



**CONVENTION**

**CONCERNANT LA COMMUNICATION  
ELECTRONIQUE EN MATIERE PENALE**

**ENTRE LES JURIDICTIONS ORDINAIRES DU  
PREMIER ET SECOND DEGRE**

**ET LES AVOCATS**

**ENTRE**

**Le Ministère de la Justice**, situé au 13 Place Vendôme, 75001 Paris,  
Représenté par le Garde des sceaux, Ministre de la Justice, agissant au nom de l'Etat,

Ci-après dénommé le « **Ministère de la Justice** » ou le « **Ministère** »,

D'UNE PART,

**ET**

**Le Conseil national des barreaux**, située au 180 Boulevard Haussmann, 75008 Paris,  
Représenté par son Président, Jérôme Gavaudan,

Ci-après dénommé le « **CNB** » ou « **Conseil national des barreaux** »,

D'AUTRE PART,

Ci-après ensemble désignés individuellement un « **Partenaire** » et collectivement les  
« **Partenaires** »,

**APRÈS AVOIR PREALABLEMENT EXPOSE CE QUI SUIT :**

## 1. Identification des Partenaires

Le **Ministère de la Justice** a en charge le développement et la maintenance des outils informatiques permettant la mise en œuvre de la communication électronique pénale. Il détermine en concertation avec le Conseil national des barreaux les modalités de mise en relation de leurs réseaux privés respectifs.

Le **Conseil national des barreaux** représentant la profession d'avocat auprès des Institutions et des Pouvoirs Publics détermine, en concertation avec le Ministère de la Justice, les modalités et conditions de mise en œuvre du réseau indépendant à usage privé des avocats aux fins d'interconnexion avec le réseau privé virtuel justice.

Il assure également l'exploitation et les développements des outils techniques permettant de favoriser la dématérialisation des échanges entre avocats (Loi n° 71-1130 du 31 décembre 1971, mod. L. 18 nov. 2016 et arrêt du Conseil d'Etat du 15 mai 2013, art. 21-1).

## 2. Contexte de la Convention

La communication électronique en matière pénale est régie par les dispositions du Code de procédure pénale, en particulier ses articles D. 590 et suivants. La convention passée entre le Ministère de la Justice et le CNB le 24 juin 2016 concernant la communication électronique entre les juridictions ordinaires du premier et du second degré et les avocats régissait principalement la communication électronique en matière civile, renvoyant pour l'essentiel – de même que l'article D. 591 du CPP – à la conclusion de protocoles locaux s'agissant de la matière pénale. Ce principe de déclinaison locale de la communication électronique pénale a constitué un frein à sa généralisation sur le territoire national et ce malgré la dématérialisation croissante des procédures pénales.

Lors de la première période d'état d'urgence sanitaire du printemps 2020, le Ministère de la Justice et le CNB ont renforcé leur coopération et ont conclu un protocole temporaire destiné à permettre l'utilisation de PLEX, plateforme sécurisée de mise à disposition de fichiers, pour la transmission de copies de procédures pénales et les notifications prévues à l'article 803-1 du CPP.

C'est dans ce contexte que le Ministère de la Justice et le CNB ont décidé de procéder à la refonte de la convention du 24 juin 2016 portant sur la communication électronique entre les juridictions et les avocats en prévoyant l'adoption de deux conventions distinctes, l'une destinée à la matière civile, l'autre à la matière pénale.

Dans le cadre de cette dernière, l'objectif est de régir :

- la communication électronique des juridictions vers les avocats par la pérennisation des dispositifs mis en œuvre dans le cadre de l'état d'urgence sanitaire ;
- la communication électronique des avocats vers les juridictions en supprimant notamment la nécessité de l'établissement d'un protocole local, permettant ainsi à tout avocat d'adresser des messages ou de former des demandes par voie électronique à toute juridiction du premier et du second degré, quel que soit son barreau de rattachement.

L'objectif attendu par cette convention est de développer massivement l'usage de la communication électronique entre les avocats et les juridictions du premier et du second degré en garantissant la sécurité des échanges mais aussi du stockage des données, l'intégrité des actes transmis entre les parties et l'identification des acteurs de la communication électronique pénale.

Elle est conclue conformément à l'article 2 du décret n°2020-1792 du 30 décembre 2020 portant sur la communication électronique pénale.

## IL EST CONVENU ET ARRETE CE QUI SUIT :

### Article 1 – Définitions /dénominations/ abréviations

---

**Le Réseau Privé Virtuel des Avocats (ou « RPVA »)** est un réseau de communication électronique au sens de l'article L.32 du code des postes et des communications électroniques, permettant l'acheminement de communications électroniques sécurisées entre les avocats et les services judiciaires du Ministère de la Justice requérant l'authentification des parties à l'échange. Le RPVA est opéré sous le contrôle et la responsabilité du Conseil national des barreaux et est interconnecté avec **le Réseau Privé Virtuel de la Justice (ou « RPVJ »)**, opéré sous le contrôle et la responsabilité du Ministère de la Justice.

**Une Interface** est un logiciel ou site internet permettant l'accès ergonomique aux services de communication électronique.

**e-Barreau** est une application, hébergée sur le RPVA et opérée sous le contrôle et la responsabilité du Conseil national des barreaux permettant notamment l'échange de communications électroniques entre les avocats et les services judiciaires. A cette fin, e-Barreau communique notamment avec les applications dédiées du Ministère de la Justice.

**La Procédure Pénale Numérique (ou « PPN »)** est un programme interministériel associant le Ministère de la Justice et le Ministère de l'Intérieur visant la dématérialisation complète de la chaîne pénale par l'usage de documents nativement numériques signés électroniquement ainsi que la dématérialisation des échanges entre les Juridictions et ses partenaires, en particulier les Avocats.

**La Communication pénale numérique (ou « CPN »)** est une brique applicative de la PPN qui a pour objectif de faciliter l'envoi et la réception de pièces de procédures numériques entre les acteurs du Ministère de la Justice et ses partenaires en matière pénale. A cette fin, elle offre aux utilisateurs justice une interface unifiée, indépendamment du canal de communication utilisé.

**La Communication électronique pénale (ou « CEP »)** définit les règles de fonctionnement des échanges électroniques entre les Partenaires en matière pénale, au niveau national comme au niveau local.

**La PPlateforme d'échange Externe (ou « PLEX »)** est une plateforme d'échanges sécurisés de fichiers entre les agents du Ministère de la Justice et les personnes extérieures à l'Etat, mis en œuvre par le Ministère de la Justice. Sa mise en œuvre est autorisée par arrêté du 24 octobre 2019 (NOR : JUST1927457A) et ses caractéristiques techniques ont été précisées dans un second arrêté du même jour (NOR : JUST1927458A).

**Les Adresses nominatives de messagerie électronique des avocats** utilisent le format suivant : `cnbf.nomprenom@avocat-conseil.fr` ou `cnbf.prenomnom@avocat-conseil.fr`

**La Table Nationale des Avocats (ou « TNA »)** répertorie l'ensemble des adresses de messagerie électronique des avocats inscrits à la communication électronique.

**Les Avocats** désignent les avocats inscrits aux services de communications électronique, et disposant d'un système d'authentification et d'identification garantissant un accès sécurisé auxdits services, dont les coordonnées sont reproduites dans la TNA.

**Les Juridictions** désignent les juridictions ordinaires du premier et du second degré.

**Les Boîtes aux Lettres CEP (ou « BAL CEP »)** sont des adresses de messagerie structurées sécurisées des services judiciaires permettant notamment la communication électronique pénale avec les Avocats.

**La Convention** désigne l'intégralité de la présente et ses annexes, dont la liste figure en article 16.

## Article 2 – Objet de la convention

La Convention a pour objet de préciser, d'une part, les obligations juridiques et financières des Partenaires et d'autre part, les voies et moyens mis en œuvre aux fins de communication électronique, en ce compris les systèmes de consultation, d'échanges électroniques, utilisés dans le cadre des procédures pénales et les prévisions de nature organisationnelle ou opérationnelle mises en œuvre, entre les Juridictions et les Avocats.

Elle n'a pas pour objet de rendre obligatoire le recours aux Services, les avocats et les Juridictions restant, chacun pour ce qui le concerne, maîtres d'y souscrire ou non.

## Article 3 – Cadre Légal et champ d'application

La Convention est destinée à faciliter la mise en œuvre des échanges dématérialisés entre les Juridictions et les Avocats dans le cadre des dispositions du code de procédure pénale et plus particulièrement des articles 114, 167, 388-4, 803-1, R. 165, D. 15-8 et D. 590 et suivants.

La Convention est conclue et s'applique dans la limite des dispositions prévues par les lois et règlements en vigueur et à venir. En particulier, elle ne saurait se substituer aux dispositions du code de procédure pénale.

