoring of electronic communications sent through the systems of a CP. The doctrine of legal professional privilege significantly limits the extent to which the Irish Government can monitor lawyers' communications.
Italy	The Italian government cannot monitor electronic communications of lawyers sent through the systems of a Cloud provider when such communications are exchanges between lawyer and client covered by confidentiality.
Norway	No
Poland	**Bar Council** No. The procedure of requesting data is presented in point 1 above.
	The National Council of Legal Advisers The government cannot monitor electronic communication if there isn't any court order or warrant.
Slovak Repunblic	Yes THE CONSTITUTIONAL ACT on the security of the state in time of war, warfare, exceptional or emergency state Possibility to limit the privacy of letters and secrecy of mailed messages. CRIMINAL PROCEEDINGS – Code on the Criminal Proceedings

Section 115

Interception and recording of telecommunications

(1) Where criminal proceedings are conducted in respect of a felony, corruption, criminal offence of the abuse of power of public official, criminal offence of laundering the proceeds of crime, or in respect of an intentional criminal offence where so provided by a promulgated international treaty, it shall be possible to issue an order to intercept and record telecommunications if there are reasonable grounds to believe that it will reveal the facts that are materially relevant for criminal proceedings. Where, in the course of intercepting and recording telecommunications, the accused is found to be in communication with his defence counsel, no information thus obtained may be used for the purposes of criminal proceedings, and any such information must be forthwith destroyed in a prescribed manner; this shall not apply to information relating to a case in which a lawyer does not represent the accused as his defence counsel.

(2) The order to intercept and record telecommunications shall be issued by the presiding judge of a panel prior to the commencement of criminal prosecution, or by a judge for pre-trial proceedings on a motion from a prosecutor. If the matter bears no delay and a prior order from a judge for pre-trial proceedings cannot be obtained, the order may be issued by a prosecutor before the commencement of criminal prosecution or in pre-trial proceedings, unless the interception and recording of telecommunications involves the entry into the dwelling of a person; such order shall have to be confirmed by a judge for pre-trial proceedings within 24 hours of its issuance; failing that, the order shall become null and void and the information obtained on its basis may not be used for the purposes of criminal proceedings and shall have to be immediately destroyed in a prescribed manner.

(3) The order to intercept and record telecommunications shall have to be in writing and based on circumstantial reasons, separately for each telephone subscriber or technical equipment. The order shall have to specify the telephone subscriber or technical equipment and, if known, the person whose telecommunications are intercepted and recorded, and the length of time during which the interception and recording of telecommunications are to be performed. Interception and recording may not exceed six months. This period may by extended by another two months, also repeatedly, on a motion from a prosecutor or a judge for pre-trial proceedings. Interception and recording of telecommunications operations shall be performed by the competent department of the Police Corps.

(5) In criminal proceedings conducted in respect of an intentional criminal offence which is different from the one referred to in paragraph 1, the order to intercept and record telecommunications may be issued by the presiding judge of a panel or, prior to the commencement of prosecution or in pre-trial proceedings, by a judge for pre-trial proceedings acting on a motion from a prosecutor, but only with the consent of the subscriber to the telecommunication equipment subjected to interception or recording.

(9) The provisions of paragraphs 1 to 8 shall apply, as appropriate, to the content data or operational data transmitted in real time via computer systems.

Section 116

(1) In criminal proceedings held in respect of an intentional criminal offence, it will be possible to issue an order for the disclosure and provision of telecommunications data that are subject to telecommunications secrecy or enjoy personal data protection, if such data are necessary to clarify the facts relevant for criminal

	proceedings. (2) The order to disclose and provide telecommunications data shall be issued in writing by the presiding judge of a panel prior to the commencement of criminal prosecution, or by a judge for pre-trial proceedings on a motion from a prosecutor in pre-trial proceedings, which must be based on circumstantial reasons; the order shall be served on the persons referred to in paragraph 3. (3) Legal entities or individuals carrying out telecommunications activities shall notify the presiding judge of a panel, or, in pre-trial proceedings, a prosecutor or a police officer about effected telecommunications. (4) The provisions of paragraphs 1 to 3 shall apply, as appropriate, to the content data or operational data transmitted in real time via computer systems.
Slovenia	Yes, under certain conditions (if a person is suspected of • having committed a certain crime, • preparing to commit it or c • omitting it and if there is reasonable cause for suspicion that certain communication tools are/have been/will be used for communications related to such a crime and other measures would not be appropriate to collect evidence or collection of evidence could threaten life and/or health of people, then monitoring of electronic communications, monitoring of IT system used by a person engaged in financial or other business activities etc. may be ordered by the court.)
Sweden	No
Spain	The government may not monitor lawyers'electronic communications sent through the systems of a Cloud provider unless there is a judicial authorization to do so according to the Constitution and the applicable legislation. Such guarantees are provided in article 18(3) of the Spanish Constitution. Also, it is necessary to take into consideration the above mentioned laws, such as the telecommunications, e-commerce and criminal procedure laws.
United Kingdom	Please see the position regarding interception on the continuation sheet.
5. Are government orders to disclose lawyers' data subject to review by a judge?[12]	
Andorra	Premièrement le Gouvernement ne peut pas faire cela mais s'ils le font il est évident qu'il faudrait le contrôle du juge.
Austria	Yes, see above.
Belgium	Yes, such orders can only be provided in criminal investigations by judges in advance, either a juge d'instruction/onderzoeksrechter, or a Procureur du Roi/Procureur des Konings. In national security investigations, the orders are given by a special Committee. The three members of this Committee are magistrates, one of which is a public prosecutor, and the other two are judges. There is a separate committee (the Permanent Committee) that conducts a posteriori checks of all ordered measures.
Czech Republic	Yes. In general, wire taping, home searches etc. have to be approved by a judge. Search of lawyer's premises has even stricter regime – see above, but this regime is not applicable to lawyer's client cloud data.
Denmark	Yes
France	Les règles qui s'appliquent sont les règles générales relatives aux recours contre les poursuites et les enquêtes (appel devant la Chambre de l'instruction ou exception de

12 "Review by a judge" encompasses either an initial review when issuing the court order, warrant, etc. or subsequent review when the court order, warrant, etc. is challenged by the service provider or customer.

	nullité). Plus exactement, le « Gouvernement » ne dispose pas de pouvoir particulier.
Finland	No, they are not. The head of the investigation (usually a police officer) can give the orders to disclose data.
Germany	Yes. To our knowledge, at Länder level as well as at federal level, the corresponding laws do provide for review by a judge. As a rule, the judge's decision has to be obtained before, in special cases (especially in urgent cases), after the intervention.
Hungary	It depends on the nature of the order. If it affects any content of a communication, it is. For more details see answer 1 and below, Annex III
Ireland	Yes
Italy	Yes, they are.
Norway	Yes
Poland	**Bar Council** Yes. As mentioned above, the decision on requesting data from the service providers may be issued by the court or the public prosecutor. If it is issued by the public prosecutor, it may be appealed against to the court.
	The National Council of Legal Advisers Lawyers' data can be disclosed only by court order or warrant.
Slovak Repyblic	- CRIMINAL PROCEEDINGS Initial review – in most cases yes as the order is issued by the judge for pre-trial proceedings or the presiding judge Subsequent review – no, the Code on Criminal Proceedings does not allow for the remedy against an order. If data were collected illegally, as a consequence it is not allowed to use the data as evidence in the criminal proceedings. - ADMINISTRATIVE PROCEEDINGS Subsequent review – yes, if final decision of an administrative body is contested under the Fifth Part of the Code on Civil Proceedings (Administrative Justice): administrative court may cancel the contested decision if an error occurred in the original proceeding which is able to influence legality of the contested decision.
Slovenia	Yes.
Sweden	Yes. If a question of disclosure would arise, such disclosure could never occur without a judicial examination. Thus, it would be up to the judicial authorities, and more precise, the court and a judge, who will have to decide on the issue of disclosure.
Spain	In any case, disclosing of lawyers' data is subject to review by a judge. Orders to disclose lawyers' data might be subject to judicial authorization, depending on the case. Such judicial authorization or order is a requisite and therefore governmental orders to disclose lawyers´ data are subject to review by a judge according to the meaning of such review provided by CCBE (footnote number 1). On the other hand, according to article 116 of the Constitution and Law on the Administrative Contentious Procedure , all the governmental activity (including administrative acts regarding data requests) is subject to control by the Courts. And law enforcement authorities are also subject to the control by Courts according to article 116 of the Constitution. In all cases, it is necessary to guarantee fundamental

	rights.
United Kingdom	Any application for a warrant or order under PACE is considered by a judge, who would be in a position to identify any improper request to seize privileged material. If privileged material were nevertheless wrongfully seized under these powers, an application could be made to the ordinary courts for its return and non-disclosure. There is no judicial involvement in the warrantry and authorisation processes under RIPA or the Intelligence Services Act. Where data have been accessed under RIPA or the Intelligence Services Act, a subsequent review may be undertaken by a specialist tribunal, the Investigatory Powers Tribunal ("IPT"). The IPT includes members of the senior judiciary but conducts its investigation into the facts in secret. Because the authorities do not give notice of the exercise of their powers, even after the event, the right to complain to the Tribunal is considered to be of limited value.
6. If a Cloud provider stores lawyers' data on servers in another country, can the government require the Cloud provider to access and disclose that data?	
Andorra	Non
Austria	Yes, by the way of judicial assistance (if the relevant international treaties are in effect).
Belgium	Yes, there are specific rules in relation to network searches in Article 88ter of the Code. These allow the juge d'instruction/onderzoeksrechter to extend any search of a computer system to any other computer system in another location if this extension is necessary to reveal the truth in relation to the crime under investigation, and if any other measures would be disproportionate or risk losing elements of evidence (i.e. the extension is seen by the lawmaker as a measure of last resort). Extensions must be limited to those systems that would have been accessible to the persons using the original computer system (i.e. it does not permit breaking into third party systems). Extensions to systems in other countries are permitted, but require the judge to immediately inform the Ministry of Justice, so that it may inform the government of the State(s) concerned, if these can reasonably be identified.
Czech Republic	We are not aware of any other than technical limits, which are apparently not an issue in the Cloud system networks.
Denmark	No
France	Non, les règles précitées – applicables en France - ont vocation à s'appliquer. Il convient de rappeler que la Loi Informatiques et Libertés interdit de transférer des données vers des pays n'offrant pas un niveau de sécurité adéquat. Les Etats Unis, notamment, sont considérés par la CNIL comme n'offrant pas les garanties suffisantes[13], comme cela apparaît sur la carte fournie par la CNIL.[14] Par ailleurs, la saisie de données d'un cabinet d'avocat impliquant des clients qui seraient stockées à l'étranger tombe sous le coup des mêmes règles de protection,

[13] Article 68 Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : « *Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un Etat n'appartenant pas à la Communauté européenne que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet.*

