FICHE PRODUIT RGPD
Legisway Essentials

1. Nature du traitement

Legisway Essentials est un logiciel SaaS (Software as a service - logiciel sous la forme de service) qui enregistre les données par le biais d'un service cloud, offrant une base de données reposant sur une plateforme pour le stockage et la gestion de documents juridiques, y compris, sans s'y limiter, la gestion de contrats et interne.

2. Catégories de Données à caractère personnel traitées

Le Sous-traitant traite les catégories de Données à caractère personnel suivantes du Responsable du traitement, exclusivement dans le cadre du Contrat :

- données d'identification (nom, prénom, identifiant) ;
- coordonnées (adresse, e-mail, adresse IP, téléphone, fax) ;
- données comportementales (historique d'utilisation).

En outre, le Sous-traitant peut traiter les Données à caractère personnel émanant du Responsable du traitement. Les Données à caractère personnel créées, introduites et téléchargées dans LEgisway par le Responsable du traitement le sont à son entière discrétion et à ses propres risques. Le Sous-traitant n'a pas accès au type de Données à caractère personnel créé par le Responsable du traitement ou n'est pas en mesure de le connaître et, par conséquent, le Sous-traitant ne peut pas savoir à l'avance le type de Données à caractère personnel créé, introduit et téléchargé dans LEgisway par le Responsable du traitement. Cependant, aux fins de l'exécution du Contrat de services, les catégories de données émanant du Responsable du traitement peuvent inclure les éléments suivants :

- données d'identification (nom, adresse, téléphone mobile, e-mail, date de naissance...) ;
- données d'identification émises par les autorités (numéro de registre national, numéro de passeport...) ;
- statut social (situation familiale...) ;
- données financières (numéro de compte bancaire...).

3. Catégories de Personnes concernées

- Clients et partenaires du Responsable du traitement.
- Actionnaires, travailleurs et autres membres du personnel du Responsable du traitement , y compris les stagiaires, assistants de recherche et travailleurs non qualifiés.
- Autres personnes dont les données sont traitées par le Responsable du traitement, comme des contreparties.

4. Finalités du traitement

Le Sous-traitant stipule que LEgisway peut être utilisé pour les finalités suivantes :

- gestion centralisée des dossiers, coordonnées et documents ;
- mise en relation avec vos sources internes et externes ;

- possibilités étendues de recherche et de rapports ;
- exportation d'informations destinées aux rapports, et ainsi de suite.

5. Durée de conservation

En tant que Responsable du traitement, vous déterminez la durée de conservation des informations vous concernant (dossiers, données d'identification...).

Le Sous-traitant effectue chaque jour une sauvegarde de toutes les bases de données du Responsable du traitement. Celle-ci est conservée pour une durée de trente jours.

Les Données à caractère personnel sont traitées et conservées pour les durées suivantes :

- après la migration de vos données depuis un autre logiciel : nous ne conservons aucune information après la migration depuis l'ancien logiciel. Le Responsable du traitement lui-même est responsable de la copie/sauvegarde de ces informations et de leur mise à disposition du Sous-traitant, le cas échéant ;
- Données à caractère personnel obtenues par le biais de l'assistance technique/du service d'assistance : les contacts sont anonymisés six mois après la fin du contrat. En tant que Responsable du traitement, vous devez vous assurer de ne pas transmettre de données sensibles pendant la résolution du problème (capture d'écran...) ;
- copie de vos données dans le cadre de l'assistance technique/du service d'assistance : nous déplaçons une copie d'une partie spécifique de vos données vers un environnement de test crypté pour résoudre un problème technique. Les données de l'environnement de production sont déplacées vers l'environnement de test au moyen de sauvegardes cryptées. Par ailleurs, l'environnement de test dispose d'un cryptage du transfert et des fichiers. Votre autorisation est demandée au préalable à cet effet. Les données en question ne sont utilisées que pour résoudre le problème et sont effacées de l'environnement de test après la procédure ;
- après la fin du Contrat : nous fournissons les Données à caractère personnel dans un format de fichier général et accessible. Le Responsable du traitement doit facilement pouvoir extraire les données, y compris les Données à caractère personnel, de LEgisway dans le format de fichier général et accessible, disponible dans le système (Excel, Word...). Ensuite, nous conservons les données sur nos serveurs pendant quatre mois.

6. Assistance technique/service d'assistance/consultants

Le Sous-traitant doit avoir accès à la base de données du Responsable du traitement pour résoudre un problème ou effectuer une configuration supplémentaire.