En cas de contradiction entre les lois et règlements, d'une part, et la présente, d'autre part, les Partenaires sont convenus que les stipulations contraires, prévues dans la présente, ne trouveront pas à s'appliquer.

## Article 4 – Description des Services

La Convention vise à offrir aux partenaires les services suivants (ci-après les « **Services** ») :

- la mise à disposition par les services judiciaires des procédures et de leurs copies aux Avocats ;
- la transmission des actes prévus par le code de procédure pénale à destination des Avocats ;
- la transmission des demandes formées par les Avocats au titre de la communication électronique pénale, conformément aux dispositions du code de procédure pénale.

Ces Services permettent notamment aux Avocats et aux Juridictions :

- de transmettre des données informatisées de procédure ;
- d'échanger des courriers électroniques, support d'une communication purement fonctionnelle ou préparatoire à la transmission de documents électroniques ;
- de transmettre et recevoir des actes et pièces de procédure par voie électronique.

Dans le respect des dispositions des lois et règlements en vigueur, toutes les étapes ou maillons de procédure pourront, selon l'avancement des développements informatiques de part et d'autre, faire l'objet de transmissions de données informatisées (au moyen de fichiers structurés ou non, de messages et de pièces jointes selon les cas) accessibles et consultables par le biais des applications mises à disposition par les Partenaires.

Les Services sont décrits plus spécifiquement à l'article 6 de la Convention.

### **Article 5 - Cadre de référence fonctionnel et technique**

---

Les Services sont assurés au travers d'applications hébergées sur des réseaux privés virtuels indépendants opérés par chaque partie.

Le périmètre fonctionnel pris en considération pour la mise en œuvre des Services concerne toutes les procédures pénales quelle que soit la Juridiction saisie.

Les cadres de référence fonctionnels et techniques des Partenaires sont définis en Annexe des présentes telles que listées en article 16.

### **Article 6 – Régime des Services offerts**

---

#### **Article 6.1 – La mise à disposition des procédures et de leur copie**

##### **6.1.1 Périmètre**

Les Partenaires conviennent que les stipulations du présent article concernent tant les transmissions de copies de procédure aux Avocats que leur mise à disposition, au sens du 5e alinéa de l'article 114 du code de procédure pénale, lorsqu'elles sont effectuées par voie électronique.

##### **6.1.2 Principes généraux**

Le Ministère de la Justice met à disposition des services judiciaires et des Avocats une plateforme d'échanges sécurisée permettant de procéder à la transmission des copies de procédures, dans les conditions prévues par le code de procédure pénale, laquelle est décrite en article 6.1.3.

Les Partenaires conviennent que la transmission des copies de procédure interviendra, en principe, sous forme numérique native ou numérisée selon les modalités définies ci-après, la mise à disposition d'un exemplaire papier n'étant prévue qu'en cas d'impossibilité matérielle ou technique rencontrée par une Juridiction, un Avocat ou l'un des Partenaires.

La mise à disposition par voie électronique des copies de procédure est gratuite par application de l'article D15-8 du code de procédure pénale.



### 6.1.3 Modalités

#### - Émetteur et destinataire

L'émetteur des transmissions des copies de procédures est un agent des services judiciaires du Ministère de la Justice. L'émission peut se faire depuis son adresse de messagerie nominative ou depuis une messagerie structurelle (y compris de type BAL CEP) à laquelle il est rattaché.

Le destinataire des transmissions est un Avocat, figurant dans la Table Nationale des Avocats (TNA).

Pour l'application de l'article D590 du code de procédure pénale, la TNA constitue le répertoire des avocats communiqué à la juridiction.

#### - Canal de transmission

La transmission des copies de procédures s'effectue par le biais de la mise à disposition des fichiers informatiques, déposés par un émetteur et accessibles au destinataire, sur une plateforme d'échanges sécurisée opérée par le Ministère de la Justice, dans le respect des conditions fixées à l'alinéa 3 du II de l'article 803-1 du Code de procédure pénale.

#### - Conditions de fonctionnement

L'agent des services judiciaires dépose les fichiers à transmettre sur la plateforme d'échanges sécurisée, ajoute le cas échéant des commentaires libres et valide l'opération. Cette opération est journalisée dans la plateforme.

L'agent émetteur choisit le délai durant lequel la copie de procédure pourra être téléchargée librement sur la plateforme par l'Avocat. Dans ce cadre, les Partenaires conviennent que les procédures transmises devront être laissées accessibles sur la plateforme durant un délai suffisant pour permettre à l'Avocat de procéder à leur téléchargement.

Le dépôt des copies de procédures sur la plateforme par l'émetteur entraîne la transmission d'un courrier électronique au destinataire, l'informant de la mise à disposition de la copie de procédures et l'invitant à la télécharger. Ledit courrier électronique est adressé à l'Avocat sur son adresse de messagerie nominative RPVA.

La copie de procédure ainsi déposée dans l'application est réputée transmise à la date de l'envoi dudit courrier électronique.

Pour accéder à la copie de la procédure mise à disposition et aux commentaires éventuellement saisis par l'agent émetteur, l'Avocat doit accéder à e-Barreau et s'y authentifier, prendre connaissance du message reçu et cliquer sur le lien hypertexte indiqué dans ledit message. L'Avocat pourra, alors, accéder à la plateforme d'échanges sécurisée opérée par le Ministère de la Justice, ouvrir le message qui lui a été adressé sur ladite plateforme et télécharger les fichiers informatiques contenant la copie de la procédure.

Le téléchargement de la copie de procédure, une fois terminé, donne lieu à l'émission et à la transmission d'un accusé de téléchargement des fichiers à destination de l'émetteur de la transmission de la copie de la procédure. Une fois l'accusé de téléchargement des fichiers transmis à l'expéditeur, la procédure est réputée avoir été téléchargée par l'Avocat.

#### **6.1.4 Situations particulières**

- Pluralité d'avocats saisis

Lorsqu'une partie a désigné plusieurs avocats pour l'assister, les copies de procédures sont transmises par l'émetteur à l'ensemble des avocats désignés par cette partie.

- Permanence

Sauf disposition contraire du protocole conclu localement en application de l'article 91 du décret n°91-1266 du 19 décembre 1991 portant application de la loi n° 91-647 du 10 juillet 1991 relative à l'aide juridique, les Partenaires conviennent qu'il est de bonne pratique que les procédures relevant de la permanence pénale soient adressées aux référents désignés par le Bâtonnier à ce titre.

#### **6.1.5 Durée de conservation**

L'Avocat destinataire d'une copie de procédure dont il n'est plus saisi s'engage, après transmission à son successeur éventuel, à la supprimer ou à l'archiver conformément à ses règles déontologiques.

### **Article 6.2 – Les transmissions réalisées à destination des avocats prévues par le code de procédure pénale**

#### **6.2.1 Périmètre**

Toute transmission à un Avocat, à l'exception des copies de procédures prévues ci-avant, dont les dispositions du code de procédure pénale prévoient qu'elles soient faites par lettre simple, par télécopie, par lettre recommandée ou lettre recommandée avec accusé de réception peut être effectuée par la voie électronique conformément à ce qui suit.

#### **6.2.2 Principes généraux**

Le Ministère de la Justice met à disposition des services judiciaires et des Avocats une plateforme d'échanges sécurisée permettant de procéder aux transmissions, dans les conditions prévues par le code de procédure pénale, laquelle est décrite en article 6.2.3.

#### **6.2.3 Modalités**

- Emetteur et destinataire

L'émetteur des transmissions des copies de procédures est un agent des services judiciaires du Ministère de la Justice. L'émission peut se faire depuis son adresse de messagerie nominative ou depuis une messagerie structurelle (y compris de type BAL CEP) à laquelle il est rattaché. Le destinataire des transmissions est un Avocat, figurant dans la Table Nationale des Avocats (TNA).

- Canal de transmission

La transmission s'effectue par le biais de la mise à disposition des fichiers informatiques, déposés par un émetteur et accessible au destinataire, sur une plateforme d'échanges sécurisée dans le respect des conditions fixées à l'alinéa 3 du II de l'article 803-1 du code de procédure pénale.

- Conditions de fonctionnement

L'agent des services judiciaires dépose les fichiers à transmettre sur la plateforme d'échanges sécurisée, ajoute le cas échéant des commentaires libres et valide l'opération. Cette opération est journalisée dans la plateforme. L'agent émetteur choisit le délai durant lequel le fichier pourra être téléchargé librement sur la plateforme par l'Avocat. Dans ce cadre, les Partenaires conviennent que lesdits fichiers seront mis à disposition pendant un délai qui ne pourra être inférieur à 10 jours, sans préjudice du respect des délais de convocations prévus par le Code de procédure pénale.

