ANNEXE 2BIS : FICHE PRODUIT RGPD ET MESURES TECHNIQUES ET ORGANISATIONNELLES DE LEGISWAY ENTREPRISE

Le Fournisseur, en tant que Sous-traitant, est susceptible de traiter des Données à caractère personnel du Client dans le cadre de l'exécution du Contrat afin de fournir des Services logiciels et/ou des Services professionnels et, par exemple, pour offrir les services suivants :

- installation et configuration de LEGISWAY ENTREPRISE ;
- hébergement et surveillance de LEGISWAY ENTREPRISE ;
- migration de données ;
- assistance et maintenance ;
- formations des Utilisateurs.

Les dispositions de l'Accord de traitement des données (« ATD ») s'appliquent entre le Fournisseur et le Client à cet égard et sont complétées par les conditions suivantes.

TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

A. 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) ;
- adresse IP des Utilisateurs (piste d'audit).

En tant que Responsable du traitement, le Client peut encoder, conserver et manipuler dans LEGISWAY ENTERPRISE des Données de Clients liées à l'identification et la gestion des contrats et, plus généralement, des Données de Clients liées aux processus des départements juridiques des sociétés, en ce compris des Données à caractère personnel.

Dans sa configuration standard, LEGISWAY ENTERPRISE offre des champs élémentaires qui peuvent être complétés par le Client et manipule des Données à caractère personnel telles que le nom, l'adresse, le numéro de téléphone, l'adresse électronique, la date de naissance...

Des informations facultatives complémentaires peuvent aussi être encodées si cela s'avère nécessaire dans le cadre d'un processus d'entreprise donné (adresse professionnelle, téléphone professionnel) en fonction de la finalité du traitement définie par le Client. La présence de ces champs résulte d'un choix délibéré du Client lors de la phase de projet (paramètres demandés au Fournisseur par le Client) ou au cours de l'administration du Logiciel (configuration/paramétrage réalisé(e) par le Client ou par une tierce partie pour le compte du Client) et relève par conséquent exclusivement de sa responsabilité.

Dans la configuration standard de LEGISWAY ENTERPRISE, il n'y a pas de champs de commentaires libres dans le répertoire des personnes physiques. La présence d'un champ de ce type résulte d'un choix délibéré du Client lors de la phase de projet (paramètres demandés au Fournisseur par le Client) ou au cours de l'administration du Logiciel (configuration/paramétrage réalisé(e) par le Client ou par une tierce partie pour le compte du Client) et relève par conséquent exclusivement de sa responsabilité.

Les Données à caractère personnel sont encodées par les Utilisateurs par le biais des fonctionnalités du Logiciel aux fins décrites aux présentes. Les Données à caractère personnel ne sont pas directement collectées auprès des Personnes concernées elles-mêmes. Les Données à caractère personnel créées, introduites et téléchargées dans LEGISWAY ENTERPRISE par le Responsable du traitement le sont à son entière discrétion et à ses propres risques.

Le fournisseur du Sous-traitant hébergeant le cloud de LEGISWAY ENTERPRISE n'est pas agréé pour l'hébergement de données de santé. Par conséquent, le Fournisseur recommande que le Client limite la configuration de LEGISWAY ENTERPRISE en matière de données de santé dans ce cadre.

B. Catégories de Personnes concernées

LEGISWAY ENTERPRISE est susceptible de traiter des Données à caractère personnel des Personnes concernées suivantes :

- les utilisateurs utilisant LEGISWAY ENTERPRISE (généralement des collaborateurs du Responsable du traitement) ;
- les signataires, les managers, les collaborateurs en charge des achats, etc. dans le cadre des contrats (module Contrat et module DialogBox) ;
- toute tierce partie dans les informations concernant les litiges (module Litiges) ;
- les personnes de contact, cadres supérieurs, actionnaires et autres personnes ayant un lien avec une société donnée enregistrée dans LEGISWAY ENTERPRISE (module Corporate) ;
- les personnes de contact (concepteurs, inventeurs, etc.) dans les informations sur les marques et les dépôts de brevet (module PI) ;
- les personnes de contact, managers et intervenants dans les informations relatives à la gestion du site (module Site) ;
- toute tierce partie dans les informations concernant les plaintes (module Plaintes).