Le caractère suffisant du niveau de protection assuré par un Etat s'apprécie en fonction notamment des dispositions en vigueur dans cet Etat, des mesures de sécurité qui y sont appliquées, des caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées. »

[14] http://www.cnil.fr/linstitution/international/les-autorites-de-controle-dans-le-monde/.

	dès lors qu'il s'agit d'un avocat français et que c'est l'exploitation en France de ces données qui serait faite. On peut ainsi valablement soutenir que le secret professionnel est une règle d'Ordre public de protection internationale, par conséquent, s'imposant à tous. Donc quelle que soit l'autorité qui demande la communication de données, la procédure particulière de la perquisition dans un cabinet d'avocats doit s'appliquer pour garantir le respect du secret professionnel. Or, un facteur de complexité peut éventuellement résider dans la mise en œuvre par le Gouvernement de mécanismes d'entre-aide avec d'autres Etats (Ex : en matière fiscale) qui peut engendrer l'obtention à l'étranger d'informations couvertes par le secret professionnel applicable à un avocat établi en France.
Finland	Yes. The government may require passwords etc. to get access to the targeted data.
Germany	No. To our knowledge, service providers are under no obligation to "call back" data from abroad (an exception is provided under § 4 of the Ordinance concerning the Technical and Organisational Implementation of Measures for the Interception of Telecommunications (Telekommunikations-Überwachungsverordnung – TKÜV) for cases where data is diverted or forwarded within Germany).
Hungary	It can require, but if the Cloud provider is technically not able to provide those data, the Cloud provider may not be fined or be subject to other sanctions. Hungarian authorities generally have jurisdiction over entities that are established or are present in Hungary. As mentioned above, section 71 para. 7 of the Criminal Procedure Act, and section 26 para. 4 of the Administrative Proceeding Act merely state that data provision can be rejected in case it would infringe applicable law, but not "any foreign applicable law". There is no specific provision for cases when the data is stored by e.g. a Hungarian entity in a foreign country; the company itself will be responsible for data provision, and to resolve its availability. Therefore, it can be concluded that in case Hungary has jurisdiction over a Cloud Service provider, it may require that entity to provide data, an impose sanctions on it in case of refusal, regardless of the grounds. However, Hungary does not have direct enforcement rights in other jurisdictions; therefore it cannot directly seize and recover data from a foreign server. To actually enforce data provision from a foreign server, the Hungarian authorities would need to engage the given foreign authority within the frames of legal aid or reciprocity to carry out such investigative actions abroad.
Ireland	The doctrine of legal professional privilege significantly limits the extent to which the Irish Government can access or disclose lawyers' data.
Italy	Yes, the government can require the Italian Cloud provider to access and disclose data stored abroad, but it is not allowed (see above) when such communications are exchanges between lawyer and client covered by confidentiality.
Norway	No, same rules as described above apply. Cross boarder situations may bring up the issue of protection of individuals and the processing of personal data.
Poland	**Bar Council** Yes, if the service provider provides services in Poland.
	The National Council of Legal Advisers As in the first question, Cloud provider cannot disclose that data.

Slovak Republic	ACT NO. 22/2004 COLL. ON ELECTRONIC COMMERCE **Sec. 3** (4) Services provider who provides information society services from another Member State shall be liable to law of the Member State in which his registered office is located. Services provider who provides information society services from another Member State shall be liable to law of the Slovak Republic in the matters of state security protection, public order protection, public health protection, environment protection and consumer protection. (Note: Statutory definition of information society services provider reads as follows: information society services provider is an individual or legal entity which provides information society services; if the provider is an entrepreneur, location of electronic devices necessary for providing information society services is not a determinant of registered office or place of business.) => YES
Slovenia	Not regulated.
Sweden	No, the same rules normally apply. In some cases, however, such cross-border situations bring up the issue of protection of individuals and the processing of personal data (see directive 95/46/EC). Especially in relation to countries outside the European union, a number of difficulties can arise, depending of the security level for electronic data of the individual state and the use of standard-form contract clauses, etc.
Spain	The government might do that in case that the cloud provider is incorporated in Spain. In that case, it would be necessary to follow the procedural rules and take into consideration the fundamental rights involved, as explained before.
United Kingdom	The powers under RIPA extend to communications into or out of the UK, so (a) data carried to or from servers outside the UK could be intercepted during its passage over a UK-based telecommunications system, and (b) a UK-based service provider could be required to provide communications data about such communications.

SUPPLEMENTARY QUESTIONNAIRE

November 2013[15]

1. **Andorra**
2. **Austria**
3. **Czech Republic**
4. **Denmark**
5. **Finland**
6. **Germany**
7. **Hungary**
8. **Ireland**
9. **Italy**
10. **Norway**
11. **Slovak Republic**
12. **Slovenia**
13. **Spain**
14. **Sweden**

a) The Structures of Regulation:

In most jurisdictions, there is a general legal framework governing access by the state to electronic data. Against this background, there are two principal models of regulation of governmental access to lawyers' data.

> ***Model A: The general regulatory regime is applied, but with exceptions or protections for lawyers (either uniquely or, to some extent in common with other professionals). These may be either legislative/regulatory or arise at common law, for example in asserting the common law privilege attaching to lawyer/client communication.***
>
> ***Model B: There is a special legislative/regulatory regime applying to lawyers.***

A1 Which is the Model of which applies in your Member State? If neither, is some other model used?

Andorra	Modèle B
Austria	Model A

[15] Certain key issues emerged from an analysis of the answers to the original questionnaire sent out to delegations earlier. In order to enable the CCBE to complete a report which properly identifies areas for concern and recommendations for return, it has been decided to issue this Supplementary Questionnaire. The second questionnaire was circulated to national delegations on 22 November 2013.

Czech Republic	Model A
Denmark	Model A
Finland	Model A
Germany	Model A
Hungary	Model A
Ireland	Model A
Italy	Model A
Norway	The confidentiality in a lawyer and client relationship is protected in Norwegian law and practice. Exceptions require clear legislation or client approval. The main regulations on confidentiality are the following: • A lawyer cannot reveal any secrecies being entrusted him in performing his legal services. Breach of the obligation to keep information secret is punished with fine or prison up to 6 months. (Straffeloven § 144 first paragraph). Same regulation apply to certain other specifically listed professions such as for example priests, doctors, psychologists, nurses. • A lawyer is banned from revealing evidence in civil and criminal cases (Tvisteloven§22-5 and Straffeprosessloven § 119) although the main rule is that witnesses have the obligation to explain themselves in all matters in civil and criminal cases. Same ban regulation apply to certain other specifically listed professions such as priests, doctors, psykologists, nurses. • A lawyer has the obligation to handle information being entrusted to him in his profession as a lawyer with discretion even if the information is not comprised by the confidentiality restrictions set out in law. (Set out in regulation Norwegian Code of Conduct for lawyers article 2.3.2) • A lawyer is bound by the general Norwegian data protection regulations. There are exceptions to the lawyers confidentiality restrictions mainly the following: • Money laundering and the obligation to report suspicion of transactions having a link to certain crime (Hvitvaskingsloven § 18 first paragraph and §2 no 1 and 2) • Norwegian law firms may be subject to tax audit by the authorities. In such cases, there will be a duty to provide information that may affect the law firm's accounting or tax assessment, cf. the Norwegian Act relating to Value Added Tax section 16-1 (1). The duty to submit data applies without regard to the professional secrecy, cf. the Norwegian Act relating to Value Added Tax section 16-1 (3). This means that documents containing sensitive information, such as the client's name/VAT number and the billed amount, in certain circumstances may be required in order to fulfil the purpose of the tax audit. • Seek to prevent certain illegal offenses at a point in time when it possible to prevent them(Straffeloven 139) • When conditions for using legal necessity regulations are fulfilled

	There are exceptions from the evidence ban mainly the following: • Same as the above exceptions from the confidentiality restrictions • Evidence that can prevent somebody from being sentenced unlawfully(Straffeprosessloven § 119 third paragraph) • Documentation/ data containing confidences between persons suspected of being an accomplice in the criminal matter (Straffeprosessloven § 204). This does however not repeal the lawyer from his confidentiality obligation. A lawyer may object against the ban in full or in part. The documentation/data claimed to be banned unlawfully shall be delivered to and kept in escrow by the court unavailable for everyone except the court and the lawyer. If the court finds that the banned documents in full or in part does not fulfill the requirements to be banned, these documents cannot be revealed to the prosecutors, but will have to be returned to the lawyer.
Slovak Republic	Model A: general legal framework with the exception for lawyers, who are obliged to comply with the statutory duty of confidentiality under the Act on the Legal Profession
Slovenia	Model A
Spain	Model A[16]
Sweden	Model A
b) The Regime Governing the collection of Data:	
A2 Who may seek access to Lawyer's data?	
Andorra	Seul le juge compétent et dûment saisi peut permettre cet accès.
Austria	The public prosecutor and the criminal investigation department can take actions during investigation proceedings (e.g. confiscation § 110 Code of Criminal Procedure, sequestration § 115 Code of Criminal Procedure). During investigation proceedings they can also seek access to Lawyer's data.
Czech Republic	The issue here is that the cloud service provider is presumably not aware of the nature of the data and the law protects the lawyer from providing the client's data, not the data itself. The cloud provider can be requested by any authority eligible to do so by law (e.g. police in criminal proceedings, intelligence – see previous questionnaire, the court in a civil proceedings).
Denmark	The authorities (i.e. the prosecution and the police) can seek access to lawyers' data based on suspicions regarding a particular client or the lawyer him/herself. This would require a court order. Communications between a criminal defence lawyer and his/her client remains confidential, see also further below.
Finland	According to the Finnish Coercive Measures Act (806/2011) preliminary investigation authorities may seek access to a lawyer's data (for example by means of document seizure and search of premises) if there is a reason to suspect that a serious offence has been committed. What is regulated regarding document seizure applies also to data.
Germany	This depends on the kind of proceedings the lawyer is in. In the framework of criminal investigation proceedings, the criminal courts, the public prosecutors' offices and the police may seek access to a lawyer's data. In civil or administrative proceedings, the civil courts as well as public authorities

[16] All translations are unofficial

	might be interested in a lawyer's data. In addition, providers, clients, IT service providers and a lawyer's staff may seek access to the data.
Hungary	**Criminal proceedings:** investigative bodies (police, customs authority), prosecutor, court. [But no documents may be seized in the possession of the lawyer at its official premises that are written communications between the accused and its defense attorney, and that are lawyer's files related to the defense.] **Civil proceedings:** court (under witness testimony). [But no client information may be disclosed unless the client has given prior consent.] **Administrative proceedings:** a special class of administrative body (agencies) called "authority". [No witness testimony may be given and no documents may be seized under administrative law that contain professional secret, unless the client has given its prior approval.]
Ireland	Access may be sought by relevant government bodies or agencies on foot of statutory entitlements or, more generally, by way of court order. Access could be denied or reviewed by the Courts. All access requests would be subject to a lawyer's duties in relation to (a) client confidentiality, (b) data protection and (c) legal professional privilege.
Italy	Prosecutor
Norway	In principle nobody can without the approval of the client seek access to lawyers data as far as these are covered by the confidentiality restrictions. See Question A1 above.
Slovak Republic	**Criminal proceedings:** investigative bodies, prosecutor, court **Civil proceedings:** court **Administrative proceedings:** administrative body (as specified in separate laws)
Slovenia	According to the Criminal Procedure Act (if a lawyer is a suspect): The investigating judge may, at the request of the public prosecutor adducing reasonable grounds, • order the operator of the electronic communications network to furnish him with information on the participants in and the circumstances and facts of electronic communications. • order the monitoring of electronic communications using listening and recording devices and the control and protection of evidence on all forms of communication transmitted over the electronic communications network in case of suspecting that a particular person has committed, is committing or is preparing or organising the commission of any of the criminal offences referred to in the second paragraph of Article 150 of Criminal Procedure Act, and if there exists a reasonable suspicion that such person is using for communications in connection with this criminal offence a particular means of communication or computer system or that such means or system will be used, wherein it is possible to reasonably conclude that other measures will not enable the gathering of data or that the gathering of data could endanger the lives or health of people.