Le dépôt du fichier sur la plateforme par l'émetteur entraîne la transmission d'un courrier électronique au destinataire, l'informant de la mise à disposition dudit fichier et l'invitant à la télécharger. Ledit courrier électronique est adressé à l'Avocat sur son adresse de messagerie nominative.

Le fichier est réputé transmis à la date de l'envoi dudit courrier électronique.

Pour accéder au fichier ainsi mis à disposition et aux commentaires éventuellement saisis par l'agent émetteur, l'Avocat doit accéder à e-Barreau et s'y authentifier, prendre connaissance du message reçu et cliquer sur le lien hypertexte indiqué dans ledit message. L'Avocat pourra, alors, accéder à la plateforme d'échanges de fichiers sécurisée opérée par le Ministère de la Justice, ouvrir le message qui lui a été adressé sur ladite plateforme et télécharger le fichier informatique.

Le téléchargement du fichier, une fois terminé, donne lieu à l'émission et à la transmission d'un accusé de téléchargement du fichier à destination de l'émetteur de la transmission. Une fois l'accusé de téléchargement transmis à l'expéditeur, le fichier est réputé avoir été téléchargé par l'Avocat.

**Article 6.3 – Les demandes formées par les Avocats au titre de la communication électronique pénale (CEP)**

**6.3.1 Périmètre**

Les demandes formées au titre de la communication électronique pénale peuvent être adressées par les Avocats à destination de l'ensemble des Juridictions peu important leur barreau de rattachement et sans qu'il soit nécessaire d'établir un protocole local à cette fin.

Le Ministère de la Justice s'engage à fournir au CNB la liste des adresses éligibles à la CEP selon un rythme et des modalités prévus en Annexe.

Seuls les actes mentionnés aux articles D. 591 et D. 592 du code de procédure pénale peuvent être formés par voie électronique dans les conditions et selon les modalités prévues par ces dispositions.

**6.3.2 Modalités**

- Émetteur et destinataire

L'émetteur du message est un Avocat. La réception est effectuée par un agent des services judiciaires sur une BAL CEP, dont l'adresse aura été préalablement transmise au CNB par le Ministère de la Justice.



En retour, le destinataire pourra répondre à l'Avocat soit par message simple adressée depuis une BAL CEP soit, dès lors que la réponse est accompagnée de fichiers informatiques joints, uniquement par les services décrits aux articles 6.1. et 6.2.

- Canal de transmission

Les messages sont transmis par les Avocats par le biais d'un courrier électronique adressé depuis e-Barreau, mise à disposition par le CNB, et sont transmises via le canal de communication sécurisé entre les réseaux privés des Partenaires.

Ces messages ne peuvent être transmis qu'à destination des BAL de type CEP communiquées par le Ministère de la Justice au CNB. Les messages sont réceptionnés par les agents des services judiciaires sur lesdites BAL CEP.

- Conditions de fonctionnement

La réception du message sur une BAL CEP donne lieu à l'émission automatique d'un accusé de réception électronique technique adressé à l'auteur de demande.

Conformément aux dispositions de l'article D. 591 du code de procédure pénale, la date à laquelle cet accusé de réception électronique technique est adressé constitue le point de départ des délais de procédure.

Toutefois, lorsque le message a été reçu en dehors des jours ouvrables ou avant 9 heures ou après 17 heures, les délais ne commencent à courir que le premier jour ouvrable suivant.

Le fonctionnement du service est assuré de manière continue.

Néanmoins, outre les conséquences d'incidents techniques régies par l'article 9 de la présente, le service peut être interrompu temporairement à l'initiative du Ministère de la Justice lorsqu'une Juridiction rencontre des difficultés organisationnelles insurmontables empêchant le fonctionnement dudit service.

Le CNB en est informé dans les meilleurs délais et les adresses concernées par cette interruption sont rendues temporairement indisponibles. Le rétablissement du service fait également l'objet d'une information au CNB et ce dans les meilleurs délais.

## Article 7 – Dispositif de sécurité

Le Ministère de la Justice et le Conseil National des Barreaux sont responsables respectivement de la sécurité, de l'intégrité, de la disponibilité, de la confidentialité et de la traçabilité des informations échangées sur leur réseau privé, des éventuels supports sur lesquels elles seraient stockées ainsi que de la sécurité des informations communiquées entre ces deux réseaux. Les Partenaires déclarent, pour ce faire, disposer d'un système d'information sécurisé, s'engagent à respecter les obligations de la présente convention et s'engagent à faire respecter ces mêmes engagements par tout prestataire exécutant des services en lien avec la présente convention. La sécurité des informations est notamment garantie par l'utilisation de dispositifs assurant que seuls les utilisateurs agréés ont accès à ces informations.

Ces dispositifs sont conformes aux standards applicables en matière de sécurité des systèmes d'information et aux directives de l'ANSSI.

En particulier :

- le CNB assure la vérification des identités des utilisateurs qui accèdent au RPVA ainsi que la sécurité des outils et services utilisés au travers du RPVA ;
- le Ministère de la Justice assure la vérification des identités des utilisateurs qui se connectent au RPVJ ainsi que la sécurité des outils et services utilisés sur le RPVJ.

Au regard des obligations incombant au Ministère de la Justice quant à l'ouverture de son réseau vers un acteur privé, en particulier le respect de la PSSI de l'Etat, le CNB s'engage à transmettre toute information relative à sa politique de sécurité et à sa mise en œuvre au service du Haut Fonctionnaire de Défense et de Sécurité du Ministère de la Justice.

Tout évènement de sécurité (détection de vulnérabilité, exploitation d'une faille, etc.) susceptible de porter atteinte à la sécurité des informations échangées entre RPVJ et RPVA doit être partagé entre les Partenaires dans les plus brefs délais.

Lorsqu'un évènement de sécurité est jugé critique (en particulier lorsque cet évènement est susceptible de propager largement une atteinte à la sécurité de l'information) les Partenaires pourront décider de suspendre le service à titre provisoire et jusqu'à complète résolution. Cette décision devra intervenir d'un commun accord entre les Partenaires après identification de la gravité des risques encourus.

## **Article 8 – Conditions d'accès aux Services par les utilisateurs finaux**

---

### **Article 8.1 – Conditions d'accès aux Services par les avocats**

L'avocat désirant bénéficier des Services doit :

- 1) posséder un dispositif de certification permettant l'authentification des avocats ou un système d'authentification avec code de connexion unique pour l'accès au RPVA ;
- 2) posséder une adresse électronique applicative e-Barreau/RPVA (de la forme n°cnbf.nomprenom@avocatconseil.fr) ;
- 3) disposer d'un logiciel de traitement de texte et de visionnage de documents acceptant les formats de fichiers spécifiés en annexe technique ;
- 4) disposer d'un accès au réseau internet ;
- 5) pour la transmission des documents numérisés, disposer d'un appareil de numérisation pouvant générer un des formats de fichier spécifiés en annexe technique.

L'avocat doit être inscrit aux services de communications électroniques avec les juridictions dans les conditions prévues en Annexe. L'inscription aux Services emporte consentement à la dématérialisation des échanges avec la juridiction.

La TNA est mise à disposition du Ministère de la Justice régulièrement selon des modalités définies par la convention relative à la communication électronique en matière civile.

### **Article 8.2 – Conditions d'accès aux Services par les services judiciaires**

Les magistrats, les auditeurs de justice, les agents de greffe, les juristes assistants, les délégués du procureur, les assistants spécialisés, les agents administratifs et, plus largement, toute autre personne les assistant dans l'exercice de leurs missions peuvent accéder aux Services.

L'accès aux Services peut se faire soit par l'utilisation de l'adresse de messagerie individuelle des personnes concernées soit par l'utilisation d'une adresse de type structurelle à laquelle elles sont rattachées.

La liste des adresses de messagerie structurelle des Juridictions utilisées dans le cadre du service exposé à l'article 6.3 est transmise au CNB régulièrement selon des modalités techniques et organisationnelles définies en Annexe.

Pour utiliser les Services, l'utilisateur des services judiciaires doit disposer d'un accès au RPVJ.

## Article 9 – Niveaux de Services

---

Les indicateurs de Niveaux de Service ainsi que les schémas d'escalade sont décrits dans l'Annexe.

Les indicateurs de Niveaux de Service pourront être revus par les Partenaires afin de les améliorer dans une perspective d'accroissement de la fiabilité des Services.

Les prévisions contenues dans ladite annexe constituent un niveau minimum d'intervention qui ne dispense en aucun cas les Partenaires d'agir selon leurs meilleurs efforts en vue d'atteindre des niveaux de services conformes aux usages professionnels en la matière.