- Le Responsable du traitement peut fournir l'accès à LEgisway au travailleur du Sous-traitant, en donnant son consentement, dans un but déterminé. Pour certains systèmes, le Responsable du traitement peut fournir l'accès à LEgisway au travailleur du Sous-traitant en activant l'option d'Accès pour l'Assistance technique dans la base de données. Le Responsable du traitement peut à tout moment désactiver cette option.
- S'il est nécessaire d'accéder aux systèmes techniques du Responsable du traitement, le Sous-traitant obtient l'accès à l'ordinateur du Responsable du traitement au moyen d'un partage de PC. Cet accès à distance nécessite l'activation par le Responsable du traitement. Cet accès à distance se fait au moyen de la saisie d'un code fourni par le Sous-traitant ou par une fenêtre contextuelle demandant votre consentement. Le Responsable du traitement est chargé de bloquer/protéger toutes les informations confidentielles avant d'accorder l'accès.

7. Mesures de sécurité

Conformément à la réglementation RGPD, le Sous-traitant prend les mesures techniques et organisationnelles appropriées, évaluées sur la base de l'état de l'art au moment de la conclusion du Contrat, et évalue ces mesures au fil du temps, en tenant compte des coûts de mise en œuvre, de la nature, de la portée, du contexte et des objectifs du traitement, et du risque de différences du degré de probabilité et de gravité pour les droits et libertés des personnes physiques.

DÉTAIL DES MESURES TECHNIQUES ET ORGANISATIONNELLES

7.1 Contrôle d'accès : bâtiments

L'accès aux bâtiments du Sous-traitant est contrôlé par des mesures à la fois techniques et organisationnelles : contrôle d'accès au moyen de badges personnalisés, verrouillage électronique des portes, procédures d'accueil des visiteurs.

Le Responsable du traitement doit également s'assurer que des mesures de sécurité et en matière d'accès à ses bâtiments adéquates sont prises.

7.2 Contrôle d'accès : systèmes

Tout accès aux réseaux, aux systèmes opérationnels, à la gestion des utilisateurs et aux applications par le Sous-traitant exige les autorisations appropriées : procédures de mot de passe avancées, expiration et blocage automatiques pour les mots de passe incorrects, comptes individuels avec historique, cryptage, pare-feu sur le matériel et les logiciels.

Le Responsable du traitement doit également s'assurer que les mesures de sécurité adéquates sont prises concernant les mots de passe et d'autres informations d'accès électroniques.

7.3 Contrôle d'accès : données

L'accès aux données par le Sous-Traitant lui-même est contrôlé par des mesures organisationnelles : gestion des utilisateurs et comptes d'utilisateurs avec accès spécifique, personnel formé au sujet du traitement et de la sécurité des données, séparation des systèmes opérationnels et des environnements de test, attribution de droits spécifiques et maintien d'historiques d'utilisation, d'accès et de suppression.

7.4 Cryptage de données

Le transfert de données HTTPS est crypté avec un certificat PKI (à clé publique) de 2048 bits et agréé par Norton.

7.5 Capacité à garantir en permanence la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement

Le contrôle de l'accès aux Données à caractère personnel suit les directives en matière de contrôle interne, notamment la politique d'accès aux informations de l'organisation, la mise en œuvre d'un système de gestion des utilisateurs et des droits d'accès, la sensibilisation des travailleurs au traitement des informations et de leurs mots de passe, le contrôle d'accès au réseau, y compris la séparation des réseaux sensibles, et le contrôle d'accès au système d'exploitation et aux applications sous-jacentes. Plus spécifiquement, les mesures comprennent :

- une structure d'autorisation écrite/programmée ;
- des droits d'accès différenciés (notamment pour la lecture, la modification, la suppression) ;
- la définition des rôles ;
- l'enregistrement/l'audit.

Les Données à caractère personnel sont isolées. Plus spécifiquement, les mesures comprennent :

- la séparation des fonctions (données de production/de test) ;
- l'isolement des données hautement sensibles ,
- la limitation des finalités/le cloisonnement ;
- des politiques/mesures pour garantir le stockage, la modification, la suppression et le transfert séparés des données.

Pour le Responsable du traitement, LEgisway requiert l'utilisation d'un mot de passe par l'utilisateur pour accéder au système LEgisway, afin de garantir la confidentialité de toutes les données introduites dans le système de gestion. LEgisway offre également la possibilité de gérer les droits des utilisateurs pour segmenter les informations accessibles au sein du système LEgisway. Le Responsable du traitement est donc tenu d'établir des règles de confidentialité au sein de l'entreprise.