Spain	Lawyer's data may be sought in the context of: 1. Police investigations (law enforcement request for administrative purposes): Article 22 of the Organic Law 15/1999 on Data Protection applies. 2. Criminal investigations according to article 579 of the Criminal Procedure Law 3. National Security Agency investigations: Organic Law 2/2002 applies.
Sweden	Anyone may seek access; the question is whether the request will be honoured. In reality, however, it is only the prosecuting authorities (and the police) who can seek access to lawyers' data, either because of suspicions related to a certain client or suspicions related to the lawyer him/her self. The main rule is that lawyers' data is confidential and the confidentiality is protected by law (the Swedish Code of Judicial Procedure, e.g. Chapter 8, Section 4, Chapter 27, Section 2, Chapter 36, Section 5 and Chapter 38, Section 2). Access can only be granted by a court under very special circumstances (see item A4 below) and only such information which is directly linked to the decision of seizure (i.e. directly connected with the suspicions). Surplus of information may not be accessed and can not be used as evidence.
A3 Is prior permission required?	
Andorra	Oui, une autorisation du juge.
Austria	In principal confiscation can only be executed by order of the public prosecutor or the criminal investigation department (under certain circumstances enumerated in § 110 Code of Criminal Procedure the criminal investigation department can take measures without such order). In the case of sequestration, the court decides on it.
Czech Republic	We are not aware of any particular case that would include such a request, but the Criminal proceedings authorities' request could be refused if it the requested person is privileged of confidentiality by law, but there are some exceptions and the privilege can be breached by a prior court order. See in Annex VI the relevant Article of the Criminal proceedings Code. This rule concerns providing data for the Criminal proceedings in general. Intelligence can seek the data according to a prior High court order – the law does not stipulate any limitation as to the data privilege. The court in civil proceedings can request the data and the cloud provider could refuse only if the provider would cause a risk of a criminal prosecution to him or his relatives (also directors if the provider would be a company). Also other confidentiality (privileged by law), e.g. lawyer's, would be respected.
Denmark	Yes, court order. In certain situations it is also possible to search data without a court order, if there is a risk the data will otherwise disappear – but it happens rarely and a court order with retroactive effect must be obtained immediately thereafter.
Finland	A district court's decision is required if a lawyer's premises will be subject to a search. Additionally the court has to appoint an agent to supervise the search.
Germany	A prior permission is required, which is usually issued by the local court (Amtsgericht) that has jurisdiction in the court district where the lawyer's premises are located. As an exception to this rule, the Public Prosecutor and police may act without a judge's permission in exigent circumstances („Gefahr im Verzug") § 98 (1) StPO (Code of Criminal Procedure, Strafprozessordnung). If a seizure takes place without a court order, the permission has to be obtained within 3 days, if the lawyer concerned was not present during the seizure or objected to it. The lawyer concerned may at any time apply for a court decision.
Hungary	**Criminal proceedings:** investigative bodies (police, customs authority), prosecutor,

	court. [But no documents may be seized in the possession of the lawyer at its official premises that are written communications between the accused and its defense attorney, and that are lawyer's files related to the defense.] **Civil proceedings:** court (under witness testimony). [But no client information may be disclosed unless the client has given prior consent.] **Administrative proceedings:** a special class of administrative body (agencies) called "authority". [No witness testimony may be given and no documents may be seized under administrative law that contain professional secret, unless the client has given its prior approval.]
Ireland	Any legitimate access to a lawyer's data would require the permission of the lawyer and/or his/her client in the absence of very limited statutory access obligations or an order of the Courts.
Italy	Yes, of judicial authority
Norway	Client approval will be required to access lawyers confidential information.
Slovak Republic	**Data stored by the lawyer – YES:** such data is covered by the professional secrecy therefore prior approval of a client is necessary **Data stored by IT service provider – NO**: he is not protected by the professional secrecy therefore he is obliged to comply with state authorities` orders or requests.
Slovenia	Yes
Spain	In Criminal and National Security Agency investigations in order to disclose lawyers' data it is needed authorization by a reasoned judicial order or Authorization of the designated Magistrate of the Supreme Court. In police investigations it is not needed authorization by judicial order if the access is to a lawyer's data exclusively, not to clients' data, and additionally: 1. It is in the context of an investigation where the subject of this investigation is the lawyer itself and 2.there is a real threat for the public safety or the suppression of crime. These cases have been narrowly interpreted by the Spanish Data Protection Agency (DPA). Allowing governmental access to lawyer's data through a Cloud provider without the required guarantees would mean circumvent the constitutional (art 18.3 and 24.2 Spanish Constitution) and legal protection already set, such as the secrecy of communications, legal guarantees and the right and duty of professional (Organic Law of the Judiciary Power and General By-Law of the Spanish Lawyers)
Sweden	Yes, in principal there need to be a court order permitting access of certain documents (seizure).
A4 What conditions must be satisfied to obtain access?	
Andorra	La demande judiciaire adressée au juge doit contenir tous les éléments nécessaires à la levée du secret professionnel, ce que le juge appréciera librement.
Austria	Prerequisite is an investigation proceeding. The public prosecutor decides on its initiation, progress and cessation (§ 101 (1) Code of Criminal Procedure). In accordance with § 9 (2) Lawyers Act the lawyer is bound to professional secrecy as regards the information entrusted to him by his clients. In principle, this right of the lawyer may not be circumvented by judicial or other authority measures (§ 9 (3) Lawyers Act). § 157 Code of Criminal Procedure enumerates persons who have the right not to testify in a procedure – lawyers are included. The Code of Criminal Procedure says that it is forbidden to ignore this right just by confiscating documents or interrogating judicial employees.

Czech Republic	See above
Denmark	The conditions that need to be fulfilled in order of the police to conduct a search can be found in the Administration of Justice Act (AJA) chapter 73. The rules governing seizure and disclosure can be found in AJA chapter 74. If the lawyer isn't a suspect him/herself, searches of dwellings, other premises or objects (including documents) may only take place if the investigation concerns an offence which under the law can result in imprisonment and there are specific reasons to presume that evidence in the case or objects, which can be seized, can be found by the search. As for the possessions of persons, who are excluded from giving testimony as witnesses in the case (incl. lawyers), written messages and similar between the suspect and the lawyer, as well as notes, are not subject to search. Seizure can take place to secure evidence; to secure the claim of the State for costs, confiscation or compensation; to secure the claim of the victim for restoration or compensation; when the defendant has absconded from further prosecution of the case. Objects, of which a person, who is not a suspect (i.e. the lawyer), has possession, can be seized as part of the investigation of an offence, which is prosecuted by the State, if there is reason to presume that the object can serve as evidence, should be confiscated or by the offence has been purloined from someone who can claim it back. As with the rules reg searches, possessions of persons who are excluded from testifying as witnesses in the case (i.e. the lawyer), written messages between the suspect and the lawyer are not subject to seizure.
Finland	There has to be a reason to suspect that a serious offence has been committed and that a document subject to a seizure may serve as evidence in criminal proceedings.
Germany	Access is prohibited if the measures concern client data and the lawyer is not suspected of an offence, aiding the perpetration of an offence, obstruction of justice or receiving and handling stolen goods (§ 160a Abs. 4 StPO). The provider will be granted access, provided he is employed by the lawyer, has signed a confidentiality agreement, and provided the client has agreed to data storage by a third party.
Hungary	See A3 above, plus the information below. Secret information gathering can only be carried out in certain cases. In relation to criminal procedure, these are crimes punishable by 5 years or more of confinement, or crimes of special relevance (where narcotics or state secrets are involved, or where corruption or similar crimes punishable by 3 years or more of confinement are involved etc.) The same secret information gathering can be carried out by national security services in carrying out certain national security tasks, but there are no further statutory limitations in this regard as to the cause of using such powers. In both criminal and national security cases, a prior approval by a judge is required. In carrying out certain national security tasks, the prior approval is given by the minister of justice.
Ireland	As per A3 above. All access requests would also have to take account of legal professional privilege.
Italy	A lawyer must be accused of commission of a crime
Norway	Client approval or in case of banned documents see section A 1 above.
Slovak Republic	**Criminal proceedings:** 1. STORAGE AND RECOVERY OF COMPUTER DATA (*Sec. 90 of the Code on Criminal Proceedings*):

	An order may be issued only if obtaining access to saved computer data is essential in order to clarify facts significant for criminal proceedings. 2. COMPARISON OF DATA IN DIFFERENT COMPUTER SYSTEMS (*Sec. 118 of the Code on Criminal Proceedings*): Such comparison may be carried out if necessary for clarification of a crime within criminal proceedings on deliberate criminal offence liable to a sentence of imprisonment with the maximum term exceeding 3 years / on corruption / on any other deliberate criminal offence if such proceedings are to be conducted pursuant to a binding international treaty. **Civil and administrative proceedings:** No special conditions under the Code on Civil Proceedings / the Code on Administrative Proceedings.
Slovenia	If there are reasonable grounds for suspecting that a particular person - has committed, - is committing or is preparing or organising the commission of any of the criminal offences referred to in the second paragraph of this Article, and if there exists a reasonable suspicion that such person is using for communications in connection with this criminal offence a particular means of communication or computer system or that such means or system will be used, wherein it is possible to reasonably conclude that other measures will not enable the gathering of data or that the gathering of data could endanger the lives or health of people, the following may be ordered against such person: 1) the monitoring of electronic communications using listening and recording devices and the control and protection of evidence on all forms of communication transmitted over the electronic communications network; 2) control of letters and other parcels; 3) control of the computer systems of banks or other legal entities which perform financial or other commercial activities; 4) listening to and recording of conversations with the permission of at least one person participating in the conversation. (2) The criminal offences in connection with which the measures referred to in the preceding paragraph may be ordered are the following: 1) criminal offences against the security of the Republic of Slovenia and its constitutional order, and crimes against humanity and international law for which the law prescribes a prison sentence of five or more years; 2) criminal offences of abduction (Article 144 of the Penal Code), the showing, possession, manufacture and distribution of pornographic material (Article 187), illicit narcotics production and trafficking (Article 196), facilitating of drug-taking (Article 197), blackmail (Article 218), abuse of inside information (Article 243), unauthorised acceptance of gifts (Article 247), unauthorised giving of gifts (Article