Toute défaillance survenant chez l'un des Partenaires fera l'objet d'une information dans les meilleurs délais, à l'autre Partenaire, lorsque ladite défaillance sera susceptible d'impacter les Services. Toute résolution d'une telle défaillance fera l'objet d'une information selon les mêmes modalités.

En cas de telles défaillances, il est procédé selon les termes prévus par les lois et règlements en vigueur.

## Article 10 – Obligations des Partenaires

---

### Article 10.1 – Obligations du Ministère

10.1.1. Le Ministère s'engage à :

- assurer et prendre en charge les coûts financiers relatifs à la maintenance évolutive des logiciels utilisés par les juridictions ordinaires de premier et de second degré dans le cadre des Services ;
- assurer l'installation et la maintenance dans les locaux de justice de ces juridictions de l'ensemble des matériels et logiciels utilisés pour la numérisation des procédures ;
- assurer les relations avec la société titulaire du marché national de maintenance.

10.1.2. D'un point de vue technique, le Ministère s'engage à :

- assurer la conception, la réalisation et la diffusion de ses applications ainsi que des matériels nécessaires auprès de ses agents. Il est responsable de la cohérence des applications au plan national ;
- mettre à disposition du Conseil national des barreaux les données techniques nécessaires à l'élaboration des systèmes de communication électronique des avocats

- assurer la transmission des listes des adresses de messagerie structurée des Juridictions selon des modalités techniques et organisationnelles définies en Annexe ;
- assurer la réception de la TNA communiquée par le Conseil national des barreaux selon les modalités décrites en Annexe. ;
- assurer la mise en œuvre du RPVJ et procéder à son exploitation quotidienne.

## **Article 10.2 – Obligations du CNB**

### **10.2.1. En contrepartie, le CNB s'engage à :**

- disposer d'une infrastructure technique permettant le raccordement de l'équipement terminal des avocats au RPVA dans les conditions définies en Annexe et à en assurer la maintenance ;
- disposer d'un logiciel chargé de l'interface d'accès des avocats aux services mis à disposition des avocats aux fins de communication électronique avec les Juridictions dans les conditions définies en Annexe et à en assurer la maintenance ;
- disposer d'une TNA à jour des avocats habilités à exercer la profession et inscrits à la communication électronique dans les conditions définies en Annexe et à en assurer la maintenance.

### **10.2.2. D'un point de vue technique, le CNB s'engage à :**

- assurer la conception, la réalisation et l'exploitation de la plateforme de services « e-barreau » mise à la disposition des avocats et des ordres ;
- assurer la mise en œuvre du RPVA et procéder à son exploitation quotidienne ;
- assurer la mise à disposition de la TNA selon les modalités définies en Annexe ;
- assurer la conception, la réalisation, l'exploitation d'une plateforme de gestion électronique de documents ayant vocation à se substituer à la plateforme actuelle en lien avec les équipes techniques de la Chancellerie.

## **Article 10.3 – Obligations réciproques**

### **10.3.1. Obligations générales**

Nonobstant les obligations prévues par la Convention, les Partenaires s'engagent réciproquement à :

- assurer la mise en œuvre de l'ensemble des mesures générales et particulières prises pour garantir la fiabilité de :
  - o l'authentification des utilisateurs parties à la communication électronique,
  - o l'identité des auteurs et l'intégrité des documents et des messages adressés par le biais des applications mises à disposition des utilisateurs aux fins de d'utilisation des Services,
  - o la sécurité et la confidentialité des échanges, et des éléments qui y sont joints, intervenant dans le cadre des Services,
  - o l'horodatage des messages envoyés et des messages reçus par les utilisateurs,
  - o des procédés de communication utilisés dans le cadre des Services ;
- disposer d'un logiciel chargé de garantir l'authentification des utilisateurs lors de leur connexion aux applications de communication électronique mises à disposition par les Partenaires et en garantir le niveau de sécurité conformément à l'état de l'art et notamment aux directives de l'ANSSI ;

- déterminer en concertation les modalités autorisant un accès unique national entre les deux réseaux privés indépendants et sauvegardant les principes de confidentialité et de secret professionnel qui permettent la réalisation des Services objet de la Convention ;
- assurer les relations avec la Commission nationale de l'informatique et des libertés pour les systèmes de communication dont sont dotés les utilisateurs.

### 10.3.2. Obligation de collaboration en cas d'évolution technique

Les Partenaires s'engagent à s'informer réciproquement des évolutions, modifications, migrations, corrections ou incidents affectant les réseaux, logiciels ou matériels utilisés par les Juridictions et les Avocats dans le cadre des Services ainsi que de toute opération de maintenance en cours ou à venir.

Par suite de cette notification, les Partenaires s'engagent à se rapprocher en vue de trouver les solutions adéquates et fourniront leurs meilleurs efforts pour prendre les arbitrages nécessaires et les mettre en œuvre pour permettre au Partenaire ayant initié l'évolution, la modification, la migration ou la correction d'aboutir dans les conditions les plus pertinentes.

Le CNB et le Ministère s'engagent également à procéder à la conduite de tests de compatibilité et de non-régression de bout en bout en cas d'évolutions prévues sur l'un ou l'autre des environnements.

Ces tests auront également vocation à permettre aux Partenaires de procéder à la recette des évolutions, modifications, migrations ou corrections considérées.

### 10.3.3. Obligation d'information

Tout changement de prestataire technique par l'un ou l'autre des Partenaires ayant un impact sur la délivrance des Services devra faire l'objet d'une notification précisant l'identité du prestataire succédant et toute information utile permettant à l'autre d'apprécier sa conformité avec l'objet des présentes. Dans la mesure du possible, les prestataires techniques choisis par l'un ou l'autre des Partenaires devront disposer de technologies compatibles avec les principes définis dans la Convention ou ses Annexes. A défaut, le Partenaire ayant pris l'initiative du changement de prestataire technique s'engage à informer l'autre Partenaire et à lui laisser un temps suffisant pour s'adapter aux modifications souhaitées. Le cas échéant, les annexes de la présente convention sont mises à jour en conséquence de ce changement de prestataire.

A défaut d'accord, les Partenaires s'engagent à agir conformément à l'article 15.

## Article 11 – Durée d'application de la Convention

La présente convention est conclue pour une durée de trois (3) ans à compter de son entrée en vigueur. Elle entre en vigueur à la date fixée par le premier arrêté pris en application de l'article 4 décret n°2020-1792 du 30 décembre 2020 relatif à la communication électronique pénale (ci-après la « Période Initiale »).

Au cours de cette période :

- elle peut être modifiée par avenant à la demande de l'un ou de l'autre des Partenaires ;
- elle peut être dénoncée par l'un ou l'autre des Partenaires uniquement en cas de faute grave et à l'expiration d'un délai d'un mois faisant suite à une mise en demeure circonstanciée adressée par lettre recommandée avec accusé de réception et non suivie d'effet.



A l'issue de cette période initiale, la Convention sera reconduite tacitement pour des périodes successives de trois (3) ans sauf dénonciation par l'un ou l'autre des Partenaires dont la notification intervenant au moins six (6) mois avant l'expiration de la période considérée par lettre recommandée avec demande d'avis de réception.

## Article 12 – Confidentialité

---

Pendant la durée de la convention ainsi qu'au cours des deux (2) ans suivant sa résiliation ou son expiration, les Partenaires s'engagent à :

- N'utiliser les informations techniques et à diffusion restreinte portées à leur connaissance dans le cadre de la Convention que dans la mesure où la Convention l'autorise et ne les transmettre de manière interne qu'aux seules personnes ayant à en connaître pour les besoins exclusifs de la fourniture des Services ;
- A ne divulguer ces mêmes informations à aucun tiers, sauf accord préalable de l'autre Partenaire. A cet égard, les Partenaires reconnaissent d'ores et déjà donner leur accord à la communication de tout ou partie de ces informations à leurs sous-traitants pour les besoins exclusifs de la fourniture des Services, à des tiers en cas de procédure d'audit, moyennant un engagement de confidentialité similaire de leur part, ainsi qu'aux organismes de la profession d'avocat ayant besoin d'en connaître;
- Prendre des mesures qui, dans leur ensemble, ne seront pas moins protectrices que les mesures qu'elles prennent pour protéger la confidentialité de leurs propres informations confidentielles ;
- Prendre toute mesure nécessaire pour avertir leur personnel respectif et leurs sous-traitants de la nature confidentielle de ces informations et des interdictions concernant leur copie ou leur divulgation.

En tout état de cause, chacun des Partenaires se porte fort du respect par les personnes morales ou physiques visées ci-dessus des dispositions de la convention.