C. Finalité du Traitement

En tant que Responsable du traitement, le Client est chargé de définir les finalités du Traitement qu'il réalise à l'aide de LEGISWAY ENTERPRISE.

LEGISWAY ENTERPRISE peut être utilisé aux fins suivantes :

- gestion d'un référentiel de plusieurs types de dossiers d'entreprises en fonction des modules de LEGISWAY ENTERPRISE achetés par le Responsable du traitement (Contrats, Litiges, Corporate, etc.) ;
- gestion d'une liste d'entreprises (internes ou externes au groupe du Responsable du traitement) utilisées dans les dossiers d'entreprises gérés ;
- gestion d'une liste de personnes de contact au sein des entreprises gérées qui sont utilisées dans les dossiers d'entreprises gérés ;
- recherche d'informations et génération de données (graphiques ou Excel) sur la base des informations gérées.

Aucune interconnexion avec d'autres systèmes n'est requise par défaut pour que LEGISWAY ENTERPRISE fonctionne correctement et, en particulier, aucune information ne sera exportée vers d'autres systèmes depuis le répertoire de personnes physiques.

Remarque : il se peut que des interconnexions soient mises en place à la demande du Client. Ces interconnexions sont alors exécutées sous le contrôle du Client, entre LEGISWAY ENTERPRISE et les autres systèmes gérés par le Client.

D. Durée de conservation

En tant que Responsable du traitement, le Client doit déterminer la durée de conservation des Données à caractère personnel gérées par/dans LEGISWAY ENTERPRISE (dossiers des contrats, litiges, données d'identification, documents liés, etc.).

En mode « cloud », le Fournisseur sera tenu d'effectuer des sauvegardes et de les conserver conformément aux dispositions du Contrat et de la présente Annexe. En mode « sur site », le Client est responsable de la conservation et de la sauvegarde des Données des Clients.

En tant que Sous-traitant, le Fournisseur conserve lui aussi des Données de Clients, en ce compris, le cas échéant, des Données à caractère personnel dans les cas et pour les durées ci-dessous :

- des Données à caractère personnel collectées via l'assistance technique/le helpdesk (informations communiquées par le Client pour les tickets de Maintenance) : le cas échéant, les Données des Clients, en ce compris les Données à caractère personnel, seront supprimées de la base de données de l'assistance du Fournisseur six (6) mois après l'expiration du Contrat ; en tant que Responsable du traitement, le Client veillera toujours à ce qu'aucune Catégorie particulière de Données ne soit transmise au Sous-traitant lors de la notification d'une Anomalie ou de tout incident aux services d'assistance du Fournisseur (sous la forme de captures d'écran, etc.) et lors du traitement de celle-ci/celui-ci ;

- la copie de Données de Clients (DUMP) transmise au service d'assistance/helpdesk : afin de résoudre un problème technique, il se peut que le Fournisseur doive obtenir ou copier une partie des Données de Clients, en ce compris, le cas échéant, des Données à caractère personnel, dans un environnement de test après avoir demandé le consentement du Client. Ces Données de Clients sont uniquement utilisées afin de résoudre le problème en question et sont supprimées de l'environnement de test une fois que l'incident a été réglé ;

- après une migration de données : le Fournisseur conserve les Données migrées pour une durée de deux (2) mois afin de finaliser les corrections nécessaires au cours de cette période. Le Client assume la responsabilité de la copie/sauvegarde des Données et de la mise à disposition de celles-ci au Fournisseur au terme de cette période, si cela s'avère nécessaire ;

- au terme/à l'expiration du Contrat : dans le cadre des services de Réversibilité prévus au Contrat, les Données des Clients seront transmises au Client dans le format convenu. Le Fournisseur conservera alors les bases de données correspondantes pendant une durée de deux (2) mois (ou pour toute autre période telle que mentionnée dans le Contrat) sur ses serveurs avant de les détruire complètement.

MESURES DE SÉCURITÉ TECHNIQUES ET ORGANISATIONNELLES

Conformément aux Lois relatives à la protection des données en vigueur, le Fournisseur prendra les mesures de sécurité techniques et organisationnelles appropriées, qui seront évaluées sur la base de l'état des connaissances au moment de la conclusion du Contrat, et évaluera ces mesures de sécurité techniques et organisationnelles au fil du temps, compte tenu des coûts de mise en œuvre, de la nature, de la portée, du contexte et des finalités du Traitement ainsi que de sa probabilité d'engendrer un risque élevé pour les droits et libertés des Personnes concernées.

