Kleos

Un environnement sûr et sécurisé pour vos données client

Chez Wolters Kluwer, la sécurité est notre priorité. Kleos est l'environnement le plus sûr et le plus sécurisé pour vos données.

Kleos est un logiciel SaaS (Software as a Service) dont le système est complétement sécurisé. Vos données sont hébergées chez T-Systems, filiale de Deutsche Telekom, une référence européenne en termes de sécurité et confidentialité des données. Les serveurs, situés en Allemagne, respectent les plus hauts niveaux de sécurité du marché ainsi que les règles de l'Union Européenne concernant la confidentialité des données.

Avec Kleos, les données de votre cabinet et de vos clients sont protégées et isolées. Chaque cabinet dispose d'une base de données privée, rien n'est partagé avec les autres cabinets.

Nous garantissons une disponibilité des données à plus de 99%, une continuité de service, et une couverture contre les sinistres. Vos données sont répliquées en temps réel sur d'autres serveurs en Allemagne et sauvegardées sur 30 jours glissants.

Tous les échanges entre les serveurs et vos postes sont cryptés en mode SSL 2048 bit, le plus haut niveau de sécurité disponible.

Kleos est également certifié par des audits quotidiens du site web et ses transmissions de données cryptées HTTPS :

McAfee® SECURE

Norton SECURED powered by Symantec

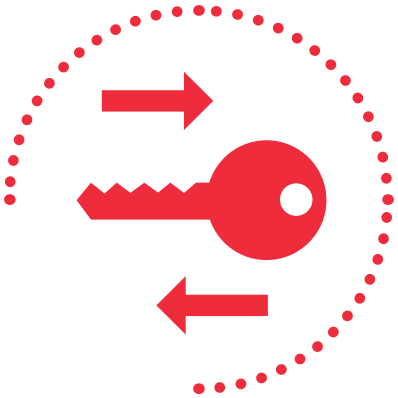
ISO 27001

Au-delà des actes de piratage, la majorité des incidents liés à la sécurité proviennent d'erreurs humaines ou d'actes délictueux des employés. Nous accordons une attention particulière à la gestion de la sécurité autour des procédures et des humains matérialisée par notre certification ISO 27001.

Tous nos services ayant trait à l'assistance Kleos, l'analyse de la qualité et la gestion des infrastructures sont soumis à un système de gestion de la sécurité de l'information certifié par l'autorité BSI qui empêche les accès non autorisés aux données confidentielles.

Information Security Management System ISO 27001 Certified

Un environnement sûr et sécurisé pour vos données client



1. PROTECTION DES TRANSMISSIONS

- **Le site hébergeant nos web services est sécurisé et certifié**
- **Protection contre les virus, les logiciels malveillants et le phishing** par des services reconnus dans la protection tels que McAfee et Norton, qui examinent aussi les autres risques de vulnérabilité.
- **Connection https sécurisée et certifiée lors de vos transferts de données.** La transmission de données, faite via le protocole HTTPS, est cryptée avec le certificat 2048-bit PKI et **certifié par Norton.**

2. PROTECTION & DISPONIBILITÉ DES DONNÉES

- **Centre d'hébergement** T-Systems de Deutsche Telekom **en Allemagne** certifié aux normes sécurité des données les plus élevées: **ISO 27 001, SAS-70 Type II.**
- **Centre d'hébergement de niveau Tier IV en conformité avec les règles européennes concernant le caractère privé des données.**
- **Disponibilité du serveur de 99,995% et accès continu à l'applicatif Kleos**, continuité de service et système supervisé 24/7.
- **Sauvegarde et récupération des données** suite à un sinistre grâce à la duplication des données sur un serveur miroir.

3. CONTRÔLES DES ACCÈS AUX DONNÉES

- Les bâtiments et serveurs sont protégés des intrusions et attaques.
- Aucun accès aux données pour les personnes non-autorisées.
- **Les données sont hermétiquement isolées de tout autre cabinet.** Chaque cabinet dispose d'une base de données privée.
- **Certification ISO 27001** de l'ensemble des processus et procédures opérationnelles de Wolters Kluwer concernant l'infrastructure, l'assurance qualité et le support niveau 3.

1. PROTECTION DES TRANSMISSIONS

Le site sur lequel sont hébergés nos webservices pour les transmissions de données est certifié par :

(1) McAfee Sécurité audite rigoureusement Kleos chaque jour afin de :

- Certifier que le site internet est résistant aux virus et intrusions et protégé des cyberattaques sur les serveurs et les transmissions de fichiers.
- Nous tenir informés en temps réel des risques en cours afin que la menace soit immédiatement neutralisée.
- Vérifiez le certificat de sécurité : *https://www.mcafeesecure.com/verify?host=kleos2.wolterskluwer.com*

(2) Norton Symantec nous fournit le certificat SSL utilisé pour chiffrer les communications entre votre ordinateur et les serveurs Kleos.