## Article 13 – Protection des données et réglementation RGPD/directive Justice, Police

---

Dans le cadre de l'exécution de la Convention, les Partenaires seront amenés à traiter des données à caractère personnel pour des finalités et selon des moyens pouvant être distincts.

Dès lors, les Partenaires agiront respectivement en tant que responsable de traitement, au sens de la réglementation applicable en France et dans l'Union européenne dans le domaine de la protection des données à caractère personnel.

Ils respectent, chacun en ce qui les concerne, les règles applicables aux traitements qu'ils mettent en œuvre.

A ce titre, les Partenaires s'engagent à traiter les Données à caractère personnelles suivant les dispositions prévues à l'Annexe « Protection des données à caractère personnel ».

## Article 14 – Suivi et Révision de la convention

---

### Article 14.1 – Suivi de la mise en œuvre de la Convention

Les Partenaires désignent des interlocuteurs privilégiés pour centraliser toutes les informations et questions relatives à l'exécution de la convention et communiquer entre eux (ci-après les « **Interlocuteurs** »).

Toute modification des Interlocuteurs devra être indiquée à l'autre Partenaire, les Partenaires faisant leurs meilleurs efforts pour assurer leur stabilité au cours de l'exécution de la Convention.

Pendant toute la durée de la Convention, l'exécution des Services sera suivie dans le cadre d'un comité de suivi partenarial auxquels les Partenaires s'engagent à participer (ci-après le « **Comité** »). Celui-ci se tient chaque semestre, nonobstant la possibilité pour les Partenaires de convoquer des réunions extraordinaires en cas d'évolutions législatives ou réglementaires rendant nécessaire l'évolution de la convention.

Le secrétariat général du Ministère de la Justice et le Président de la commission numérique ou le Président du CNB sont chargés de composer et réunir la première instance du Comité.

Chacun des Partenaires peut inviter aux réunions du Comité susvisé toute personne dont la présence s'avérerait utile compte-tenu de l'ordre du jour proposé en amont.

Les décisions prises lors des réunions du Comité pourront modifier la Convention si les Partenaires en conviennent d'un commun accord. Dans cette hypothèse, ces modifications donneront lieu à un écrit signé des Partenaires tenant lieu d'avenant.

### Article 14.2 – Révision de la Convention

Les Partenaires conviennent de se réunir à la demande de l'une d'entre elles, chaque fois que cela sera nécessaire et, en particulier, pour procéder aux aménagements contractuels qui leur paraîtraient utiles:

Tout aménagement contractuel à la présente convention rendu ainsi nécessaire pour des motifs financiers, fonctionnels ou techniques fera l'objet d'un avenant. Tout avenant à la convention nationale sera immédiatement applicable, suivant les modalités qu'il prévoit, et en particulier un délai de prévenance suffisant pour les mettre effectivement en œuvre.

Par dérogation, des aménagements d'ordre fonctionnel ou technique pourront toutefois être apportés aux dispositions prévues aux annexes sur commun accord des partenaires sans qu'il soit nécessaire de réunir le comité. La mise en œuvre de cette modification prend effet dès que l'accord est formalisé, les Partenaires pouvant convenir d'un délai de prévenance suffisant pour sa mise en œuvre.

## Article 15 – Résolution des litiges

---

Les Partenaires s'engagent, en cas de difficultés dans l'exécution de la Convention et préalablement à toute procédure judiciaire, à tenter de résoudre amiablement leur différend.

A ce titre, le Partenaire qui souhaite mettre en jeu la procédure de résolution amiable devra notifier à l'autre Partenaire son intention de mettre en jeu ladite procédure en précisant les difficultés d'application rencontrées.

Les Partenaires s'engagent à se réunir dans un délai maximum de quinze (15) jours calendaires suivant la réception de la notification écrite précitée.

Pendant toute la période durant laquelle de telles difficultés seraient constatées, les Partenaires conviennent que la continuité des services objet de la Convention, l'emporte sur toute autre considération. En conséquence, les Partenaires s'engagent, sous réserve de leurs droits, à continuer à exécuter les services prévus à la Convention en dépit des difficultés rencontrées, dans les conditions prévues par les présentes.

## Article 16 – Documents formant l'intégralité de la Convention

La Convention est constituée :

- du présent document comportant les articles 1 à 16 ; et
- des annexes suivantes :

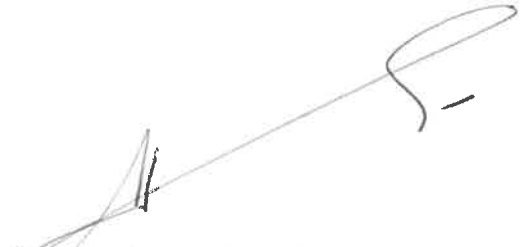

Annexe publique :

- o Annexe 1 – Description des traitements de données à caractère personnel ;

Annexes en diffusion restreinte :

- o Annexe 2 – Description du RPVJ ;
- o Annexe 3 – Description du RPVA ;
- o Annexe 4 – Description de l'interconnexion du RPVA et du RPVJ ;
- o Annexe 5 – Description des modalités de mise en œuvre des échanges entre le RPVJ et le RPVA ;
- o Annexe 6 – Description des principes d'échanges d'information
- o Annexe 7 – Spécifications des formats de fichier
- o Annexe 8 – Niveau de Services ;
- o Annexe 9 – Description du rythme et des modalités de transmission des adresses de messageries des BAL CEP et des adresses nominatives des Avocats.

Fait à Paris, le 5 février 2021,  
En deux exemplaires originaux.

 Pour le Ministère, le Garde des Sceaux	 Pour le CNB, le Président
---	---

# SPÉCIFICATIONS ANNEXÉES À LA CONVENTION

## Liste des annexes :

- Annexe publique :

Annexe 1 – Description des traitements de données à caractère personnel.

- Annexes à diffusion restreinte :

Annexe 2 – Description du RPVJ

Annexe 3 – Description du RPVA

Annexe 4 – Description de l'interconnexion du RPVA et du RPVJ

Annexe 5 – Description des modalités de mise en œuvre des échanges entre le RPVJ et le RPVA

Annexe 6 – Description des principes d'échange d'information

Annexe 7 – Spécifications des formats de fichiers

Annexe 8 – Niveaux de service

Annexe 9 – Description du rythme et des modalités de transmission des adresses de messageries des BAL CEP et des adresses nominatives des Avocats

## Annexe 1 – Description des traitements de données à caractère personnel

Dans le cadre de la Convention, les Partenaires sont chargés de préciser les obligations juridiques et financières auxquelles ils sont tenus, ainsi que les voies et moyens mis en œuvre aux fins de communication électronique, en ce compris les systèmes de consultation, d'échanges électroniques, utilisés dans le cadre des procédures pénales et les prévisions de nature organisationnelle ou opérationnelle mises en œuvre, entre les Juridictions et les Avocats.

La mise en œuvre de la communication électronique entre les Avocats et les Juridictions conduit à la transmission de données à caractère personnel issues des traitements respectivement mis en œuvre par les Partenaires.

En conséquence, chacun des Partenaires agit dans ce cadre en tant que responsable de traitement qu'il met en œuvre au sens de la réglementation applicable en France et dans l'Union Européenne dans le domaine de la protection des données à caractère personnel.

En tant que responsable de traitement, les Partenaires reconnaissent être seul responsable de la détermination de l'objet et des moyens des traitements des données à caractère personnel, chacun pour ce qui le concerne. Ils reconnaissent également être garant de l'exactitude, l'adéquation et de la complétude des informations communiquées dans le cadre des présentes, ainsi que de la licéité, loyauté, transparence des traitements des données à caractère personnel entrepris dans ce cadre.

A ce titre, les Partenaires s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractères personnel (ci-après la « Réglementation Informatique et libertés ») et en particulier :

- la loi relative à l'informatique, aux fichiers et aux libertés n° 78-17 du 6 janvier 1978 modifiée et ses éventuelles mises à jour ;
- le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) ;
- la directive n°2016/680 « Police-Justice » du 27 avril 2016, transposée en France au sein du chapitre XIII de la loi Informatique et Libertés ;
- l'arrêté du 24 octobre 2019 l'arrêté du 24 octobre 2019 autorisant la mise en œuvre d'un traitement automatisé de données personnelles dénommé « PLINE » et « PLEX » ;
- le décret n°2020-767 du 23 juin 2020 portant création d'un traitement automatisé de données à caractère personnel dénommé « dossier pénal numérique »
- le cas échéant, les dispositions issues du droit européen et/ou interne susceptibles de s'appliquer aux données à caractère personnel traitées dans le cadre de la mise en œuvre de la communication électronique en matière pénale ;
- les décisions et délibérations émanant d'autorités de contrôle, notamment de la Commission Nationale de l'Informatique et des Libertés (Cnil).