A. Contrôle d'accès : bâtiments

Sites du Fournisseur/Sous-traitant : 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 des portes, procédures d'accueil des visiteurs. En sa qualité de Responsable du traitement, le Client doit également s'assurer que des mesures de sécurité adéquates visant à empêcher l'accès à ses bâtiments soient mises en œuvre.

Sites des sous-traitants du Fournisseur (uniquement en mode CLOUD) : aux fins de l'exécution du Contrat, le sous-traitant chargé de l'hébergement est CLARANET : ses serveurs et sa plateforme sont situés en France dans l'Equinix Data Center, dans un espace réservé à CLARANET. Le serveur de base de données répliqué est également situé en France, dans un espace réservé à CLARANET.

B. Contrôle d'accès : systèmes

L'accès aux réseaux, aux systèmes opérationnels, à la gestion des utilisateurs et aux applications du Fournisseur exige les autorisations appropriées : procédures de mot de passe avancées, expiration et blocage automatiques en cas de mot de passe incorrect, comptes individuels avec historique, cryptage, pare-feu sur le matériel et les logiciels.

En tant que Responsable du traitement, le Client doit également s'assurer que des mesures appropriées soient mises en œuvre afin de protéger ses mots de passe et ses autres informations d'accès électroniques.

C. Contrôle d'accès : données

En sa qualité de Sous-traitant, le Fournisseur applique les mesures suivantes : gestion des utilisateurs et comptes d'utilisateur avec accès spécifique, personnel formé au traitement des données et à la sécurité des données, cloisonnement des systèmes opérationnels et des environnements de test, attribution de droits spécifiques et tenue de journaux d'utilisation, des accès et de suppression.

D. Cryptage des Données et protection des échanges

Les flux de données applicatives entre le Client et le Fournisseur sont cryptés par le biais du protocole HTTPS.

Pour les échanges associés à l'application de l'authentification LDAP ou SSO dans le cadre des déploiements du cloud, le Fournisseur recommande d'utiliser un tunnel IPSEC crypté.

Si le Client souhaite mettre en place des interfaces entre le Logiciel et un système qui lui est propre dans le cadre de déploiements du cloud, le Fournisseur lui recommande également d'implémenter un tunnel IPSEC crypté.

Des messages (e-mails) sont envoyés par la plateforme afin d'informer les Utilisateurs de certains événements (échéances, tâches à accomplir, etc.). Ces e-mails ne sont pas cryptés, mais ils ne contiennent aucune information sensible de l'entreprise et aucun contenu en particulier (contrat, document lié, etc.).

En option, les Fournisseurs peuvent crypter certains champs de données sensibles (correspondant à des données sensibles) dans la base de données. Si le Client a payé pour cette option, le Client et le Fournisseur définissent ensemble les champs qui doivent être cryptés. Ces champs sont cryptés et décryptés par le serveur d'applications lorsqu'un accès pour lecture et écriture est donné.

E. Développement du Logiciel

Lors du développement du Logiciel, le Fournisseur met en œuvre les bonnes pratiques recommandées par l'OWASP (www.owasp.org) et plus particulièrement les recommandations du projet « Top 10 » : https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Des tests de sécurité sont réalisés régulièrement. Les résultats de ces tests sont utilisés pour limiter davantage les risques résiduels.

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

F.1 Chez le Fournisseur

Le contrôle de l'accès aux Données à caractère personnel est conforme aux directives en matière de contrôle interne, notamment la politique d'accès aux informations de Wolters Kluwer, la mise en œuvre d'un système de gestion des utilisateurs et des droits d'accès, la sensibilisation des collaborateurs à la gestion des informations et de leurs mots de passe, le contrôle d'accès au réseau et aux applications sous-jacentes. Les mesures consistent en :

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

Les Données à caractère personnel sont cloisonnées. Les mesures comprennent :

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

Mesures propres au déploiement « sur site »

Pour les déploiements sur site, les processus essentiels liés à l'utilisation et à la sécurité relèvent de la responsabilité du Client.