	248), money laundering (Article 252), smuggling (Article 255), accepting of a bribe (Article 267), giving of a bribe (Article 268), acceptance of gifts to secure unlawful intervention (Article 269), giving of gifts to secure unlawful intervention (Article 269.a), criminal association (Article 297), unauthorised production of and trade in arms or explosives (Article 310), and causing of danger with nuclear substances (third paragraph of Article 319); 3) other criminal offences for which the law prescribes a prison sentence of eight or more years.
Spain	In Criminal investigations and according to article 579 of the Criminal Procedure Law, interception of communications, in the course of a criminal investigation, requires two elements: • Reasons to believe that the interception may lead to finding or proving a fact circumstance relevant to a criminal procedure, and Authorization by a reasoned judicial order and cases of terrorism. The law regulates exceptions to secrecy in matters of terrorism or if there are grounds to believe on an involvement of the lawyer in the criminal acts (in fact, the lawyer is not acting as a lawyer). There is a judicial interpretation of the Constitutional Court that establishes that the two conditions are cumulative and not alternative. In other words, the only intervention of communications between a lawyer and a client with judicial validity during the criminal investigation is in the event there are incriminating grounds on the lawyer and when the crime under investigation is terrorism. Both are cumulative conditions. Therefore, a lawyer´s cloud provider could only disclose lawyers´ data to the government if these guarantees and conditions are met. Otherwise, such access would infringe fundamental rights and therefore would be illicit or illegal. And with regard to National Security Agency investigations, the Organic Law 2/2002 regulates the terms and conditions under which the National Intelligence Agency may intercept communications. Any interception of communications, as affects a fundamental right, would require authorization of the designated Magistrate of the Supreme Court.
Sweden	As regards seizure of documents at law firms and professional secrecy of advocates, the Swedish Supreme Court has decided upon seizure in law firms (Case nr Ö 2144-09, given 4 March 2010, referred in NJA 2010 p. 122). In this case question arose whether the seizure of documents in a law firm was subject to seizure ban. An advocate at the law firm was a suspect of a crime in his role as a representative of a company in which he, together with his partner, constituted the board. When the search of the law firm was carried out materials assignable to the company in question was seized. The decision was appealed. The Supreme Court initially found that a prerequisite for the seizure ban is that the document can be considered to have been entrusted with the advocate by the client in the advocate's professional capacity. The Court also found that, if the advocate is the legal representative of a company, documents entrusted to him relating to the company can be considered to be entrusted with the advocate in his professional capacity, if the company is the advocate's client. If this is considered to be the case, then the knowledge the advocate acquires from his client would be covered by the advocate's professional secrecy. The company in question had turned to the law firm with a request for assistance with ongoing legal matters and with the representation on the board of directors. The Court found that this was sufficient

	enough to consider it to be a client relationship and that the advocate was bound by his professional secrecy. The Prosecutor pleaded that the ban did not apply due to the fact that the ban only applies to the seizure of documents which contains contents of which the holder may not be called to give testimony. The Court found that the ban is intended to protect the client´s (and not the lawyer's) interests, not least when the client is suspected of a crime, and that there was no reason to make another assessment of this if the advocate was the suspect of a crime. A client's legitimate interest of confidentiality does not need to be less if his advocate is suspected of a crime, the Court stated. The provision thus applies and the documents were subject to the seizure ban. It is interesting to note that also the European Court of Human Rights recently has come to the same conclusion on client privilege protection and search/seizure at law firms. In the case of Robathin v. Austria (Application no. 30457/06, Judgement 3 July 2012) the Court found that Austria violated Art. 8 of the Convention by searching a lawyer's office and confiscating all documents being found within the lawyer's premises. The Court's decision strengthens the general principle of professional confidentiality of lawyers. It demonstrates quite clearly that the search and confiscation of a law firm's documents may only take place on a very limited scale and may only comprise documents and data related to a specific matter of investigative interest.
A5 How is permission obtained?	
Andorra	Dans le cadre d'une procédure judiciaire.
Austria	See answer to A3.
Czech Republic	See above
Denmark	By court order – both search and seizure.
Finland	Document seizure shall be decided by an official with the power of arrest or a court may decide a seizure during the trial. Special search of premises requires a court's decision. Additionally the court has to appoint an agent to supervise the search.
Germany	Only the public prosecutor's office may apply for a permission to search the premises.
Hungary	Permission for search and seizure has to be filed at the investigatory judge by the prosecution, the investigation authority or the national security service body involved. Permissions for secret information gathering are regulated in a lot more detail, including the content of request, and there is a special investigatory judge for such approvals (all such evidence becomes state secret and require special treatment including at the management of files). Such decisions have to be brought by the judge within 72 hours, use of secret information gathering methods may be approved for a period of 90 days which may be renewed as necessary.
Ireland	As per A3 above. Specific consent, statutory obligations or Court Order
Italy	An application must be filed during investigations
Norway	Client approval collected through his lawyer. Or decision by court in case of a claim that documents/data has been illegally banned.
Slovak Republic	**Criminal proceedings:** 1. STORAGE AND RECOVERY OF COMPUTER DATA: If obtaining access to saved computer data (including operational data) is essential in order to clarify facts significant for criminal proceedings,

	investigative bodies / prosecutor / court may ask for the order. After assessing the claim prosecutor / judge presiding to the tribunal may issue the order which - must be justified by factual circumstances - must state a period of time during which data storage shall be carried out, maximum period is 90 days (new order must be issued if more time is needed) 2. COMPARISON OF DATA IN DIFFERENT COMPUTER SYSTEMS: If comparison of data is necessary investigative bodies / prosecutor / court may ask for the order. After assessing the claim prosecutor / judge presiding to the tribunal may issue the order which shall contain identification of an obliged person (entity), identification of relevant data and information necessary to carry out the comparison.
Slovenia	By the investigating judge at the request of the public prosecutor adducing reasonable grounds.
Spain	Through a Judge in criminal investigations or Designated Magistrate (corresponds to Higher Judge in Spain) of the Supreme Court in National Security Agency investigations. In police investigations, when access is to lawyer´s data clients, then the lawyer´s professional secrecy does apply. Therefore the request to a cloud provider should be done through the lawyer as "owner of information" and in particular when the request involves personal data as the lawyers is the controller of such data. Differently, it would be if the access is to lawyer´s data as subject of the investigation, the cloud provider shall provide those data always that the conditions stated above (there is a real threat for the public safety or the suppression of crime) are met. There are yet needs to improve the regulation on issues such as the maximum delay of the intervention (no limit of number of prorrogations), limiting the type and seriousness of the alledged facts of the investigation on the lawyer. The ECHR on a decision rendered in 18th of february 2003 itself declared that the art. 579 LECrim does not fulfill the requirements related to the provision of an "ingérence legale". In the famous case against Baltazar Garzón for taping lawyers conversations the instructing judge established that: "en un Estado de Derecho el fin de la búsqueda de la verdad material no justifica cualquier medio". A translation would be: "Under the Rule of law, the aim of the search of a material truth does not justify all means".
Sweden	Court order – decision for seizure (and sometimes for search of premises).
A6 Is the lawyer or any other person (e.g. the client or Bar) informed?	
Andorra	L'avocat en sera informé, ainsi que le demandeur.
Austria	Before the search the lawyer has to be invited stating the relevant reasons to allow the search or to surrender freely the wanted item or data (§ 121 (1) Code of Criminal Procedure). The lawyer has the right to be present during the search (§ 121 (2) Code of Criminal Procedure). If an investigation proceeding against a lawyer is initiated, the disciplinary prosecutor of the competent local bar has to be informed (§ 24 Disciplinary Act). If a search warrant is executed at the lawyer's office, a representative of the competent local bar has to be present (§ 121 (2) Code of Criminal Procedure).
Czech	This is not regulated in case of cloud data. As an example - in criminal proceedings

Republic	– if a person had been wire tapped, but the wiretapping has not been used in criminal proceedings, then the person has to be informed about this fact (unless some exceptions apply). Note that wiretapping of a client (accused person) – lawyer telephone communication in a criminal proceedings is forbidden. We think that this rule does not govern the cloud data (transfer and storage).
Denmark	Main rule is yes, except where the lawyer him/herself is the suspect. The client is expected to be informed through the lawyer. However, there are also situations where it is deemed necessary that searches are conducted in secrecy, and then the lawyer nor the client is (naturally) informed immediately. The Bar is generally not informed, unless the lawyer him/herself provides the information.
Finland	If a lawyer/person, whose premises is a subject to a search, is not present during the search, he/she shall be notified without delay including a record of the search.
Germany	There is no prior notification of the lawyer or any other persons. After termination of the search, the lawyer has to be notified (§ 101 StPO).
Hungary	No.
Ireland	In any legitimate access to a lawyers data, the lawyer and/or his/her client must be informed.
Italy	Not necessarily; only in case of physical access
Norway	The lawyer and or the client shall be informed about evidence ban.
Slovak Republic	**Criminal proceedings:** The order must be addressed and delivered to a person in whose possession or under whose control such data are, or to a service provider of such services. By the same order they may be imposed the obligation of keeping in secret the measures contained in the order.
Slovenia	An investigation of the law office shall be permitted only subject to an ordinance of the competent court and only with reference to the records and objects explicitly stated in the ordinance of investigation. The investigation shall not affect the confidentiality of other documents and objects. Present at the investigation of the law office shall be a representative of the Bar Association of Slovenia. The representative of the BAS has no legal remedy at disposal.
Spain	If the request involves personal data in cases according to article 22(2) of the Organic Law 15/1999, considering that such communication of personal data to the law enforcement authority fulfils the requirements provided in such article or there is a judicial request, notification to the lawyer would not be needed, but only if the own lawyer is subject to the investigation. In other cases or specific circumstances, the cloud provider might have to keep secrecy in order not interfere with a criminal investigation if this is referred to the lawyer. Additionally, it may be relevant to bear in mind Art 32.2 General By-Law of the Spanish Lawyers in those cases where there is a register of the lawyer's office. It states "In case that the President of the Bar Association or who replaces him by statute were required by virtue of the legal rule or warned by the Judicial Power or governmental authority, competent for the register in a lawyer's office, he should appear in person to the diligences that take place in that office safeguarding the Legal Professional Privilege" Nevertheless, the legal profession pleads for further regulation. For instance, if there are grounds to believe that a lawyer is involved, the instructing judge should not