### Article 1 – Descriptions des données mises à disposition

Les Partenaires échangent les données personnelles suivantes.



### **Article 1.1 – Les données issues de la table nationale des avocats**

Il s'agit des données permettant à l'Avocat d'accéder aux services de la communication électronique pénale. Elles sont tenues à jour par l'Ordre des avocats, agissant dans le cadre de ses missions légales, dans un outil mis à disposition par l'UNCA, puis sont transmises au CNB, à l'exception des données à caractère personnel des Avocats inscrits au barreau de Paris, mises à disposition par l'Ordre de Paris directement. Ces données sont ensuite mises à la disposition du Ministère de la Justice, par le Conseil national des barreaux au travers d'une plateforme d'échanges sécurisée.

### **Article 1.2 – Les données relatives aux procédures pénales**

Il s'agit des données contenues dans les convocations, avis et procédures transmises par les juridictions aux avocats en application de la présente convention.

## **Article 2 – Régime applicable aux données mises à disposition**

---

### **Article 2.1 – La table nationale des avocats**

Les données de la table nationale des avocats sont mises à disposition du Ministère de la justice pour intégration par le traitement PLEX prévu par l'arrêté du 24 octobre 2019 autorisant la mise en œuvre d'un traitement automatisé de données à caractère personnel dénommé « PLINE » et « PLEX ».

Les principales dispositions sont les suivantes :

- Finalité

La finalité du traitement destinataire des données est la mise en place d'un système d'échanges sécurisés de fichiers entre les agents du ministère de la justice et les personnes extérieures à l'Etat.

- Durée de conservation

Les données de la table nationale des avocats sont écrasées toutes les 24 heures par la nouvelle mise à disposition.

Les adresses de courrier électronique de l'émetteur et du destinataire du fichier sont conservées dans l'application durant un an à compter de leur dernière utilisation.

- Destinataires

Les magistrats et les fonctionnaires du greffe et, le cas échéant, les avocats.

### **Article 2.2 – Les données relatives aux procédures pénales**

Ces données sont mises à disposition du CNB pour intégration dans le traitement mis en œuvre pour la communication électronique et soumises au régime suivant :

- Finalité

La finalité du traitement destinataire des données est la gestion des services de Communication électronique des Avocats avec les juridictions aux fins d'authentification, d'identification et d'échanges de messages et, plus largement, de données avec les Juridictions.

- Durée de conservation

Les données sont conservées pendant cinq ans à compter du terme de la procédure concernée par la CNB, en vertu des délais de prescription applicables au terme de l'article 2225 du code civil.

Elles sont en outre conservées par chaque avocat concerné conformément à ses règles déontologiques.

- Destinataires

L'avocat concerné et toute personne habilitée par les textes applicables sous réserve du respect du secret professionnel.

### Article 3 – Collaboration entre les Partenaires

Chaque personne concernée peut exercer ses droits dans les conditions et limites prévues par la Réglementation Informatique et libertés ainsi que les dispositions du code de procédure pénale, auprès de l'un ou l'autre des responsables de traitement.

En tout état de cause, chacun des responsables de traitement s'engage à informer l'autre, dans les meilleurs délais, de toutes de demandes relatives à l'exercice d'un droit par une personne concernée, portant directement ou indirectement sur les données mises à disposition dans le cadre des présentes. Dans cette hypothèse, ils s'engagent également à collaborer dans le cadre du traitement de la demande et, lorsque nécessaire, à fournir une réponse commune.

Le même dispositif de collaboration est mis en œuvre par les responsables de traitement dans l'hypothèse où l'un ou l'autre d'entre eux serait victime d'une violation de données au sens de la réglementation informatique et libertés.

### Article 4 – Obligations des Partenaires

Les Partenaires s'engagent à prendre toutes les mesures nécessaires au respect de leurs obligations y compris par leurs personnels, et notamment à ne pas traiter, consulter les données à caractère personnel ou les fichiers à d'autres fins que la mise en œuvre des Services et pour les finalités prévues ci-avant.

### Article 5 – Identité et coordonnées du Responsable de traitement et/ou délégué à la protection des données

Le Ministère de la Justice ainsi que le CNB, dont les coordonnées sont renseignées en tête de la présente Convention, ont respectivement la qualité de responsable de traitement.

Le délégué à la protection des données du Ministère de la Justice peut être contacté :

- Par voie postale Ministère de la Justice, DPD, 13 Place Vendôme, 75001 Paris,
- Ou par e-mail : [dpd@justice.gouv.fr](mailto:dpd@justice.gouv.fr)

Le délégué à la protection des données du CNB peut être contacté :

- Par voie postale : Conseil National des Barreaux, Délégué à la protection des données, 180 Boulevard Haussmann, 75008 Paris,
- Ou par e-mail : [donneespersonnelles@cnb.avocat.fr](mailto:donneespersonnelles@cnb.avocat.fr).

## Annexe 2 – Description du RPVJ

Le ministère de la justice s'est doté d'un réseau privé virtuel (RPVJ) en vue d'interconnecter toutes les juridictions.

Le RPVJ assure pour chaque agent du ministère la mise à disposition de services tels que la messagerie et la consultation de serveurs webs internet et intranet.

Ces services sont rendus principalement par deux plates-formes :

- Une plate-forme de services « externalisée » gérée par le prestataire désigné par le ministère de la Justice ;
- Une plate-forme de service gérée directement par le ministère de la Justice.

Ces plates-formes permettent l'interconnexion de réseaux externes tels le RPVA, les protocoles utilisés pour ces interconnexions sont HTTP et SMTP.

## Annexe 3 – Description du RPVA

Le Conseil national des barreaux s'est doté d'un réseau privé virtuel (RPVA) en vue d'interconnecter tous les cabinets d'avocats et les ordres.

Le RPVA assure pour chaque avocat, par cet accès réseau et spécifique opéré sous la responsabilité du Conseil National des Barreaux, la mise à disposition de services tels que la messagerie et l'accès à la plateforme de services du RPVA dont le service e-Barreau.

Le RPVA intègre les dispositifs de sécurité suivants :

- Une authentification des utilisateurs des services e-Barreau par certificat électronique conformément à l'état de l'art et notamment aux directives de l'ANSSI, aujourd'hui stocké sur un support physique cryptographique dédié par avocat (dispositif à mémoire avec « connectique » USB). Le processus d'authentification est partie intégrante de la politique de sécurité et de certification mise en œuvre par le Conseil national des barreaux qui assure le rôle d'Autorité d'Enregistrement Administrative et Autorité d'Enregistrement Technique (AC). L'authentification par identifiant/mot de passe avec code à usage unique (OTP) est acceptée seulement pour la préparation des messages mais la clé de certification reste obligatoire pour leur envoi.
- Des pare-feu permettent le filtrage des requêtes en provenance de la plateforme RPVA (et plus précisément du service e-Barreau) vers la plateforme RPVJ et vice-versa.

Outre ces dispositifs de sécurité, le RPVA intègre entre autres :

- Un service de messagerie e-Barreau sécurisé ;
- Une plateforme d'échange de mail de type relais SMTP ;
- Une plateforme de web services (SOAP/XML) permettant de gérer les échanges et les présentations des données par l'avocat, de générer des requêtes XML et d'intégrer les messages XML

### **1- Concernant les flux entrants en provenance du RPVJ :**

- Les réponses HTTP seront routées vers le serveur gérant l'application e-Barreau ;
- Les messages en provenance du domaine de messagerie « justice.fr » seront acheminés vers le serveur de messagerie e-Barreau. Les messages à destination des adresses structurales seront ensuite relevés par la plateforme de service e-Barreau.

Les messages en provenance du domaine de messagerie justice.fr qui arriveront par un autre canal que le RPVJ ne seront pas acheminés vers les destinataires.

### **2- Concernant les flux sortants à destination du RPVJ :**

- Les messages en provenance des utilisateurs ou de l'application e-Barreau destinés au domaine de messagerie « justice.fr » commençant par un chiffre du domaine avocat-conseil.fr sont routés vers le RPVJ.
- L'accès de l'équipement terminal des avocats au réseau privé du MJ s'effectue exclusivement à partir du RPVA via une passerelle de connexion entre les deux réseaux.

Le barreau de Paris a l'entière responsabilité de l'authentification des avocats inscrits à son barreau qui passeraient par sa plateforme d'authentification (AVOCLE) pour accéder à e-Barreau.



## Annexe 4 - Description de l'interconnexion du RPVA et du RPVJ

L'interconnexion entre le RPVA et le RPVJ est constituée par des liens installés par des prestataires désignés par le Ministère de la Justice et le Conseil National des Barreaux sur leurs infrastructures afin d'interconnecter les deux systèmes d'informations.

