Wolters Kluwer

FICHE PRODUIT RGPD

Kleos

1 Nature du traitement

Logiciel de gestion en ligne pour avocats, juriste d'entreprise, des autres professions juridique et et les départements avec une organisation basée sur des dossier.

2 Catégories de données à caractère personnel qui seront traitées

Wolters Kluwer, en tant que sous-traitant, traite exclusivement les catégories suivantes de données à caractère personnel dans le cadre du présent addendum :

- Les données d'identité (nom, prénom, nom d'utilisateur, *login*) ;
- Les coordonnées (adresses physique, électronique, téléphone, fax) ;
- Les données relatives au comportement (historique d'utilisation).

En tant que Responsable du traitement, vous avez la possibilité de saisir dans Kleos des informations personnelles supplémentaires de vos clients. Les champs de base qui sont fournis dans Kleos et qui peuvent être remplis par vous sont :

- Données d'identité (nom, adresse, GSM, e-mail, date de naissance, …) ;
- Données d'identité fournies par les pouvoirs publics (numéro de registre national, numéro de passeport…) ;
- Statut social (situation familiale…) ;
- Informations financières (numéro de compte bancaire, …) ;
- Vous pouvez toujours ajouter d'autres données personnelles supplémentaires avec la fonction "champs supplémentaires", , l'orientation et le contenu de ces champs sont sous votre entière responsabilité.

3 Catégories de personnes concernées

- Clients et associés du Responsable du traitement.
- Actionnaires, partenaires, collaborateurs et autres membres du personnel du Responsable du traitement, dont les stagiaires, les assistants de recherche etc….
- Autres personnes, telles que par exemple les parties adverses, dont les données sont traitées par le Responsable du traitement.

4 Finalités du traitement

Wolters Kluwer prévoit que vous pouvez utiliser Kleos pour les finalités suivantes :

- gestion centralisée de dossiers, coordonnées et documents ;
- connexion certifiée avec la DPA (plateforme numérique de contact avec les avocats) ;
- Kleos Connect : échange sécurisé de vos fichiers ;
- comptabilité et facturation : en vous basant sur les prestations et frais enregistrés, vous établissez automatiquement avec Kleos vos notes d'honoraires et vos factures, vous envoyez des rappels, vous établissez la déclaration à la TVA et vous créez des listings de clients ;
- lien vers vos sources internes et externes ;
- possibilités étendues de recherche et de rédaction de rapports ;
- exportation d'informations en fonction des rapports et analogues.

5 Durée de conservation

En tant que Responsable du traitement, vous fixez vous-même le délai de conservation des informations de vos clients (dossiers, données d'identité, documents, etc.).

Wolters Kluwer effectue quotidiennement une sauvegarde (*back-up*) de toutes les bases de données sur les clients. Cette copie est conservée pendant trente jours

Du côté Wolters Kluwer (sous-traitant), les données à caractère personnel sont traitées et tenues pendant les périodes suivantes :

- Après la migration de vos données depuis un autre progiciel : nous ne conservons pas d'informations après la migration au départ du progiciel précédent. Le Responsable se charge lui-même de les copier/sauvegarder et de les remettre à disposition de Wolters Kluwer en cas de nécessité ;
- Données à caractère personnel via le support/helpdesk : les contacts sont anonymisés six mois après la cessation du contrat ; vous veillez néanmoins à ne pas transmettre des données sensibles lors de la résolution de ticket (sous forme de copie d'écran, etc.) ;
- Copie de vos données au support/helpdesk : pour résoudre un problème technique, nous déplaçons une copie d'une partie déterminée de vos données vers un environnement de test après vous avoir demandé votre consentement à cet effet. Les données de la production à l'environnement de test sont transportées avec des sauvegardes cryptées, et l'environnement de test dispose à la fois du transport et du chiffrement de fichiers. Ces données servent uniquement à résoudre le problème qui s'est produit et elles sont supprimées de l'environnement de test après l'intervention ;
- après la cessation du contrat : nous remettons les données dans un format de fichier général et accessible. Ensuite, nous les conservons pendant trois mois sur nos serveurs.