Sous-traitance : aucune dans la phase d'exploitation.

Sauvegardes et restaurations : le Fournisseur recommande d'exécuter une sauvegarde quotidiennement. L'exécution et le contrôle de ces sauvegardes relèvent exclusivement de la responsabilité du Client.

Environnement de test/d'acceptation : le Fournisseur recommande au Client de disposer d'au moins deux environnements sur sa plateforme : un environnement de production et un environnement de test/d'acceptation.

Mesures propres au déploiement « cloud »

Sous-traitance : à la Date d'entrée en vigueur du Contrat, l'hébergement et l'externalisation des serveurs du Fournisseur sont sous-traités à CLARANET.
CLARANET dispose d'une certification ISO 27001 pour les activités d'hébergement qu'il offre au Fournisseur.
Sauvegardes et restaurations : les configurations des serveurs d'applications sont sauvées quotidiennement sur l'infrastructure de sauvegarde de CLARANET sur un site distant.
La base de données du Client est sauvegardée tous les jours sur la structure de sauvegarde de CLARANET se trouvant sur un site distant.
Les sauvegardes sont conservées pour une durée de quatre semaines. Les sauvegardes ne sont pas cryptées.

Environnement de test/d'acceptation : le Fournisseur recommande au Client de disposer d'au moins deux environnements sur la plateforme : un environnement de production et un environnement de test/d'acceptation.

Filtrage des accès par le biais des adresses IP : indépendamment de la sécurité garantie par la solution de gestion des identités, le Fournisseur met en œuvre pour le Client un filtrage des accès selon une liste d'adresses IP (liste blanche) correspondant aux adresses IP publiques des passerelles Internet du Client.

Isolement : l'architecture physique et logique garantit que le Client travaille dans un environnement qui est isolé et séparé des autres clients. Chaque client dispose d'une base de données dédiée et d'une instance du serveur d'applications Tomcat dédiée.

Mises à jour de sécurité : CLARANET surveille les failles de sécurité et les mises à jour y associées et fait régulièrement des recommandations au Fournisseur concernant des mises à jour de sécurité. Ces mises à jour de sécurité sont appliquées régulièrement sur la base des recommandations.

Protection antivirus : une solution antivirus est déployée et maintenue sur le Logiciel du Fournisseur.

Plan de continuité des activités (PC) *:* un plan de continuité des activités est mis en place afin d'assurer le basculement du service vers un centre de données secondaire en cas d'interruption du service sur le serveur primaire.

Procédure de gestion des incidents de sécurité : le Fournisseur met en place une procédure de gestion des incidents de sécurité prévoyant la notification de la violation de Données conformément à l'Accord de traitement des données.

Effacement des Données *:* conformément aux dispositions du Contrat.

F.2 Chez le Client

Gestion des permissions : LEGISWAY ENTERPRISE intègre des fonctions de protection des Données des Clients personnalisées dès la conception et par défaut, lesquelles permettent au Client de gérer les niveaux de droits afin de segmenter les informations accessibles aux Utilisateurs et de définir le niveau de protection adéquat en fonction des Données à caractère personnel qui seront traitées.

Les profils d'utilisateur sont attribués aux Utilisateurs par les administrateurs du Client lorsqu'ils sont intégrés/enregistrés dans le Logiciel.

Le répertoire des Données de personnes physiques est protégé au sein de la base de données du Logiciel de la même manière que toutes les Données manipulées dans le Logiciel. Ces données sont uniquement accessibles par le biais du Logiciel aux Utilisateurs qui ont reçu les autorisations correspondantes de la part du Client. En tant que Responsable du traitement, le Client est par conséquent tenu d'établir des règles de confidentialité à sa convenance et il revient au Client de définir les niveaux d'autorisation de l'Utilisateur en fonction des profils d'utilisateur.

Traçage : LEGISWAY ENTERPRISE offre une fonction de piste d'audit qui enregistre dans la base de données du Client une série d'informations concernant les accès et l'utilisation qui est faite du Logiciel par chaque Utilisateur. Ces informations comprennent en particulier un journal des connexions (réussies ou ayant échoué) ainsi que le contenu auquel l'Utilisateur a eu accès et/ou qu'il a modifié. Ces informations sont accessibles à un administrateur autorisé du Client.