	allow a conference between him and his client without warning that the communications with the lawyer are no longer protected by professional secrecy.
Sweden	Yes, except in the very rare situation where the lawyer him/her self is suspected of a crime.
A7 Can a lawyer contest an order for recovery of data or seek assistance, for example, from his Bar?	
Andorra	Oui
Austria	N/A
Czech Republic	See A8
Denmark	Yes, a lawyer can contest a court order. The Danish Bar occasionally provides assistance in such matters if the situation regards fundamental issues, e.g. reg. lawyer/client confidentiality.
Finland	A lawyer is entitled to appeal on the decision concerning a document seizure and/or copying.
Germany	Yes, the lawyer may make a claim to recover data, if original data media were seized (§ 98b (3), first sentence, StPO). Yes, the lawyer may seek assistance from his Bar.
Hungary	For search and seizure, yes, the lawyer may contest the court order, but this will not delay the search and seizure. There is no such possibility for secret information gathering, as the lawyer (due to its secret nature) may not even be informed of it. (Of course, the lawyer may use the generic complaint procedure at the national security services or the police, but this is not effective.)
Ireland	Yes, a lawyer can contest an access request in the Courts (eg. by judicial review or by injunction proceedings. It would not be usual for the representative bodies (Law Society or Bar Council) to offer assistance in a specific case. However, both representative bodies would be concerned about the broad impact of data recovery and data access issues on their respective memberships.
Italy	Yes, there are judicial remedies
Norway	A lawyer can contest an order for recovery of data. The Norwegian Bar Association sometimes assist in specific cases. The Norwegian Bar Association also gives advice to its members on a general basis.
Slovak Republic	**Criminal proceedings:** No - if all conditions mentioned in A3 above are met including client`s prior consent. **Civil / administrative proceedings:** If a client released the lawyer from the duty of confidentiality, the lawyer is obliged to comply with the request to provide information.
Slovenia	Not provided by law! In an individual case by a complaint at court.
Spain	Yes
Sweden	Yes, a lawyer can contest a court order in order to recover data taken from his files. The Swedish Bar Association normally assist in such cases if the lawyer so requires and the Bar also gives formal statements and opinions on the legal issues of the data collection in the specific case, if the court has asked for the opinion of the Bar.
A8 Would the answer to any of the foregoing questions differ dipending on whether the data is stored in a lawyers' office or with an IT Services provider?	
Andorra	Non, cependant ce serait préférable.
Austria	N/A
Czech Republic	Yes, search of lawyers premises in criminal proceedings is governed by a special regime (e.g. a representative of the bar has to be present, the data will be sealed and handed over to the bar if the representative states that it includes client data and then the police has to apply to the court in order to receive the data).

Denmark	In principle no. The server and/or cloud is regarded an "extended office" for the lawyer, and the lawyer has the same obligations to ensure that data stored online/server/cloud is duly stored, as with data/case files kept physically at the lawyers' office. This is provided that the server is on Danish soil.
Finland	No, however the court's decision would not be directed at a service provider but a lawyer
Germany	Yes
Hungary	Yes, please see answer A3.
Ireland	In principle, no. In practical terms, a distinction must be drawn between data stored physically or virtually in a lawyer's office and data stored externally with a service provider. It is more difficult for a lawyer to be aware of any un-notified access to data stored externally.
Italy	In case of physical access it is necessary the presence of the President of the Bar where the lawyer is registered
Norway	No, not in principle. The obligation to keep information confidential follows the information/documentation. However when information is kept in outside storage with an IT service provider (or physical documents are stored outside)it is of major importance that there is a good legal framework between the lawyer and the outside storage provider including his suppliers in respect of ensuring that the lawyer confidentiality restrictions are understood and complied with by the provider and his suppliers .
Slovak Republic	Please see answer A3
Slovenia	No
Spain	It should not, as long as the provider knows that the information belongs to a professional relationship involving a lawyer or a legal matter.
Sweden	In principle no. The information is still confidential and belongs to the lawyer even if it is stored at an external IT-provider.
c) The use of Data once obtained	
A9 What happens to the data once obtained?	
Andorra	En principe, elles ne doivent être obtenues. Nous n'avons pas d'antécédent.
Austria	If the lawyer refers to his professional secrecy he can veto the confiscation. As a result the confiscated documents have to be sealed to prevent unauthorized access or alteration and have to be deposited at court (§ 112 (1) Code of Criminal Procedure). Within a reasonable, at least 14 days long, period the lawyer has to name those (parts of the) documents or data which disclosure would constitute a circumvention of his professional secrecy (§ 112 (2) Code of Criminal Procedure).
Czech Republic	In general - obtained data would be added to the file as evidence or returned if not used. Unused (i.e. not for evidence) wiretapping data should be stored by the police and protected from unauthorized use.
Denmark	Data obtained will be used in the further investigations and in possible court proceeding.
Finland	The data must be destroyed if it is unnecessary or if a court finds that it shall not be used as evidence.
Germany	Data must be deleted without delay once it is no longer required for the criminal proceedings (§ 98 (3), second sentence, StPO).
Hungary	This is regulated by the rules of evidence under criminal procedure. There are special rules for information gathered by secret information gathering powers, as these remain state secrets, and therefore the prosecution/investigation authority has to create a "report" of the results of secret information gathering, and generally, the report itself will be used only in the criminal procedure.
Ireland	If a lawyer's data has been legitimately accessed or obtained, it can be used only for

	the purpose for which it was sought.
Italy	It is used in investigations
Norway	Questions A 9, A 10 and A 11 Data obtained can as the main rule be used solely for the purpose for which it was originally collected provided the information is exempted from the confidentiality obligations and the evidence ban described under A1 above. Exemptions from the main rule requires clear law regulation. There are exemptions for example: Banned documentation can be handed to the tax authorities, even if it is qualified to fall within the lawyers confidentiality obligation, provided it is in the interest of the prosecutors to do so and further provided the information is used solely for the purpose of making a decision on a new tax assessment and additional tax (as a punishment). Information received by the prosecutors according to the regulations in the in respect of money laundering and illegal tax avoidance can be delivered to the tax authorities.
Slovak Republic	**Criminal proceedings:** Where there is no longer a need to store computer data, for the purposes of criminal proceedings, the presiding judge or the prosecutor (prior to the commencement of criminal prosecution or in pre-trial proceedings) shall issue an order reversing the obligation to store the data. The data carrier shall be returned and collected data destroyed.
Slovenia	If information is collected lawfully, then it can be used in court in an individual criminal case. If the state prosecutor declares that he will not commence criminal prosecution against a suspect, or if he does not issue such a declaration within two years of the end of application of the measures, the material from the preceding paragraph shall be destroyed under the supervision of the investigating judge. The investigating judge shall make an official note of the destruction. Before destruction the investigating judge shall inform the suspect of the use of these measures or the person against whom the measure was applied, who shall have the right to be informed of the material obtained.
Spain	If it is legally obtained it can be used in strict accordance with the law and the judicial order
Sweden	Data obtained according to law may be used in the way stated in law. Unlawful obtained data may not be used and would anyway have none or very little use as evidence.
A10 For example, can it be used in Court or other proceedings?	
Andorra	Nous n'avons pas d'antécédent.
Austria	The court has to make a decision whether the document may be used or not (§ 112 (2) Code of Criminal Procedure).
Czech Republic	Yes – provided it was obtained according to the law.
Denmark	See A9 above.
Finland	One of the prerequisites regarding seizure is that the document or data can be used as evidence in court proceedings which means that the data has to be used in the court proceedings.
Germany	Yes
Hungary	Yes, please see above A9.
Ireland	It can only be used for the specific Court proceedings for which it was accessed or

	obtained (assuming it is admissible in the proceedings).
Italy	Yes, of course (only if the proceeding has been correctly followed)
Norway	See above A9
Slovak Republic	**Criminal proceedings:** COMPARISON OF DATA IN DIFFERENT COMPUTER SYSTEMS: Yes, in this case it is possible, if the conditions in A4 are met, i.e. the other proceedings is also related to a criminal offence liable to a sentence of imprisonment with the maximum term exceeding 3 years / crime of corruption / any other deliberate criminal offence if such proceedings are to be conducted pursuant to a binding international treaty.
Slovenia	It can be used in court, if collected lawfully. If measures from Articles listed in Criminal Procedure Act were carried out without an order from an investigating judge, or in contravention of such an order, or if extension of application of the measures was not reviewed by the panel, the court may not base its decision on information, messages, recordings or evidence obtained in this manner.
Spain	The judge guarantees what part of the information may or may not be used. A decision failing to respect professional secrecy or the rights of defense can produce a sanction against the judge.
Sweden	See A9 above.
A11 Can it be used for other purposes than that for which it was originally collected?	
Andorra	Non
Austria	No. In accordance with § 112 (2) Code of Criminal Procedure it is forbidden to use those documents or data that has been excluded due to the veto mentioned in A9 for further investigative measures or as evidence.
Czech Republic	In general – yes, there is no special regime for cloud data. For example – wiretapping can be used in a different criminal case if in the other case wiretapping would also be possible (upper limit of a punishment at stake at least eight years of imprisonment or some other crimes).
Denmark	It depends. As a point of departure the material will be used in the case currently being dealt with, but naturally, if the search provides information about e.g. large scale tax fraud, the information will be passed on to the relevant authorities.
Finland	No.
Germany	Yes, but there is a highly complex and rather confusing regime governing the use and processing of data (§§ 98 (a) (1), 98 (c), 100 (a) (4), 100 (c) (4) to (7), 100 (d) (5) StPO). Data, the collection of which was only permitted under special conditions (e.g. telecommunication surveillance), may only be used again for the prosecution of other criminal offences, provided these offences would again allow the introduction of such an investigative measure.
Hungary	No, other than the following: if the data thus gathered contains evidence of a crime, the investigation authority will be able to initiate a new criminal procedure against the persons involved.
Ireland	In general, it cannot. See A.9 above
Italy	For other criminal proceedings
Norway	See above A9
Slovak Republic	**Criminal proceedings:** No
Slovenia	No.

	Information, messages, recordings or other evidence may not be used as evidence, if they were obtained by means of any of the measures from Articles listed in Criminal Procedure Act and they do not relate to any of the criminal offences for which an individual measure may be ordered.
Spain	The judicial mandate has to establish clear and strict conditions in respect with procedural and constitutional rights.
Sweden	In principle no. Documents obtained may only be used for the purpose upon which the decision for access was founded. Obtained documents cannot in general be used for any other purposes. Such information obtained together with the information searched (surplus of information) may not be used as evidence or in any other way. As has been stated above, search and seizure of a lawyer's documents may only take place on a very limited scale and may only comprise documents and data related to a specific matter of investigative interest.

