kanta

CONDITIONS GÉNÉRALES DE SERVICES

Dernière modification : 1er mai 2026

Les présentes Conditions Générales de Services (les « **CGS** ») sont conclues entre Kanta SAS, société par actions simplifiée, immatriculée au Registre du Commerce et des Sociétés de Caen sous le numéro 889 924 320, dont le siège social est situé 304, boulevard des Belles Portes, 14200 Hérouville-Saint-Clair, France (« **Kanta** » ou « **nous** »), et le client (le « **Client** ») (chacun étant une « **Partie** » et ensemble les « **Parties** »).

Kanta est une solution logicielle métier en mode SaaS (Software as a Service) destinée aux experts-comptables, commissaires aux comptes et professions réglementées, accessible sur la plateforme https://www.kanta.fr (la « **Plateforme** »).

La Solution Kanta propose deux modules principaux :

(**i**) **le module « LAB »** (Lutte Anti-Blanchiment) : une solution d'automatisation des procédures de conformité LCB-FT (Lutte contre le Blanchiment des Capitaux et le Financement du Terrorisme), permettant notamment l'évaluation et la classification des risques, la vigilance continue, la documentation des diligences et la préparation aux contrôles de l'Ordre ;

(**ii**) **le module « PLM »** (Prospects et Lettres de Mission) : une solution de gestion de la prospection commerciale et de génération de lettres de mission conformes aux normes de l'Ordre des experts-comptables, intégrant un tableau de bord Kanban, la récupération automatique des documents d'entreprise (RBE, statuts, justificatif d'immatriculation) et la signature électronique ;

Ces deux modules sont ci-après désignés les « **Services** », tels que décrits à l'Annexe 1 « **Description des Services** ». Le périmètre des Services souscrits par le Client est précisé dans le bon de commande (ci-après désignés le « **Bon de Commande** »).

Les Services sont fournis en mode SaaS. La Solution est hébergée par Kanta auprès de prestataires d'hébergement situés en France et est accessible par le Client et ses utilisateurs via un navigateur web. La Plateforme offre une interopérabilité avec les principaux outils métier des cabinets, via des connecteurs prêts à l'emploi et une API publique.

Le Client déclare disposer des compétences nécessaires pour comprendre les Services et s'assurer que ces derniers sont pertinents et adaptés à ses besoins. Les mises à jour, correctifs et services d'assistance technique décrits à l'Annexe 2 seront fournis conformément aux conditions des présentes conditions générales de service.

ARTICLE 1. DÉFINITIONS

« Abonnement » : désigne la formule d'accès aux Services souscrite par le Client, telle que définie dans le Bon de commande.

« Bénéficiaire Effectif » : désigne toute personne physique qui soit possède, directement ou indirectement, plus de 25% du capital ou des droits de vote de la société ou entité déclarante, soit exerce sur cette dernière, par tout autre moyen, un pouvoir de contrôle au sens des 3° et 4° du I de l'article L.233-3 du Code de commerce et dont les informations sont renseignées par le Client sur la Plateforme.

« Bon de commande » : désigne le bon de commande signé par les Parties précisant les Services souscrits, le nombre d'Utilisateurs, la durée de l'engagement, les conditions tarifaires et les conditions particulières applicables.

« Client » : désigne la personne morale identifiée dans le Bon de commande qui souscrit aux Services.

« Clients Finaux » : désigne les clients personnes physiques ou morales du Client dont les données sont traitées via la Plateforme dans le cadre de la fourniture des Services.

« Compte du Client » : désigne le compte créé par le Client sur la Plateforme pour accéder aux Services.

« Compte Utilisateur » : désigne l'espace d'accès individuel, strictement personnel et nominatif, créé au nom d'un Utilisateur désigné par le Client, permettant à celui-ci, sous la responsabilité du Client, d'accéder à la Plateforme et d'utiliser les Services au moyen de ses Identifiants propres, dans la limite du nombre de postes souscrits au Bon de commande.

« **Conditions Générales de Services » ou « CGS** » : désignent les présentes conditions contractuelles et ses annexes régissant les relations entre Kanta et le Client au titre de la fourniture des Services, de l'accès à la Plateforme et de l'utilisation de la Solution.