- Un examen de vulnérabilité est effectué mensuellement et un rapport nous est envoyé.
- Vérifiez le certificat de sécurité : *https://trustsealinfo.verisign.com/splash?form_file=fdf/splash.fdf&dn=kleos2.wolterskluwer.com&lang=en*
- McAfee et Norton Symantec mettent en place des tests quotidiens et mensuels afin de vérifier la fiabilité du site internet de Kleos et des transmissions de données. Tant que nous gardons ce niveau de sécurité, Kleos sera certifié conforme aux exigences de sécurité. Notre certification ISO 27001 sur le service Kleos est vérifiée et renouvelée chaque année.
- **Toutes les données transmises entre les postes de travail utilisant Kleos et les serveurs sont encryptées avec un certificat SSL 2048-bit PKI.** Ce cryptage correspond au plus haut niveau de sécurité possible après celui des banques qui sont les seules à disposer d'un niveau encore plus élevé.

2. PROTECTION & DISPONIBILITÉ DES DONNÉES

Kleos s'appuie sur l'expertise reconnue de Deutsche Telekom/T-Systems en termes de service d'hébergement pour la protection des données de votre cabinet.

- T-Systems est une entreprise certifiée de Deutsche Telekom, avec des serveurs localisés en Allemagne (Munich), en accord avec les lois européennes concernant la protection des données et les normes les plus exigeantes du marché en matière de sécurité. En conséquence les données ne sont pas soumises au Patriot Act.
- Les centres de données T-Systems disposent des certifications internationales suivantes : ISAE 3470, ISO/IEC 27001, SAS-70 Type II. Celles-ci sont alignées avec l'exigence des normes du marché.
- Les serveurs T-System, certifiés Tier IV, affichent un taux de disponibilité de 99,995%. Cette certification Tier IV est la plus haute du marché, permettant une maintenance à chaud sans arrêt de service et une tolérance aux pannes.
- Les centres de données sont protégés contre toute corruption de données, intrusion et vol de données par des périphériques hardware tels que des pare-feux, anti-virus périmétriques effectuant des analyses de paquets (Stateful Packet Inspection ou SPI) et des détections d'intrusion (Intrusion Détection ou ID).
- **Les données client sont toujours sauvegardées en double afin d'être protégées de tout type d'incidents.**

L'application Kleos est surveillée en temps réel :

- La santé du système et les performances de l'application pour chaque client sont supervisées tous les jours.
- Des tests d'intrusions sont réalisés chaque année par une société externe indépendante.
- De surcroît, un système de détection d'intrusion est toujours actif et alerte en temps réel.

Disponibilité élevée, continuité de service, couverture contre les sinistres :

- Les données client sont toujours accessibles : les composants de la technologie Kleos sont redondants à tous niveaux (stockage, serveurs de base de données, serveur applicatif).
- Haute disponibilité de l'application Kleos architecturée sous forme de cluster. Dans le cas d'une panne d'un des serveurs applicatif, l'accès à Kleos se fera de manière transparente au travers d'un autre serveur applicatif.
- Les données clients sont répliquées sur un autre serveur dans un autre centre d'hébergement T-System «miroir» (géographiquement éloigné mais toujours en Allemagne) permettant la récupération des données en cas d'accident au centre d'hébergement principal.

3. CONTRÔLES DES ACCÈS AUX DONNÉES

L'accès aux données Kleos est restreint par le contrôle du personnel et des processus au sein du centre d'hébergement et chez Wolters Kluwer.

3.1 CONTRÔLE DES ACCÈS AUX SYSTÈMES ET SERVEURS DE T-SYSTEM

Les systèmes d'hébergement de T-System sont certifiés ISO 27 001 et ISO 9 001 (version 2008).

Cela implique que tout accès aux bâtiments des centres de données est restreint et contrôlé afin de protéger vos données des risques d'intrusion et d'accidents

- Surveillance continue 24h/24, 7 jours sur 7.
- L'accès aux bâtiments se fait sous des conditions strictes et est permis exclusivement aux administrateurs possédant une accréditation spécifique (carte à puce) avec l'autorisation expresse du client concerné.
- Chaque accès est tracé et sauvegardé à travers un système externe et certifié en accord avec les lois de protection des données.
- Les bâtiments sont résistants à une attaque à l'explosif.

3.2 CONTRÔLE DES ACCÈS AUX DONNÉES KLEOS

Kleos encrypte et isole les accès aux données client.

- Les données sont hermétiquement isolées de tout autre cabinet. Chaque cabinet dispose d'une base de données privée. Il est donc impossible pour un cabinet d'accéder aux données d'un autre cabinet.
- L'accès à l'application Kleos est contrôlé par un login et un mot de passe dont le client peut contrôler la complexité et l'expiration.

Wolters Kluwer est certifié ISO 27 001 qui est la norme internationale de système de gestion de la sécurité de l'information.

- Nous avons mis en place plus d'une centaine de contrôles sur nos services Kleos basés sur les 14 catégories de l'Annexe A du certificat ISO 27001.
- Nous appliquons des procédures spécifiques relatives au certificat ISO 27001 afin de gérer la sécurité de nos services Kleos tels que le support niveau 3, l'infrastructure et l'assurance qualité.
- Les incidents, problèmes et gestion du changement concernant l'infrastructure de Kleos sont gérés à travers des processus spécifiques inspirés de l'ITIL v3 afin de protéger les données.