ANNEX I – ADDITIONAL INFORMATION – FRANCE

Droit des technologies de l'information Réponse au questionnaire CCBE Accès par les autorités aux données des avocats en Cloud

Le cloud consiste à recourir à des prestataires de services aux fins d'externalisation des traitements des données soit en mode de sauvegarde, soit en mode de production (ex : traitement de texte, gestion d'agenda, contact, base clients …), soit les deux (cela n'est pas limitatif). Les lignes directrices du CCBE de septembre 2012 permettent de comprendre l'étendue de ces prestations pour les avocats.

Or, en l'état, il semble que les avocats de heurtent à un vide juridique concernant la protection de ces données stockées et gérées en cloud, ce qui constitue un risque majeur pour tous les cabinets d'avocats qui ont recours à de tels traitements. En effet, il devient indispensable de règlementer la question du transfert des données dans un lieu autre que le cabinet et assurer la protection du secret professionnel. L'enjeu est d'autant plus grand que les données du cabinet d'avocat sont susceptibles, chez le prestataire, d'être mutualisées au sein des mêmes moyens techniques que ceux d'une agence immobilière, d'une grande surface…

Ainsi, il est indispensable que l'avocat s'assure de ce que le contrat qui lie son cabinet au fournisseur de stockage en cloud ne souffre d'aucune faille dans la sécurité du stockage et que la confidentialité de ces données soit assurée efficacement, au besoin, en en faisant une condition déterminante du contrat et en mettant le fournisseur face à ses responsabilités en cas de fuites ou de violations du secret.

Force est de constater les instruments juridiques contractuels de niveau communautaire susceptibles d'apporter des garanties sont aujourd'hui insuffisantes. La Commission européenne a en effet adopté des Clauses contractuelles types[17] d'application obligatoire pour tout responsable de traitement, y compris pour les avocats, destinées à encadrer les transferts de données personnelles vers un pays situé hors UE aux fins d'externalisation de prestations de traitement dans le pays de destination vers des sous-traitants de données établis dans un Etat n'offrant pas un niveau de protection adéquat. En substance, ces clauses reposent sur les grands principes de la Directive européenne 95/46/CE sur la protection des données personnelles. Elles ont un champ d'application général et présentent des insuffisances au regard de l'exigence de protection du secret professionnel des avocats. Ces clauses permettent de préciser l'existence de données sensibles, mais pas au sens de celles qui seraient couvertes par un secret professionnel. Destinées à apporter aux autorités de contrôle en matière de protection des données personnelles la preuve des garanties adoptées au regard de la Directive précitée, les Clauses contractuelles types n'ont pas vocation à se substituer aux garanties contractuelles que doivent apporter les contrat de prestation de services éventuellement conclu entre l'avocat et son fournisseur de technologies.

Une réflexion concrète doit par conséquent être menée afin que soient pris en compte sous l'angle des contrats de prestation de service les enjeux de sécurité et de continuité de service soulignés par les Lignes directrices du CCBE.

[17] http://www.cnil.fr/linstitution/actualite/article/article/adoption-de-nouvelles-clauses-contractuelles-types-vers-une-meilleure-prise-en-compte-de-lexterna/

Des enjeux fondamentaux se posent au regard des exigences du secret professionnel lorsque l'avocat recourt à un prestataire de service externe. Cet enjeu prend une dimension complexe lorsque le prestataire de l'avocat se situe hors du pays de résidence de l'avocat. Indépendamment des éventuelles garanties qui pourraient être apportées à l'avocat lorsque son prestataire est situé hors de France mais au sein de l'Union Européenne, il convient de faire preuve de vigilance lorsque le prestataire se situe dans un pays soumis à des règles de droit d'ordre public qui résultent de la territorialité de ce prestataire. L'exemple des Etats-Unis d'Amérique est éloquent au regard notamment des procédures dites de e-discovery qui y sont applicables, mais également au regard des pouvoirs de contrôle dont pourraient disposer des autorités étatiques habilités dans un cadre quasi-judiciaire.

Il convient également de noter que la Commission nationale de l'informatique et des liberté, la CNIL, l'autorité nationale française de contrôle de l'informatique et des libertés, recommande vivement de régler le problème de la sécurité dans le contrat, au moyen des clauses publiées par la Commission[18]. Toutefois, la CNIL n'évoque pas la question spécifique du secret professionnel des avocats dans le Guide rédigé à destination de notre profession.[19]

La loi Informatique et libertés contient une disposition générale en matière de confidentialité et de sécurité des données, qui fait du responsable des traitements le garant vis-à-vis de son sous-traitant des obligations à respecter dans ce domaine. Cette obligation est accompagnée de deux incriminations pénales (CP L 226-17 et L 226-17-1)[20]. L'attention du fournisseur du prestataire de services externe, ainsi que celle de l'avocat en sa qualité de responsable des traitements, doivent être attirée sur le fait qu'il en va de leur responsabilité commune de s'assurer que les données stockées en nuage sont protégées[21].
La question se pose également du devoir d'alerte du sous-traitant en cas de mise en jeu de la règle du secret professionnel en cours d'exécution ou à l'issue de l'exécution du contrat de prestations de services.

En conclusion, il est impératif d'inscrire dans un texte contraignant que le secret professionnel d'ordre public s'applique impérativement aux services informatiques externalisés proposés aux avocats, à fortiori à ceux relevant du cloud computing, ne se limitant pas aux seuls transferts de données, quels que soient les moyens et le lieu du traitement comme le rappellent les Lignes directrices du CCBE de septembre 2012, y compris dans l'hypothèse où la convention de prestations de services ne mentionne pas l'obligation au respect du secret professionnel. L'un des axes de prévention doit consister à ce que le prestataire n'ignore pas la qualité d'avocat de son client et l'alerte immédiatement en cas de risque pour la préservation du secret professionnel.

18 « *Cloud Computing : la CNIL se prononce* », étude publiée le 2 juillet 2012.

19 http://www.cnil.fr/linstitution/actualite/article/article/un-nouveau-guide-pratique-a-destination-des-avocats/ .

20 http://www.cnil.fr/documentation/textes-fondateurs/sanctions-penales/ .

21 Article 34 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : « *Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.* »

ANNEX II - ADDITIONAL INFORMATION – GERMANY

The German delegation believes that the CCBE's questions address a highly complex field. For some part here are currently no rules at all, for other parts legislation is extremely fragmented. Therefore, the delegation takes the view that it is impossible to answer certain questions with certitude. This is precisely part of the problem, and, according to our experts, an argument against the use of the Cloud for case-related information.

General comments:

The focus on questions relating to the "legal" risks for case-related data (governmental access) when using external Cloud solutions is questionable. A substantial argument against using the Cloud is the technical and organisational risk involved, in particular with a view to illegal disclosure to third parties. On the contrary: A large part of the legal access by police and investigation authorities as well as secret services described above is not limited to data stored "in the Cloud". The respective enabling provisions would also apply to lawyers' own data processing systems.

Another problem "beside" the CCBE's approach chosen in the present questionnaire is Germany's § 203 StPO. According to the current version of the law, transmission of case-related data into a Cloud (with the exception of cases of undecryptable encoding prior to transmission and storage) is a sanctioned criminal offence, unless the client has given his prior informed consent to the use of the cloud and has not revoked it.

ANNEX III – ADDITIONAL INFORMATION – HUNGARY

More detailed reasoning:

Answer 1.
Under Hungarian law, the government may require lawyer data from a Cloud Service Provider according to the following procedural rules:

a) a criminal procedure against the lawyer,

b) a criminal procedure against the client of the lawyer, where the lawyer is defending the client,

c) a criminal procedure against the client of the lawyer, where the lawyer does not act as a defending attorney (e.g. a civil law client), and

d) an administrative procedure against the lawyer.

Cases a) - c) are **criminal procedures**, in which the respective court, the prosecutor's office and the investigating authority (either the police or the customs authority) have the right to require information or data or the provision of documents from any party (including business companies or other authorities) that may possess or otherwise have knowledge of any information related to the potential offense within the frames of **general data request** (section 71 of Act XIX of 1998 on Criminal Procedure – hereinafter the "Criminal Procedure Act"). Within this general formal data request, the respective authority may impose fines on those entities who reject provision of data. However, if the entity concerned refuses to provide data based on statutory prohibitions, the authority cannot require data or conduct any procedural actions against that entity (section 71 para. 7 of the Criminal Procedure Act).

As for lawyer data, however, there are a number of cases when data provision by lawyers is restricted by their confidentiality, or when the law specifically excludes them from being witnesses.

In respect of case a) above, a lawyer is not automatically exempted from confidentiality. The Ethical Code of the Hungarian Bar Association (resolution no. 8/1999 (III.22.) , a mandatory regulation for lawyers, provides that a lawyer, when acting as a defendant, may presume to be allowed to disclose client data to the extent necessary for defending himself, if the respective procedure was initiated by the client itself (section 4/9 point c) of the Ethical Code). Otherwise lawyers are bound by professional confidentiality obligations even when they are defendants.

In case b), the lawyer is statutory excluded from making testimony as a witness before the respective authority on the facts that came into his/her knowledge within the course of defending the defendant or what he/she communicated to the defendant respectively (section 81 para. 1 of the Criminal Procedure Act).

In case c) the lawyer may refuse to testify, due to confidentiality, unless the client exempts the lawyer from confidentiality, or the client itself is obliged by law to provide the certain data to the given authority.

In addition to general data requests, the government may also issue a search warrant, pursuant to section 149 of the Criminal Procedure Act, to investigate certain premises or a computer system or a data carrier found at the subject premises. As the Criminal Procedure Act does not expressly clarify the actual scope of a "computer systems", it may be concluded that in case the Cloud Service Provider has premises in Hungary and at least a server, the authorities may enter the entire network accessible from that server. However, such search warrant may be limited by section 8 para.2 of the

Attorney Act, which provides that the lawyer cannot disclose client related documents and data within the course of an official inspection held at its premises, but may otherwise not disturb such inspection.

In case of the **administrative proceeding** set out in d) above, Act CXL of 2004 on the General Rules of Administrative Proceedings and Services ("Administrative Proceeding Act") provides that data may be requested from the subject party of the procedure on a non-mandatory basis (section 51 para. 1).

In case of mandatory data provision, however, the Administrative Proceeding Act only cites confidentiality as an obstacle to provide a statement in case of witnesses (section 53 para. 3 of the Administrative Proceedings Act). However, in case data provision is based on an act or decree, the confidentiality of lawyers is not listed amongst the reasons to refuse making a mandatory statement (section 51 para 4 of the Administrative Proceedings Act). Even though omitting this explicit provision and the authorities obligation to keep data confidential that belongs to the secrecy oath of lawyers may imply that lawyers are not prevented from providing data to the authorities, our findings above related to data provision when a lawyer is a defendant shall be applied in this case as well, i.e. lawyers may not disclose client data unless exempted by the client itself.