7.6 Capacité à restaurer rapidement la disponibilité des Données à caractère personnel et l'accès à celles-ci en cas d'incident physique ou technique.

La disponibilité des données est contrôlée au moyen d'un système de surveillance permanente du réseau. Afin d'éviter la perte de données, une sauvegarde quotidienne des données est réalisée, avec des durées de conservation définies. D'autres mesures comprennent :

- des procédures de sauvegarde ;
- une protection contre les surtensions ;
- l'entreposage à un endroit physiquement distinct des supports de données de sauvegarde ;
- la mise en miroir des disques durs du serveur (RAID) ;
- des systèmes antivirus/filtres antispam/pare-feu/systèmes de détection des intrusions/plans de reprise après sinistre ;
- des systèmes de protection contre les incendies/inondations (y compris un système d'extinction d'incendie, des portes coupe-feu, des détecteurs de fumée/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 Sous-traitant met à la disposition du Responsable du traitement toutes les informations nécessaires en vue de démontrer le respect des obligations exposées dans le présent Contrat relatif au traitement des données et en vertu de l'article 28 du RGPD, y compris la possibilité d'examiner les rapports d'audit sur place au bureau désigné du Sous-traitant. Le Responsable du traitement n'ignore pas qu'un quelconque audit en personne et sur place est susceptible de perturber substantiellement les activités du Sous-Traitant et peut engendrer des frais notables en termes de coût et de temps. C'est pourquoi les Parties conviennent de ce qui suit :

i. le Sous-traitant permet au Responsable du traitement d'examiner le respect du présent contrat par le Sous-traitant en mettant à la disposition du Responsable du traitement, à sa demande, tout rapport d'audit déjà en sa possession ;

ii. s'il existe des indications suggérant que le Sous-traitant ne se conforme pas aux obligations qui lui incombent aux termes du présent Contrat, le Responsable du traitement peut réaliser un audit secondaire, moyennant l'accord du Sous-traitant. Les coûts d'un audit secondaire sont supportés par le Responsable du traitement, sauf si l'audit démontre un quelconque non-respect de la part du Sous-traitant (auquel cas le Sous-traitant supporte des coûts

raisonnables). Si l'audit secondaire révèle que le Sous-traitant ne se conforme pas aux obligations qui lui incombent aux termes du présent Contrat, celui-ci doit annuler et/ou rectifier sans délai les manquements identifiés lors de l'audit.

8. Fournisseurs du Sous-traitant

Le(s) fournisseur(s) du Sous-traitant suivant(s) effectue(nt) des services pour le compte du Sous-traitant concernant les Données à caractère personnel :

Nom(s) du(des) fournisseur(s) du Sous-traitant	Finalités de l'utilisation	Data localisation	Sous-sous traitant/finalités/Localisation
Wolters Kluwer Global Business Services Italia. Via dei Missaglia 97 20142 Milano, Italia	Management of Cloud	Italie	AWS Europe (Amazon EMEA SARL)/Hosting/Allemagne AWS Europe (Amazon EMEA SARL)/Hosting–recovery-Backup /Irlande
DELLA AI UK Ltd. at 5 Countess Road, NW5 2NS, London, UK	Seulement par Indexing Service*: fournisseur de services et assistance de deuxième niveau	France	Orange Business service/ hosting/France
Wolters Kluwer Deutschland GmbH Wolters-Kluwer-Straße 1 50354 Hürth	Seulement Teamdocs* (option): Fournisseur de services	Allemagne	Telekom Deutschland GmbH (Scanplus GmbH)/hosting/Allemagne
Wolters Kluwer Deutschland GmbH Robert-Bosch-Str. 6, D-50354 Hürth	Seulement for Teamdocs* (option) : assistance de deuxième niveau	Allemagne	Toppan Merrill GmbH /software editor and support level 3/Allemagne
Claranet SAS 2 Rue Breguet, 75011 Paris, France	Seulement for Mail to Legisway* (option) : Hosting and datacenter	France	Equinix/hosting/France Telecity/hosting /France
Wolters Kluwer Global business services B.V. Zuidpoolsingel 2, 2408 ZE Alphen aan den Rijn, The Netherlands	Seulement for Word2PDF* (option): Hosting and datacenter	Pay-Bas	Azure, Europe/Hosting