6 Support/helpdesk

Pour résoudre un problème ou réaliser une configuration supplémentaire, Wolters Kluwer doit pouvoir accéder à la base de données du Responsable du traitement.

- Le Responsable peut donner au collaborateur de Wolters Kluwer l'accès à Kleos en activant le Support User dans la base de données. Le Responsable peut désactiver cette option à tout moment.
- Si l'accès aux systèmes techniques du Responsable du traitement est requis, Wolters Kluwer obtient l'accès à l'ordinateur du Responsable via le partage du PC. Cet accès à distance nécessite que le client procède à une activation en saisissant le code communiqué par Wolters Kluwer. Le Responsable du traitement doit isoler/verrouiller toutes les informations confidentielles avant d'octroyer l'accès.

7 Mesures de sécurité

Conformément à la réglementation RGDP, Wolters Kluwer prendra les mesures techniques et organisationnelles appropriées, qui seront évaluées sur la base de l'état de la technique au moment de la conclusion du contrat de prestation de services, et évaluera ces mesures dans le temps, en tenant compte des coûts de mise en œuvre, de la nature, de la portée, du contexte et des objectifs du traitement, ainsi que du risque de différences dans le degré de probabilité et de gravité des droits et libertés des personnes physiques.

DETAIL DES MESURES TECHNIQUES ET ORGANISATIONNELLES

7.1 Contrôle d'accès : bâtiments

L'accès aux bâtiments de Wolters Kluwer sera contrôlé au moyen de mesures tant techniques qu'organisationnelles : contrôle d'accès avec badges personnalisés, verrouillage électronique des portes, procédures d'accueil des visiteurs.

Le Responsable du traitement doit également s'assurer que les mesures adéquates de sécurisation et d'accès à leurs bâtiments sont prises.

7.2 Contrôle d'accès : systèmes

En tant que sous-traitant, l'accès aux réseaux, aux systèmes d'exploitation, à l'administration des utilisateurs et aux applications Wolters Kluwer nécessitera les autorisations requises: procédures avancées par mot de passe, temporisation automatique et blocage en cas de mot de passe erroné, comptes individuels avec historiques, chiffrement, pare-feu matériels et logiciels.

Le Responsable du traitement doit également s'assurer que les mesures adéquates de sécurisation de leurs mots de passes et toute autres informations d'accès électronique sont prises.

7.3 Contrôle d'accès : données

En tant que sous-traitant, l'accès aux données au sein de Wolters Kluwer est régi par des mesures organisationnelles : administration des utilisateurs et comptes utilisateurs à accès spécifique, personnel formé au traitement de données et à la sécurité, cloisonnement entre systèmes d'exploitation et environnements de test, octroi de droits spécifiques et tenue d'historiques d'utilisation, d'accès et d'effacement.

7.4 Chiffrement des données

7.4.1 Transport

La transmission de données via HTTPS est chiffrée au moyen d'un certificat PKI à clé de 2048 bits et a été certifiée par Norton.

7.4.2 Au repos

Nous chiffrons des bases de données sur des disques avec un certificat / clé privée spécifique, en utilisant l'algorithme AES

7.5 Moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constante des systèmes et services de traitement :

Pour Wolters Kluwer, le contrôle de l'accès aux données personnelles est conforme aux directives du contrôle interne, notamment la politique d'accès aux informations de l'organisation, la mise en place d'un système d'administration des utilisateurs et de droits d'accès, la sensibilisation des collaborateurs à la gestion d'informations et de leurs mots de passe, le contrôle de l'accès aux réseaux, dont la séparation des réseaux sensibles, et le contrôle de l'accès au système d'exploitation et aux applications sous-jacentes. Concrètement, les mesures consistent :

- en une structure d'autorisation écrite/programmée ;
- en droits d'accès différenciés, notamment pour lire, modifier ou effacer des données ;
- en une définition des rôles ;
- en un journal d'activités et d'audit.