As for third parties, the Administrative Proceeding Act provided that state or other entities or persons in possession of relevant information may be requested to provide data that is in the possession of this entity and is necessary to conclude the given proceeding (section 26 para. 1 point c)). However, as the Administrative Proceeding Act is a background act of various other acts and decrees, such other law may the scope of entities – some listing business companies – that may be requested to provide certain data.

Answer 4.
Secret information obtaining methods, such as monitoring of electronic communications by investigating authorities in cooperation with the electronic communication service provider may be applied before or in criminal proceedings (section 178 para. 2, and section 200 of the Criminal Procedure Act, and 92 of Act C of 2003 on Electronic Communications). Secret data collection facilitated within section 200 of the Criminal Procedure Act is subject to judicial approval and may be solely used as an ultimate solution to collect evidence.

In case a) referred above, the general limitations may be applied; it is neither provided nor excluded that such secret data collection would overwrite the confidentiality binding the lawyer even as a defendant.
As for case b), section 202 para. 3 of the Criminal Procedure expressly stipulates that such monitoring may only be applied in relation to an attorney (including electronic communications) defending the defendant in the given case, if it is presumed that the attorney prepares a criminal offence related to his/her defendant's case.
In case the lawyer is not involved in the case, he/she cannot be subject to secret data collection, solely in case their guilty association to the defendant is presumed (section 202 para 2. of the Criminal Procedure Act).

Answer 5
Criminal procedures:

- general data requests are not subject to judicial review. However, if data was obtained unlawfully by violation of the above limitations, the certain evidence may be deemed to be unlawful, and may result in their inadmissibility (section 77 para. 1 and section 78 para. 4 of the Criminal Procedure Act).

- in case of search warrants, they may be subject to prior judicial approve, but they can be also carried out by the decision of the prosecutor, or in certain cases, the investigating authority as well. In case of law firm, a search warrant of their premises (including their computer system) is subject to review by the judge. Otherwise, decisions or search warrants may be subject to legal remedy depending on the issuing body (section 195 para. 6 and 215 of the Criminal Procedure Act).

- in case the lawyer is the defendant, he/she may cite the unlawful collection of evidence in his/her respective appeal against the final decision.

Administrative procedure

In case of an administrative procedure, the data collection of the authority may be challenged in the appeal against its respective decision, either by the lawyer or the Cloud Service Provider, who finds the decision harmful (section 98 of the Administrative Proceeding Act).

ANNEX IV - ADDITIONAL INFORMATION – SPAIN

National rules related to governmental access to data and professional secrecy

In order to answer the questions, we include here a list of the most relevant applicable national rules. Such national rules would be as follows[22]:

- National security, law enforcement and due process:
    - Spanish Constitution of 1978 (articles 18 and 55).
    - Organic Law 2/2002, of 6 May, that regulates the previous judicial control of the National Intelligence Agency, published in the Official Spanish Gazette nº 109, of 7 May.
    - Organic Law 2/1986, of 13 March, on Law Enforcement Authorities, published in the Official Spanish Gazette Journal nº 63, of 14 March 1986;
    - Royal Decree of 14 September 1882 that approves the Criminal Procedure Law.
    - Organic Law 6/1985, of 1 July, of the Judiciary Power, published in the Official Spanish Gazette nº 157, of 2 July 1985.
    - Royal Decree 769/1987, of 19 June, on the regulation of the Judiciary Police, published in the Official Spanish Gazette nº 150, of 24 June 1987.
    - Law 34/2002, of 11 July, on Information Society Services and Electronic Commerce, published in the Official Spanish Gazette nº 166, of 12 July 2002.
    - Law 32/2003, of 3 November, on Telecommunications, published in the Official Spanish Gazette nº 264, of 4 November 2003.
    - Convention on Cybercrime, ratified by Spain on 20 May 2010, published in the Official Spanish Gazette nº 266, of 17 September 2010.

- Professional secrecy
    - Royal Decree 658/2001, of 22 June, by which the General By-Law of the Spanish Lawyers is approved, published in the Official Spanish Gazette of 10 July 2001.

- Personal data protection:
    - Organic Law 15/1999, of 13 December, on the Protection of Personal Data, published in the Official Spanish Gazette Journal nº 298, of 14 December 1999.
    - Royal Decree 1720/2007, of 21 December, which approves the Regulation implementing Organic Law 15/1999, of 13 December, on the Protection of Personal Data, published in the Official Spanish Gazette nº 17, of 19 January 2008.

[22] All translations of the legal texts included in this document are **unofficial.**

It is important to highlight that the answers provided are related to requests of information or data from law enforcement authorities, so requests from other governmental authorities are excluded. The expression "all types of law enforcement authorities and other governmental agencies, recognising that the rules may be different for law enforcement and national security access" is too broad and specific requests would require a case-by-case legal reasoning.

On the other hand is also necessary to underline that **Data Protection Legislation does not apply to "Files established for the investigation of terrorism and serious forms of organized crime"** (Organic Law 15/1999, Art. 2(2)*c)*).

Question nº 1 – Additional Information (see also above in the comparative table)
May the government require a Cloud provider to disclose lawyers' data in the course of a Government investigation?

The Cloud provider and the lawyers´ data according to the data protection legislation

From a data protection perspective and according to the Spanish legislation on data protection, the lawyer is considered as a controller and the cloud provider as a processor. Such distinction is relevant as the processor *"processes personal data on behalf of the controller"* according to the definition of the processor provided in article 3(g) of the Organic Law 15/1999.

Such processor can only process personal data on behalf of the controller, acting according to stipulations of the contract to which article 12(2) of the Organic Law 15/1999 refers[23].

According to article 20(3) of the Regulation of the Organic Law, that regulates relations between the data controller and data processor, *"3. Should the data processor use the data for another purpose, disclose or use them in breach of the stipulations of the contract to which Article 12(2) of Organic Law 15/1999, of 13 December, refers,* ***he shall also be considered the data controller, answering for the breaches he has personally caused****."* (Emphasis added)[24]

The processor may not disclose the information that process on behalf of the data controller, unless the data controller authorizes the processor to do so. And such statement is based also on the fact that those personal data are also under the lawyers´ right and duty of professional secrecy.

Furthermore, the Spanish Data Protection Authority (DPA) and the General Council of Spanish Lawyers (Spanish Bar Association), released on 18th June 2012 a report on the use of Cloud

---

23 Article 12(2) states *"Processing on behalf of third parties shall be regulated in a contract which must be in writing or in any other form which allows its performance and content to be assessed, it being expressly laid down that the processor shall process the data only in accordance with the instructions of the controller, shall not apply or use them for a purpose other than that set out in the said contract, and shall not communicate them to other persons even for their preservation.*
The contract shall also set out the security measures referred to in Article 9 of this Law, which the processor is obliged to implement." (Unofficial translation).

24 In this sense, Opinion 5/2012 of the Working Party 29 on Cloud Computing, adopted July 1st 2012 (WP 196), with regard to contractual safeguards of the "controller" – "processor" relationship(s) mentions that *"To ensure legal certainty the contract should also set forth the following issues:*
[…]
5. Inclusion of a confidentiality clause, binding both upon the cloud provider and any of its employees who may be able to access the data. Only authorized persons can have access to data.
[…]
7. The contract should expressly establish that the cloud provider may not communicate the data to third parties, even for preservation purposes unless it is provided for in the contract that there will be subcontractors. The contract should specify that subprocessors may only be commissioned on the basis of a consent that can be generally given by the controller in line with a clear duty for the processor to inform the controller of any intended changes in this regard with the controller retaining at all times the possibility to object to such changes or to terminate the contract. […]
8. Clarification of the responsibilities of the cloud provider to notify the cloud client in the event of any data breach which affects the cloud client's data."
The mentioned Opinion is available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

Computing by law firms and data protection[25] that focus on the professional secrecy. With regard to this issue, the report says that *"This right-duty imposes on law firms a **qualified diligence** regarding the observance by the services provider of all legal guaranties regarding security requirements on data, documents and actions under the professional secrecy."*[26] (Emphasis added).

Other fundamental rights: secrecy of communications and judicial guarantees

Access to lawyers´ data affects several fundamental rights, in addition to or independently from the fundamental right to data protection. Such fundamental rights are:

- The fundamental right to secrecy of communications: Article 18(3) of the Spanish Constitution states that *"Secrecy of communications is guaranteed, particularly regarding postal, telegraphic and telephonic communications, **except in the event of a court order**"* (emphasis added).

- With regard to the fundamental right to secrecy of communications, article 55(2) of the Spanish Constitution states that *"**An organic act** may determine the manner and the circumstances in which, on an **individual basis and with the necessary participation of the courts and proper parliamentary control**, the rights recognized in section 17, subsection 2, and **18, subsections** 2 and **3**, **may be suspended for specific persons in connection with investigations of the activities of armed bands or terrorist groups**.*

  Unwarranted or abusive use of the powers recognized in the foregoing organic act shall give rise to criminal liability as a violation of the rights and freedoms recognized by the laws." (emphasis added).

- The fundamental right to judicial guarantees: Article 24(2) of the Spanish Constitution states that *"all have the right to the ordinary judge predetermined by law; to defense and assistance by a lawyer; to be informed of the charges brought against them; to a public trial without undue delays and with full guarantees; to the use of evidence appropriate to their defense; not to make self-incriminating statements; not to plead themselves guilty; and to be presumed innocent.*

  ***The law shall specify the cases in which, for reasons of** family relationship or **professional secrecy, it shall not be compulsory to make statements regarding allegedly criminal offences**."* (emphasis added)

Right and duty of professional secrecy

This right and duty of professional secrecy is also a legal obligation according to article 542(3) of the Organic Law 6/1985 that states:

> *"Lawyers must keep secret regarding the facts or news that they know by reason of any form of their professional actions and may not be compelled to testify about them."*

[25] Available, in Spanish, at http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/junio/informe_CLOUD.pdf

[26] See, in Spanish, page 11 of the mentioned report of the Spanish DPA and the General Council of Spanish Lawyers.

Allow governmental access to lawyer´s data through a Cloud provider without the required guarantees would mean circumvent the constitutional and legal protections already set, such as the secrecy of communications, legal guarantees and the right and duty of professional secrecy.

Also, the General By-Law of the Spanish Lawyers[27] includes several provisions regarding lawyers´ duty of professional secrecy.

