

Guide d'Installation Numérique *de l'avocat*



Les outils essentiels de l'avocat

La clé RPVA



La clé RPVA (Réseau Privé Virtuel des Avocats) est indispensable pour communiquer avec les juridictions via e-Barreau.

Validité :
3 ans

Coût :
135 EUR HT

Délai moyen de
traitement :
environ 2 mois

Documents requis

- Avis de situation SIREN de moins de 3 mois (avocats individuels et collaborateurs)
- Extrait KBis de moins de 3 mois (pour les structures)
- Copie d'un justificatif d'identité en cours de validité (CNI, passeport ou carte de séjour)

Les étapes

Transmettre votre SIREN au Service Exercice Professionnel de l'Ordre (exerciceprofessionnel@barreau92.com)

Retirer la clé dans les bureaux du service professionnel de l'Ordre sur présentation d'une pièce d'identité

Commander en ligne sur ebarreau.certeurope.fr avec vos justificatifs

Activer la clé et installer le logiciel e-Barreau

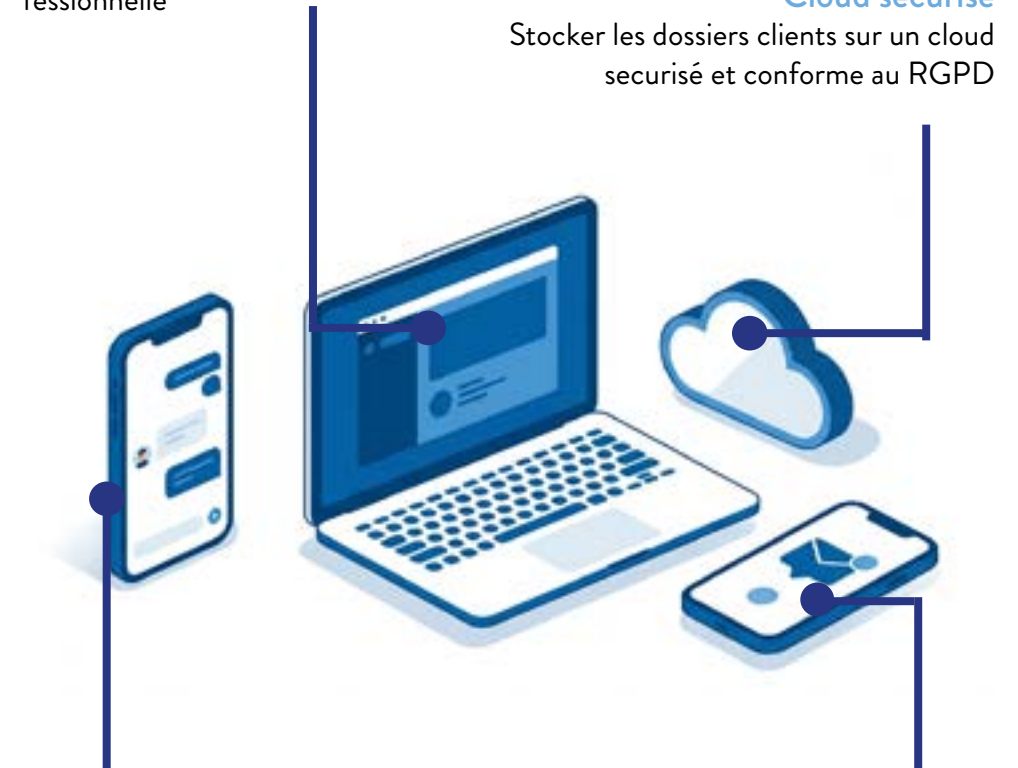
Les outils professionnels indispensables

Ordinateur dédié

Utiliser un ordinateur dédié à l'activité professionnelle

Cloud sécurisé

Stocker les dossiers clients sur un cloud sécurisé et conforme au RGPD



Messagerie séparée

Avoir une messagerie professionnelle distincte de la messagerie personnelle

Téléphone professionnel

Utiliser un téléphone professionnel distinct de votre téléphone personnel.