Le débit du lien est de 20 Mbits/seconde jusqu'à son remplacement par la double interconnexion commandée sur le marché RIE.

A ce jour, l'interconnexion avec le RPVA se fait au travers de 2 liens distincts (non redondés) :

- Un lien de 8 Mbps opéré par SFR. Ce lien sera décomissionné à court terme (hors marché).
- Un lien de 20 Mbps FO opéré par Celeste. Ce lien sera décomissionné à court terme (fin de marché).

Les liens transportent des services différents.

Un changement de marché arrivant sous peu, ces 2 liens seront remplacés par 2 liens de 40 Mbps redondés portés par le marché RIE.

### **A. Pour le ministère de la Justice, accès sur la patte Ethernet du « firewall » central du RPVJ dédié au RPVA :**

- Site du prestataire désigné par le ministère de la Justice ;
- Plateforme « Extranet justice ».

### **B. Pour les avocats, accès fibre privée sur la patte Ethernet du firewall RPVA dédié au RPVJ, authentifié au travers des certificats d'authentification Avocat :**

- Site du prestataire désigné par le Conseil National des Barreaux ;
- Plateforme « e-Barreau ».

#### • Côté justice :

Cette liaison sera raccordée côté plate-forme justice à un serveur "pare-feu" auquel est associée une plate-forme "DMZ extranet". Seuls les serveurs présents dans cette zone sont accessibles par les avocats.

Un relais SMTP :

- Les messages en provenance du domaine « avocat-conseil.fr » ne sont acceptés à travers cette liaison que s'ils proviennent du relais SMTP « e-Barreau » du RPVA ;
- Les seuls domaines visés acceptés sont : « justice.fr », « justice.gouv.fr » et « listes.justice.gouv.fr » ;
- Les messages sont redirigés ensuite vers le relais "Central" justice interne ;
- Le relais "Central" se charge enfin d'orienter les messages vers les serveurs de destination (TJ de Paris par exemple).

Un relais HTTP :

- Ce relais est le seul serveur HTTP accessible depuis le RPVA ;

- Il se charge de relayer les demandes SOAP vers le serveur civil de la juridiction concernée ;
- Il gère donc une table de correspondance entre les noms externes et des noms internes ;
- Il utilise la ligne d'en-tête Host du protocole HTTP 1.1 pour obtenir le nom du site visé (par exemple penal.ca-paris.intranet.justice.fr)
- Seuls les accès en provenance du relais du RPVA sont acceptés.

A l'introduction du RIE l'entrée dans le RPVJ sera sécurisée par la plateforme de sécurité (PFS) opérée par ce dernier. Seuls les flux mentionnés dans la matrice de référence sont autorisés par le RIE.

- **Côté avocats :**

Un relais SMTP « e-Barreau » :

- Les messages en provenance des domaines « justice.fr » et « justice.gouv.fr » ne sont acceptés que s'ils proviennent du relais SMTP du RPVJ ;
- Le seul domaine visé accepté est : « avocat-conseil.fr » ;
- Les messages sont redirigés ensuite vers la plate-forme de services e-Barreau.

Un Reverse Proxy :

- Ce relais est le seul serveur HTTP accessible depuis le RPVJ ;
- Il se charge de relayer les demandes SOAP vers le serveur pénal de la juridiction concernée ;
- Il gère donc une table de correspondance entre les noms externes et des noms internes ;
- Il utilise la ligne d'entête Host du protocole HTTP 1.1 pour obtenir le nom du site visé ;
- Seuls les accès en provenance du relais du RPVJ sont acceptés.

## Annexe 5 - Modalités de mise en œuvre des échanges entre le RPVJ et le RPVA

Tous les flux d'informations entre l'équipement terminal d'un avocat raccordé au RPVA (selon le descriptif en annexe technique) et le RPVJ transiteront exclusivement par le système de passerelle d'interconnexion reliant ces deux réseaux indépendants privés.

Les protocoles utilisés dans le RPVJ sont :

- SMTP pour le service de messagerie ;
- HTTP / SOAP pour les services web (les services web étant non usités pour l'heure au pénal).

Les protocoles utilisés dans le RPVA sont :

- SMTP pour le service de messagerie ;
- HTTP / SOAP pour les services web et HTTPS pour les échanges web.

Les pièces jointes aux messages doivent impérativement être encodées au format MIME (le format UUENCODE n'est pas supporté par l'application).

L'utilisation des procédés de signature électronique au sens du projet de directive européenne du 29 avril 1999 est différée jusqu'à la publication par le ministère de la Justice d'une politique de certification des identités numériques (PCI).

### **A) Protocole SMTP**

Les adresses pour la communication électronique pénale sont identifiées par le préfixe « cep » et hébergées par le serveur de messagerie de la cour d'appel de rattachement dont le nom de domaine est « justice.fr ».

L'adresse de la boîte aux lettres sécurisée de l'avocat est de la forme où « cnbf.nomprenom » identifie l'avocat.

La boîte aux lettres sécurisée de l'avocat est hébergée par un serveur de messagerie dont le nom de domaine est « avocat-conseil.fr ».

#### **- Le rejet des messages provenant de l'internet à destination du RPVA ou du RPVJ**

Les relais de messagerie du RPVJ sont configurés afin de rejeter tout message en provenance de l'internet ou de tout autre réseau avec une adresse dont le nom de domaine serait « avocat-conseil.fr » et de la forme cnbf.nomprenom@avocat-conseil.fr y compris à destination d'une adresse de la forme « cep.XXX@justice.fr »,

Les relais de messagerie du RPVA sont configurés afin de rejeter tout message en provenance de l'Internet ou de tout autre intranet avec une adresse dont le nom de domaine serait « justice.fr » et « justice.gouv.fr ».

Les relais de messagerie du RPVA sont configurés afin de rejeter tout message provenant de l'internet ou de tout autre réseau intranet à destination d'une adresse de messagerie cnbf.nomprenom@avocat-conseil.fr.

Les relais de messagerie du RPVJ sont configurés afin de rejeter tout message en provenance de l'internet à destination d'une adresse de la forme « cep.XXX@justice.fr ».

Les relais de messagerie du RPVJ sont configurés pour n'acheminer les messages provenant d'une adresse de la forme « cep.XXX@justice.fr », qu'à destination des boîtes aux lettres applicatives avocats ou à destination des boîtes aux lettres dédiées à la permanence pénale dans les ordres ou à destination de boîtes aux lettres internes hébergées au sein du ministère.

- **Le routage des messages**

Les relais de messagerie du RPVJ sont configurés pour forcer le routage des messages dont les destinataires appartiennent au domaine « avocat-conseil.fr » vers la passerelle d'interconnexion.

Les relais de messagerie du RPVA sont configurés pour forcer le routage des messages dont les destinataires appartiennent aux domaines « justice.fr » et « justice.gouv.fr » vers la passerelle d'interconnexion.

**B) Protocoles HTTPS et HTTP / SOAP**

Les avocats sont dans l'obligation de s'authentifier au service e-Barreau par l'utilisation de la certification assurant l'identification de l'émetteur mis en place par le Conseil National des Barreaux. L'authentification par identifiant/mot de passe avec code à usage unique (OTP) est acceptée seulement pour la lecture ou la préparation des messages mais la clé de certification reste obligatoire pour leur envoi.

La délégation d'accès à e-Barreau entre avocats est acceptée dès lors que les règles professionnelles et celles du code de procédure pénale sont respectées.

Dans le RPVJ, l'avocat est identifié par son numéro CNBF.

Pour l'heure la communication pénale ne fait pas appel à des webservices, une évolution en ce sens devrait répondre aux principes de ce paragraphe B.

## Annexe 6 - Description des principes d'échanges d'information

Les échanges entre le RPVJ et le RPVA se font dans le respect des principes suivants :

- Toute information, structurée ou non, envoyée par la juridiction du premier ou du second degré vers e-Barreau est émise sous forme d'un courrier électronique SMTP avec ou sans documents joints. Le RPVA permet en outre, notamment par le biais d'échanges avec PLEX, la transmission par la juridiction à l'avocat qui en fait la demande par les formes prescrites dans le Code de procédure pénale des procédures pénales numérisées dans lequel il est désigné, outre des avis d'audience, des notifications et plus généralement tous les actes visés à l'article 803-1 du Code de procédure pénale.
- Toute information, structurée ou non, envoyée depuis e-Barreau à la Juridiction pour y être traitée est émise sous forme d'un courrier électronique SMTP avec ou sans documents joints ;
- Chaque partie est responsable de la conception, de la réalisation et de l'exploitation des services interactifs (sites web) destinés à ses utilisateurs finaux ;
- Toute information servant à alimenter un service interactif (site web) d'une partie, détenue par l'autre partie, est obtenue par l'appel d'un service web (HTTP/SOAP) ;
- Toute information transmise devant déclencher un processus automatisé est structurée à cet effet. Pour les échanges SMTP, l'information structurée est stockée dans un fichier XML joint. Pour les échanges HTTP/SOAP, l'information structurée est transmise dans un flux XML.