According to article 21(b), lawyers cannot *"Share services or premises with disqualified lawyers, if this could affect the guarantee of The Legal professional Privilege".* Also, article 25 states that *"The following advertising shall be considered contrary to the rest of the Rules of the Professional Conduct, if it:*

a) Discloses directly or indirectly facts, data or circumstances supported by the Legal Professional Privilege;"

In particular, article 28, regarding join practice of the legal profession, states in its section 2 that *"The association cannot share premises or services with any cause of incompatibility, if this affects the safeguard of the Legal Professional Privilege."* And in section 6 of the mentioned article that *"The practising lawyer shall reflect his performance in his Bar Association. Nevertheless, all the members of an associated office shall accomplish Legal Professional Privilege, […]."*

Article 32 also relates to the professional secrecy and states that: *"1. In compliance with what is established in Section 437.2 of Organic Law from the Judicial Power,* ***lawyers shall maintain confidentiality each fact or news that they are acquainted with any type of their practice and they must not declare them****.*

2. In case that the President of the Bar Association or who replaces him by statute were required by virtue of the legal rule or warned by the Judicial Power or governmental authority, skilled for the register in a lawyer's office, he should appear in person to the diligences that take place in that office safeguarding the Legal Professional Privilege." (emphasis added)

Finally, article 42, related to the lawyers´ obligation with regard to the parties, states that: *"The lawyer obligations in relation with his client are defending him with the maximum care as possible and keeping the Legal Professional Privilege, apart from those obligations arising out of contracts."*

Such duty is specific and independent from the secrecy duty that provides article 10 of the Organic Law 15/1999, and is related to the fundamental right to judicial guarantees (article 24 of the Spanish Constitution).

Disclosing of data by a cloud provider

A lawyer´s cloud provider may not disclose lawyer´s data unless the constitutional and due process guarantees are met.

With regard to the governmental requests of access, it would be possible to distinguish two cases. First, a law enforcement request for administrative purposes, and second, criminal investigations or even national security investigations.

On the one hand, a law enforcement request for administrative purposes does not require initially (when fulfilling the requirements provided in article 22 of the Organic Law 15/1999) an authorization

[27] Approved by Royal Decree 658/2001. Already cited. Unofficial translation.

by a judicial order. In this case, data subject´s consent is required or such processing can only be carried out according articles 6 and 11 of the Organic Law 15/1999. The processing of personal data in this case is under the general regime of the Law (according to article 22.1 *in fine* of the Organic Law 15/1999). Nevertheless, taking into consideration the rights involved, the fundamental right to secrecy of communications (article 18(3) of the Spanish Constitution), the fundamental right to judicial guarantees (article 24(2) of the Spanish Constitution), the right and duty of professional secrecy imposed to lawyers, any request to a cloud provider should be done through the lawyer as "owner of the information", unless referred to an investigation about him/her. And in particular when the request involves personal data as the lawyer is the controller of such data.[28]

Also, the Law 32/2003 on Telecommunications , with regard to secrecy of communications, states in its article 33 that:

> *"Operators who run public electronic communications networks or deliver publicly available electronic communications services must guarantee the secrecy of communications in accordance with articles 18.3 and 55.2 of the Constitution and therefore must take the necessary technical measures accordingly.*
>
> *Likewise operators must take at their own cost the measures established by regulation for the performance of interceptions provided for pursuant to the terms established in article 579 of the Code of Criminal Procedure and Organic Act 2/2002 of 6 May regulating prior judicial supervision by the National Intelligence Centre."*

On the other hand, according to article 579 of the Criminal Procedure Law, interception of communications, in the course of a criminal investigation, requires two elements:

- Reasons to believe that the interception may lead to finding or proving a fact circumstance relevant to a criminal procedure, and
- Authorization by a reasoned judicial order.

Therefore, a lawyer´s cloud provider could only disclose lawyers´ data to the government if these guarantees are met. Otherwise, such access would infringe fundamental rights and therefore would be illicit or illegal.

And with regard to national security, the Organic Law 2/2002 regulates the terms and conditions under which the National Intelligence Agency may intercept communications. Any interception of communications, as affects a fundamental right, would require authorization of the designated Magistrate of the Supreme Court.

---

28 In this sense, it would be recommendable to consider §173 of the Explanatory Memorandum of the Convention on Cybercrime, already ratified by Spain, that states *"173. Under paragraph 1(a), a Party shall ensure that its competent law enforcement authorities have the power to order a person in its territory to submit specified computer data stored in a computer system, or data storage medium that is in that person's possession or control. The term "possession or control" refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory (for example, subject to applicable privileges, a person who is served with a production order for information stored in his or her account by means of a remote online storage service, must produce such information). At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement."* Therefore, it would be possible to argue that the processor is not in possession, as acts following the instructions of the controller. In other cases that do not involve personal data, a similar argument would be feasible when involving lawyers´ data as covered by the professional secrecy. The Explanatory Memorandum is available at http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

ANNEX V – UK CONTINUATION SHEET

Question 1

Search and seizure in criminal investigations

In England and Wales, the powers of the police to search for and seize material, including data, are governed largely by the Police and Criminal Evidence Act 1984 ("PACE"). Where data subject to these powers are encrypted, Part 3 of the Regulation of Investigatory Powers Act 2000 ("RIPA") entitles the police to demand its decryption. Data held by lawyers (including data stored or processed by a Cloud provider) in the course of providing professional advice, or handling litigation, is protected by legal professional privilege. The powers of the police under PACE to search for and seize material with or without a warrant are expressly limited so as not apply to anything that is believed, on reasonable grounds, to be privileged. Similarly, the power of the police under PACE to obtain an order from a judge to access certain categories of material ("special procedure material") expressly excludes privileged material. However, privilege does not apply to material held by a lawyer outside the scope of the client relationship or litigation handling (eg. material held by a lawyer entirely for his or her own business purposes. Nor does it apply to information held with the intention of furthering a criminal purpose – this is known as the as the "iniquity exception". Such data are subject to search and seizure.

The position is effectively the same in Northern Ireland, where the Police and Criminal Evidence (Northern Ireland) Order 1989 makes equivalent provision to PACE.

In Scotland, the equivalent powers of search and seizure are largely based on the common law and are subject to limitations of similar scope to protect legally privileged material. Though largely based on common law, there are some legislative interventions in Scotland - for example, Part 3 of RIPA applies also in Scotland.

Interception of communications and acquisition of communications data

Surveillance generally is governed throughout the United Kingdom by RIPA (which is varied and supplemented in relation to supervision of surveillance by the Regulation of Investigatory powers (Scotland) Act 2000 ("RIPSA"). Special provision is made for interception and acquisition of communications data throughout the United Kingdom by RIPA, which provides the police and security services, together with a narrow range of other agencies, with power to obtain a warrant from a senior minister authorising interception of communications, ie. access to the content of private communications. The powers apply to information carried over a "public telecommunications system" which may include Cloud computing services and certainly includes the transmission of data to, from or between the storage and processing systems operated by Cloud service providers.

RIPA also provides the police, security services and a wider range of other agencies with power to obtain and disclose communications data, ie. non-content information about communications carried over a public telecommunications system. The categories of information correspond to those which service providers are obliged to retain under UK implementation of Directive 2006/24/EC. RIPA enables each agency to operate a self-authorisation procedure involving a senior officer.

The legislation contains no exception for communications to or from lawyers, even where those communications are, or are reasonably believed to be, privileged. However, the Interception Code of

Practice issued under RIPA advises that “Consideration should be given to any infringement of the privacy of individuals who are not the subject of the intended interception, especially where communications relating to religious, medical, journalistic or legally privileged material may be involved”. The Bar Council of England and Wales has pressed the UK Government to amend the legislation to provide explicit protection for privileged communications, so far unsuccessfully.

As matters stand, the protection for privileged data would ultimately come in to play not explicitly to prevent its interception, but under PACE and, in Scotland, common law to prevent its use in subsequent Court Proceedings.

Other conduct by the intelligence services

The Intelligence Services Act 1994 (which applies throughout the United Kingdom and the Channel Islands) provides the security and intelligence services with power to obtain a Government warrant authorising an interference with property or with wireless telegraphy. It is possible that these powers could be used to obtain access to data stored or processed in the Cloud. The provisions contain no exception for legally privileged information.

ANNEX VI – CZECH REPUBLIC – CODE OF CRIMINAL PROCEDURE – SECTION 8

Section 8

Code of Criminal Procedure (141/1961 Coll. ACT of 29 November 1961 on Criminal Procedure, as amended).

(1) Public authorities, legal entities and natural persons are required to comply with letters of request from law enforcement authorities for the performance of their actions without undue delay and unless a special regulation stipulates otherwise, to comply without payment. Furthermore, public authorities are also obliged to immediately notify the public prosecutor or the police authorities of facts indicating that a criminal offence has been committed.

(2) If the criminal proceedings require a proper investigation of the circumstances suggesting that a criminal offence has been committed or to assess the circumstances of the accused during court proceedings or for the enforcement of a decision, the public prosecutor and, after the indictment or a punishment petition, the presiding judge may request information that is subject to banking secrecy and data from the security register. Pursuant to Section 180 of the Criminal Code, the law enforcement authority may request individual data obtained under a special Act for statistical purposes during the criminal proceedings. The conditions under which the law enforcement authority may require the data obtained in the administration of taxes are stipulated under a special Act. Data obtained under this provision may not be used for a purpose other than the criminal proceedings for which such data was requested.

(3) For the reasons as stated in Subsection 2, the presiding judge may, and upon the proposal of the public prosecutor during a preliminary hearing, order the surveillance of the bank accounts or accounts of persons entitled to the records of investment instruments under a special Act for a maximum period of six months. If the reason for which the surveillance of an account was ordered exceeds this time, it may be extended upon the order of a judge from a court of higher instance and, during preliminary hearing, upon the proposal of the public prosecutor of the County Court judge for a further six months, and such prolongation can be performed repeatedly. Information obtained under this provision may not be used for a purpose other than the criminal proceedings for which it was obtained.

(4) The performance of obligations under Subsection 1 may be rejected with reference to the obligation to maintain the secrecy of classified information protected by a special Act or imposed by the State or the recognised duty of confidentiality; this does not apply

a) if the person who has the obligation would otherwise risk criminal prosecution for the failure to notify or prevent a criminal offence, or

b) in executing the request of a law enforcement authority with regards to a criminal offence, where the requested person is also the reporter of the criminal offence.

The State recognised obligation of confidentiality under this Act does not consider such obligation the scope of which is not defined by law but instead arises from a legal action taken under the law.

(5) Unless a special Act stipulates the conditions under which information may be disclosed for the purpose of criminal proceedings that are deemed classified pursuant to such Act or which is subject to an obligation of secrecy, such information may be requested for criminal proceedings upon the prior consent of the judge. This does not affect the obligation of confidentiality of an attorney under the Advocacy Act (Act No. 85/1996 Coll., on the Legal Profession, as amended).

(6) The provisions of Subsection 1 and 5 shall not affect the obligation of confidentiality imposed on the basis of a declared international treaty to which the Czech Republic.