La Sécurité

Sécuriser sa connexion internet

VPN

Masque votre adresse IP et chiffre votre trafic.
Indispensable en déplacement ou au tribunal.

Wi-Fi sécurisé

Connexion par câble ou Wi-Fi
WPA2/WPA3 uniquement.
Ne jamais utiliser les réseaux Wi-Fi
publics sans VPN.

Mises à jour

Activez les MAJ automatiques : système, navigateur, antivirus.
Téléchargez uniquement depuis les sites ou stores officiels.

Sécuriser son matériel

Verrouillage automatique

Configurez un verrouillage automatique de votre session après 5 minutes d'inactivité. Utilisez un mot de passe pour déverrouiller votre ordinateur.

Ecran de confidentialité

Utilisez un filtre de confidentialité sur votre écran pour éviter les regards indiscrets, surtout au tribunal ou dans les transports.

Sécuriser son matériel



Chiffrement du disque

Activez BitLocker (Windows) ou FileVault (Mac) pour chiffrer l'intégralité de votre disque dur en cas de vol.

Antivirus professionnel

Installez un antivirus reconnu avec protection en temps réel, anti-phishing et mises à jour automatiques. Effectuez des analyses régulières.

Sécuriser votre téléphone

Votre smartphone contient vos emails, vos contacts clients, vos documents et parfois vos mots de passe. Il est aussi exposé aux menaces que votre ordinateur et mérite le même niveau de protection.

VPN

- Chiffre votre connexion sur les Wi-Fi publics (tribunaux, hôtels, gares)
- Empêche l'interception de vos échanges et identifiants
- Masque votre adresse IP et protège votre vie privée en déplacement

Bonnes pratiques

- Ecran de confidentialité
- Mises à jour automatiques (OS et apps)
- Ne pas installer d'application hors stores officiels



Antivirus

- Détecte les applications malveillantes avant installation
- Protège contre le phishing
- Sécurise la navigation web et bloque les sites dangereux

La Messagerie Professionnelle

Protéger vos échanges avec une messagerie compatible avec le secret professionnel

Pourquoi bien choisir sa messagerie ?

Votre messagerie est le principal vecteur d'échange de données confidentielles avec vos clients et avec vos confrères. Un mauvais choix vous expose à une violation du secret professionnel ou à la suppression inopinée des services utilisés.

Les critères essentiels d'une messagerie adaptée

- Chiffrement des messages en transit
- Hébergement des données en Europe
- Pas de lecture automatique du contenu par le fournisseur
- Authentification forte (2FA) disponible
- CGU compatibles avec le secret professionnel
- Gère les noms de domaine personnalisés



Gmail, Outlook.com, Yahoo, etc. : les messageries grand public sont incompatibles avec le secret professionnel notamment car nombre d'entre elles réalisent des analyses automatiques des données hébergées (CA Paris, 24 janvier 2025)

Nos recommandations de messagerie

Plusieurs solutions sont compatibles avec les exigences du secret professionnel. Quel que soit votre choix, assurez-vous qu'il réponde aux critères présentés précédemment. Voici nos recommandations :



Gratuit

- Fournie par le CNB
- Adresse officielle reconnue par les juridictions
- Chiffrement intégré



Payant

- Solution française, hébergement en France.
- Conforme RGPD.
- Compatible avec les noms de domaine personnalisés.



Payant

- Messagerie suisse
- Possibilité de chiffrement de bout en bout zero-access.
- Compatible avec les noms de domaine personnalisés.

Nom de domaine perso
Flexible

Créez votre propre domaine (ex. cabinet-dupontfr) et associez-le avec l'hébergement email de votre choix.