## Annexe 7 – Spécifications des formats de fichier

### **1. Concernant le format de fichier d'un document numérisé**

Le format de fichier d'un document numérisé est le format PDF, conforme aux normes ISO 19005-1 (PDF/A) ou ISO 32000 (PDF 1.7). Le document est lisible et indexable par des outils libres ou gratuits.

Le nom du fichier comporte l'extension PDF.

La taille du fichier est limitée à 10 Mo au total ; pour ce faire, il est recommandé de paramétrer le scanner de la façon suivante : noir et blanc, texte seul (éviter couleur, grisé ou image), 300 dpi maximum.

Tout document de taille supérieure se verra rejeté par le système de messagerie.

### **2. Concernant le format de fichier d'un document texte**

Le nom du fichier comporte l'extension PDF ou ODT.

Si le document texte ne nécessite pas d'être modifié par un traitement de texte mais simplement consulté, copié ou imprimé, le format de fichier est PDF (Portable Document Format). Le nom du fichier comporte l'extension PDF.

Dans ce cas, le document au format PDF est un fichier dont le texte est issu d'une conversion d'un fichier produit au moyen d'un logiciel de traitement de texte au format PDF/A, conformément à la norme ISO 19005-1 qui définit le format PDF/A, rendu obligatoire par le RGI (Référentiel général d'interopérabilité) pour la conservation des documents.

Les documents au format PDF transmis sont des fichiers au format PDF/A protégés contre la modification, mais enregistrables, copiables et imprimables.

La taille du ou des fichiers joints est limitée à 10Mo. Tout document de taille supérieure se verra rejeté par le système de messagerie.

### **3. Concernant le format de fichier de données structurées**

Le format de fichier de données structurées est le format XML.

Le nom du fichier comporte l'extension XML.

## Annexe 8 – Niveaux de service

### Niveaux de services RPVJ

- 8H/18H, 5j/7, incident grave (niveau 1) : 4h ouvrées
- Déclenchement :
  - o Pour les incidents de niveau 1, SFR a une surveillance préventive et donc n'attend pas le déclenchement d'un ticket. De plus le CNB dispose d'un routeur redondé ce qui limite les cas de pannes.
  - o Pour les incidents de niveau >1 : Le délai court à réception de la demande par SFR or le CNB doit envoyer un ticket au CSI pour envoi à SFR.

*Attention toutefois, la plate-forme SFR ne gère que l'arrivée des flux RPVA (CNB) vers RPVJ, pour la transmission RPVA (CNB) vers cette plate-forme SFR cela relève d'un spécifique au CNB et donc les SLA affichées ne s'appliquent pour les incidents relevant de cette partie des échanges (resp. MJ).*

### Niveaux de services du RIE (ci-après la « Prestation concernée »)

- 24H/24, 7j/7, heures « calendaires » ;
- Détail par criticité

<b>Priorité 1</b>	Perte totale de la Prestation concernée ou dégradation de la Prestation concernée telle que le bénéficiaire n'est pas en mesure d'utiliser la Prestation concernée et est prêt à la libérer en vue de réaliser des tests immédiats.	4 heures
<b>Priorité 2</b>	Dégradation (Ex : perte d'un lien sur les 2) de la Prestation concernée lorsque le bénéficiaire est en mesure de ou souhaite continuer à utiliser la Prestation concernée et n'est pas prêt à la libérer en vue de réaliser des tests immédiats.	6 heures
<b>Priorité 3</b>	Enquête de qualité de la Prestation concernée non spécifique à une Liaison d'Accès en particulier.	12 heures
<b>Priorité 4</b>	Demande d'assistance technique du bénéficiaire portant sur le test d'un équipement et la vérification de la connectivité. Ex : il n'y a pas de coupure franche mais SFR ne détecte pas d'incident donc nécessité d'une investigation/reboot	24 heures
<b>Priorité 5</b>	Demandes du bénéficiaire n'affectant pas la Prestation concernée et autres demandes non couvertes par les catégories 1 à 4 ; ou maintenance programmée	48 heures

- Le délai de la GTR court à la création d'un ticket auprès du Pôle Hypervision du RIE, à l'initiative du CNB, du ministère de la Justice ou du Pôle Hypervision, précisant que :
  1. Le CNB a la possibilité d'activer le support du Pôle Hypervision en direct dont les coordonnées téléphonique et mél, en premier, deuxième et 3e niveau d'escalade, seront communiquées au CNB ;
  2. Le MJ a la possibilité d'activer le support du Pôle Hypervision en direct ;
  3. Le fournisseur assure une supervision proactive 24/7 de la solution au sein d'un Centre de Gestion du Réseau (CGR / NOC).

- La résilience de l'interconnexion est obtenue par un double lien en fibre optique redondée de bout en bout ;
- Bande passante garantie : 40Mb/s ;
- Latence maximale garantie : 45ms pour la data ;
- Aucune maintenance programmée ne peut avoir lieu sur les deux liens simultanément ;
- Une QOS pourra être examinée mais pour l'heure elle n'est pas nécessaire dans la mesure où seules des DATA seront traitées.

### **Alerte**

Le CNB est systématiquement alerté et informé de tout incident sur le RIE le concernant, alerte déclenché au moment de l'incident, ainsi qu'à sa résolution.

### **Pénalités**

Par ailleurs les pénalités encourues en cas de dépassement de la GTR sont déterminées, pour chaque accès, sur un mois calendaire, par cumul des durées de dépassement pour tous les manquements à la GTR observés dans le mois.

Des pénalités sont appliquées en cas de dépassement de la GTR et cela pour chaque accès, sur un mois calendaire, par cumul des durées de dépassement pour tous les manquements à la GTR observés dans le mois. Elles font partie du contrat passé par l'opérateur et sont donc soumises à confidentialité.

## Annexe 9 – Description du rythme et des modalités de transmission des adresses de messageries des BAL CEP

Pour le service prévu à l'article 6.3 de la convention, le Ministère transmet au CNB un fichier informatique de type .txt comportant notamment :

- Les adresses mail déclarées par les juridictions comme étant éligibles à la CEP ; ces adresses sont au format [cep.xxx@justice.fr](mailto:cep.xxx@justice.fr)
- L'indication de la juridiction, du service et le cas échéant du sous-service auquel l'adresse est rattachée.

Les données de ce fichier sont intégrées dans l'interface e-barreau par le CNB.

Seules les adresses figurant dans ce fichier doivent être exposées aux avocats pour leur permettre de faire usage du service exposé à l'article 6.3. Pour rappel, toute demande envoyée à une adresse ne figurant pas dans le fichier transmis par le Ministère de la Justice est irrecevable par application du décret n° 2020-1792 du 30 décembre 2020 relatif à la communication électronique pénale.

La collecte des adresses par le Ministère de la Justice, son envoi au CNB et l'alimentation d'e-barreau par ce dernier n'étant pas à ce jour automatisés, les partenaires conviennent que :

- Le Ministère de la Justice transmettra selon un rythme mensuel, le 1<sup>er</sup> lundi de chaque mois, le fichier précité comportant les adresses éligibles à la CEP ;
- Suite à cet envoi, le CNB l'intégrera dans les meilleurs délais à e-barreau et en informera immédiatement le Ministère de la Justice pour lui permettre d'en assurer la communication auprès de son réseau.

Par dérogation à ce qui précède, les Partenaires acceptent que le rythme de transmission par le Ministère de la justice puisse être plus fréquent, notamment en application des stipulations de l'article 6.3.2 de la convention, dans le cas où une juridiction souhaite interrompre temporairement le service en raison de difficultés organisationnelles insurmontables.

Dans cette hypothèse, le Ministère transmet dans les meilleurs délais au CNB un fichier des adresses actualisé ; celui-ci s'engage à assurer la mise à jour des adresses dans les meilleurs délais et en informe le Ministère de la Justice.

De la même manière, les Partenaires conviennent que le rythme de mise à jour peut exceptionnellement être plus fréquent que le rythme mensuel prévu ci-avant lors de la phase de mise en place du service prévu à l'article 6.3.

Les Partenaires manifestent leur intention d'œuvrer conjointement à la mise en place d'un service permettant d'automatiser la collecte, la transmission et l'alimentation des adresses éligibles à la CEP afin de permettre une mise à jour en temps réel de l'évolution des adresses éligibles.