Les données à caractère personnel sont cloisonnées. Les mesures consistent :

- à séparer les fonctions (données de production/de test) ;
- à isoler les données particulièrement sensibles ;
- à limiter la finalité/à appliquer un compartimentage ;
- en règles/mesures visant à garantir le stockage, la modification, la suppression et le transfert séparés de données.

Pour le Responsable du traitement, Kleos oblige l'utilisateur à utiliser un mot de passe pour s'identifier, ce qui garantit la confidentialité de toutes les données saisies dans le système de gestion. Kleos offre aussi la possibilité de gérer les niveaux de droits pour segmenter les informations accessibles au sein du cabinet du Responsable du traitement, si le Responsable le souhaite. Le Responsable du traitement est donc tenu d'instaurer des règles de confidentialité au sein du cabinet à sa propre convenance.

7.6 Moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique :

La disponibilité des données est contrôlée au moyen d'un système de surveillance permanente des réseaux. Pour empêcher que des données soient perdues, des copies de sauvegarde assorties de délais de conservation définis en sont effectuées tous les jours. D'autres mesures consistent :

• en procédures de sauvegarde ;
• en une protection contre les surtensions ;
• en une séparation du stockage physique des supports de données sauvegardées ;
• en l'écriture miroir (*mirroring*) des disques durs des serveurs (RAID) ;
• en systèmes antivirus/filtres antispam/pare-feu/système de détection d'intrusion/plan de reprise après sinistre ;
• en systèmes de protection contre l'incendie/l'eau (notamment un système d'extinction, des portes coupe-feu, des détecteurs de fumées/d'incendie)..

7.7 Procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour garantir la sécurité du traitement :

Le système Kleos est contrôlé en permanence :

- dans le cadre de la surveillance permanente, tant l'état de santé du système que les performances de l'application sont contrôlés avec précision pour chaque client ;
- chaque année, une société externe indépendante procède à des essais d'intrusion ;
- de plus, le système de détection d'intrusion est toujours actif et lance des alertes en temps réel ;
- le site web Kleos a été également certifié :
- McAfee Security contrôle Kleos minutieusement chaque jour :
    - certifie que le site est sécurisé, résistant aux virus et tentatives d'intrusion, et protégé contre les attaques de pirates sur les serveurs et la transmission de données ;
    - nous sommes informés en temps réel de risques éventuels afin de pouvoir bloquer immédiatement les attaques ;
- Norton Symantec contrôle en permanence nos transmissions de données cryptées au moyen du certificat SSL ;
    - une analyse de vulnérabilité a lieu tous les mois et le rapport y afférent nous est envoyé.

7.8 Certification disponible

Certification ISO/IEC 27001

8 Sous-traitants

Les sous-traitants prestant les services relatifs aux données à caractère personnel pour le compte de Wolters Kluwer sont les suivants :

Nom	Adresse	Finalité de l'utilisation
Teleperformance Portugal	Cais dos Argonautas Lote 2.34.01 Lisbonne – Portugal	Support du premier niveau
Capgemini Nederland B.V.	Reykjavikplein 1 3543 KA Utrecht - Nederland	Services de conseil pour l'implémentation et le développement de Salesforce
Sendinblue	Rue d'Amsterdam 55 75008 Paris France	Envoyer de factures et de rappels par e-mail.
Salesforce EMEA Limited	Floor 26 Salesforce Tover 110 Bishophsgate London EC2N 4AY - United Kingdom	Outil de suivi des tickets de support
Wolters Kluwer Global Business Services	Zuidpoolsingel 2 2408 ZE Alphen aan den Rijn Nederland	Support niveau 2 et development
Wolters Kluwer Italia	Centro Direzoniale Milanoflori Strada 1, Palazzo 6 20090 Assago - Italië	Support niveau 2 et 3 et development
T Systems	Data centre Munich/Allach Dauchauer Strasse 665 80995 München, Germany Data Centre Munich/Eip Elisabeth Selbert Strasse 1 80939 München, Germany	Datacenter

9 Transfert de données à caractère personnel

Toutes les données personnelles telles qu'elles figurent dans cette fiche produit ne seront transmises qu'aux sous-traitants susmentionnés et uniquement dans le cadre de l'exécution du présent contrat.