Gestion des Mots de Passe

Un mot de passe compromis peut donner accès à l'ensemble de vos dossiers clients. Le choix d'un gestionnaire de confiance est crucial : privilégiez un prestataire reconnu, avec chiffrement zero-knowledge, qui garantit que même lui ne peut pas lire vos données.

Les règles d'or



- 12 caractères minimum (majuscules, minuscules, chiffres, spéciaux)
- Un mot de passe unique par service
- Ne jamais pré-enregistrer dans le navigateur
- Activer l'authentification à deux facteurs (2FA)
- Changer immédiatement en cas de doute de compromission du mot de passe

Gestionnaire de mots de passe

Utilisez un coffre-fort numérique qui stocke et génère vos mots de passe de manière sécurisée.

Keeper	Certifié SOC 2, zero-knowledge
1Password	Interface intuitive, mode voyage
Bitwarden	Open source, gratuit ou premium

Authentification à double facteur (2FA)

La double authentification ajoute une couche de sécurité essentielle : même si votre mot de passe est compromis, l'accès reste protégé. Privilégiez une application d'authentification plutôt que le SMS, plus vulnérable aux interceptions.

Comment ça marche ?

Mot de passe + Code temporaire généré par l'application
=
Accès sécurisé

Nos recommandations :



Populaire

[Microsoft Authenticator](#)

- Application de référence, intégrée à l'écosystème Microsoft 365.
- Sauvegarde cloud
- Notifications push
- Vérification biométrique



Open source

[Aegis Authenticator](#)

- Application open source pour Android
- Chiffrement du coffre-fort local
- Import/export facile
- Interface claire et moderne.



Open source

[2FAS](#)

- Application open source multiplateforme (Android, iOS).
- Interface simple
- Sauvegarde chiffrée
- Pas de compte requis

Cloud et Sauvegarde

Vos dossiers clients sont des données protégées par le secret professionnel. Le choix du prestataire cloud est déterminant : privilégiez un hébergeur européen, et non des prestataires hors-UE, qui peuvent être soumis à des réglementations permettant à des autorités étrangères d'avoir accès à vos données (ex. Cloud Act américain).

Solutions Cloud sécurisés



Le cloud sécurisé permet le partage de fichiers volumineux avec vos clients et confrères en toute confidentialité.

Cloud du CNB



Hébergement dédié aux avocats



- Chiffrement zero-access
- Écosystème Proton
- Stockage en Suisse



- Hébergement suisse
- Suite bureautique intégrée

RGPD et Protection des Données

Le RGPD s'applique à tous les cabinets d'avocats, quelle que soit leur taille. Les avocats traitent des données souvent sensibles (condamnations pénales, données de santé, vie privée...) : la conformité n'est pas une option mais une obligation.

Vos obligations essentielles



- Tenir un registre des activités de traitement (obligatoire)
- Informer clients et salariés du traitement de leurs données
- Définir une durée de conservation pour chaque traitement
- Notifier la CNIL en cas de violation dans les 72 heures
- Assurer la sécurité et la confidentialité des données

Le registre des traitements



Document central de votre conformité, il recense tous les traitements de données personnelles (l'Ordre met à votre disposition un modèle) :

- Gestion des dossiers clients
- Gestion des ressources humaines
- Gestion des fournisseurs et prestataires
- Comptabilité du cabinet
- Site internet et communication
- Lutte anti-blanchiment (LCB-FT)

Checklist d'installation

Utiliser du matériel dédié à votre activité professionnelle
(ordinateur, téléphone)



Créer votre messagerie sécurisée



Installer un gestionnaire de mots de passe



Configurer une app 2FA



Configurer un cloud sécurisé



Commander votre clé RPVA



Activer le chiffrement du disque de votre ordinateur
(BitLocker / FileVault)



Configurer les mises à jour automatiques



Créer votre registre des activités de traitement (RGPD)



Rediger votre politique de confidentialité



La Commission Numérique vous accompagne
En cas d'interrogation
numerique@barreau92.com