Authentification : plusieurs modes de gestion des authentifications sont disponibles en fonction des options que le Responsable du traitement a souscrites :

- une authentification « simple » utilisant des noms d'utilisateur et des mots de passe définis/choisis par les utilisateurs et les administrateurs ;
- une authentification par le biais d'un lien vers le répertoire LDAP du Responsable du traitement ;
- une authentification par le biais d'une intégration avec une solution SSO (Single Sign-On) ;
- un filtrage des accès par le biais des adresses IP. (Une liste blanche qui correspond à l'adresse IP publique des passerelles Internet du Responsable du traitement).

Dans le cas de l'authentification simple via un nom d'utilisateur/mot de passe, une politique de mots de passe doit être instaurée par le Responsable du traitement. Cette politique couvre les aspects suivants :

- longueur minimum du mot de passe ;
- complexité du mot de passe ;
- interdiction de mots de passe « triviaux » ;
- expiration régulière du mot de passe.

Cryptage des Données : le Fournisseur propose une option payante afin de chiffrer certains champs de Données (dans la base de données). Le but est de faire en sorte que ces informations restent inaccessibles, même en cas de diffusion non autorisée de la base de données du Client. Si le Client achète cette option, les champs en question sont cryptés et décryptés par le serveur d'applications lorsqu'un accès pour lecture et écriture est donné. Les clés de chiffrement sont gérées au niveau du serveur d'applications.

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

Le système LEGISWAY ENTERPRISE est surveillé en permanence :

- le partenaire hébergeur du Sous-traitant CLARANET surveille en permanence les failles de sécurité et les mises à jour correspondantes et fournit régulièrement des recommandations concernant les mises à jour de sécurité au Sous-traitant. Ces mises à jour de sécurité sont appliquées régulièrement sur la base de ces recommandations ;
- une entreprise externe indépendante réalise des tests d'intrusion chaque année ;
- un système de détection des intrusions est toujours actif et donne des avertissements en temps réel ;
- une analyse de vulnérabilité est effectuée régulièrement.

FOURNISSEURS DU SOUS-TRAITANT

À compter de la Date d'entrée en vigueur du Contrat, les fournisseurs du Sous-traitant suivants effectuent des services pour le compte du Sous-traitant concernant les Données à caractère personnel.

Nom du fournisseur du Sous-traitant	Activité	Localisation des données	Fournisseur du second degré du Sous-traitant/Activité/Localisation
VP&White SAS 62 bis avenue André-Morizet, 92100 Boulogne-Billancourt	configuration	France	--
S. Blavet	configuration	France	--
Pharmadvize SARL 37 rue d'Amsterdam 75008 Paris	formation	France	--
Formateurs, personnes physiques	formation	France	--
Claranet SAS* 2 rue Breguet, 75011 Paris	Hébergement et centre de données pour Cloud ENTERPRISE	France	Equinix/hébergement/France Telecity/hébergement/France Telehouse/hébergement/France
DELLA AI UK Ltd. 5 Countess Road, NW5 2NS, London	Fournisseur de Service d'indexation Et assistance de niveau 2	France	Orange Business service/hébergement/France
Wolters Kluwer Deutschland GmbH Wolters-Kluwer-Straße 1 50354 Hürth, Germany	Fournisseur du service (optionnel) Teamdocs	Allemagne	Telekom Deutschland GmbH (Scanplus GmbH)/hébergement/Allemagne
Wolters Kluwer Deutschland GmbH Wolters-Kluwer-Straße 1, 50354 Hürth, Germany	Assistance de niveau 2 Teamdocs (optionnel)	Allemagne	Smartwork Solutions GmbH/éditeur de logiciel et assistance de niveau 3/Allemagne
Claranet SAS 2 rue Breguet, 75011 Paris	Hébergement et centre de données E-mails à Legisway (optionnel)	France	Equinix/hébergement/France Telecity/hébergement/France
Wolters Kluwer Global business services B.V. Zuidpoolsingel 2, 2408 ZE Alphen aan den Rijn, Pays-Bas	Hébergement et centre de données Word2PDF (optionnel)	Pays-Bas	Azure, Europe/Hébergement

***** CLARANET dispose d'une certification ISO 27001 pour ses activités d'hébergement et d'externalisation.