« Contrat » : désigne l'ensemble formé par les présentes CGS, ses annexes et le Bon de commande.

« Données du Client » : désignent l'ensemble des données, informations et documents transmis, saisis ou générés par le Client ou ses Utilisateurs dans le cadre de l'utilisation des Services, y compris les données des Clients Finaux et de leurs Bénéficiaires Effectifs, constituant des données confidentielles communiquées par le Client à Kanta dans le respect de ses obligations déontologiques.

« Données Personnelles » : désignent toute information de quelque nature que ce soit, quel que soit le type de support, se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, en vertu de la loi informatique et liberté du 6 janvier 1978 relative à la protection des personnes à l'égard du traitement des données personnelles et du Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

« Documentation » : désigne la documentation technique et fonctionnelle relative à la Solution et aux Services, mise à disposition du Client par Kanta.

« Identifiants » : désigne les identifiants de connexion (adresse e-mail et mot de passe) permettant au Client et à ses Utilisateurs d'accéder à la Plateforme et d'utiliser les Services.

« **Informations Confidentielles** » désignent toutes les informations, quel qu'en soit le support ou le mode de communication, transmises par une Partie à l'autre Partie dans le cadre de l'exécution du Contrat, dès lors qu'elles sont identifiées comme confidentielles ou que leur nature confidentielle résulte raisonnablement de leur contenu ou des circonstances de leur divulgation. Constituent notamment des Informations Confidentielles, sans que cette liste soit limitative : (**i**) pour le Client : les Données du Client, en particulier les données des Clients Finaux et de leurs Bénéficiaires Effectifs, les informations financières, commerciales et stratégiques du Client, ainsi que toute information relevant du secret Client auquel le Client est tenu ; (**ii**) pour Kanta : le code source, l'architecture technique, les algorithmes, les méthodes de traitement, les savoir-faire, les données commerciales et tarifaires non publiques, ainsi que toute information relative à la stratégie, aux projets et aux développements de Kanta.

« Lois Applicables » : désigne l'ensemble des lois, règlements et normes applicables à la fourniture et à l'utilisation des Services.

« Niveau de Risques » : désigne le niveau de risque d'une Relation d'Affaire déterminé par la Solution à partir des Données des Clients Finaux, sur la base de la Réglementation LCB-FT, en particulier des standards de la dernière version de la norme NPLAB établissant les critères de classification des risques (caractéristiques client, activité, localisation et missions effectuées).

« Plateforme » : désigne la plateforme en ligne accessible à l'adresse https://app.kanta.fr permettant aux Utilisateurs désignés par le Client d'accéder aux Services.

« Prix » : désigne le prix de l'Abonnement défini dans le Bon de commande.

« **Portefeuille Clients** » : désignent l'ensemble des Clients Finaux.

« **Rapport LCB-FT** » : désigne le rapport de risques et de vigilance d'un Client généré automatiquement suite à l'évaluation des risques d'un Client.

« **Relation d'Affaires »** : désigne la relation professionnelle ou commerciale entretenue par le Client avec le Client, et le cas échéant, le Bénéficiaire Effectif.

« **Réglementation Déontologique** » : désignent les règles et obligations professionnelles applicables aux Clients de l'expertise comptable, telles qu'elles résultent notamment de l'ordonnance n° 45-2138 du 19 septembre 1945 portant institution de l'Ordre des experts-comptables et réglementant le titre et la profession d'expert-comptable, du décret n° 2012-432 du 30 mars 2012 relatif à l'exercice de l'activité d'expertise comptable, du Code de déontologie des Clients de l'expertise comptable intégré aux articles 141 à 169 dudit décret, ainsi que des normes Clientles édictées par le Conseil supérieur de l'Ordre des experts-comptables, en ce compris les obligations relatives à la lettre de mission, au secret Client, à la prévention des conflits d'intérêts et à la lutte contre le blanchiment de capitaux et le financement du terrorisme.

« Réglementation LCB-FT » : désigne l'ensemble des dispositions législatives et réglementaires relatives à la lutte contre le blanchiment des capitaux et le financement du terrorisme, en ce compris notamment les articles L. 561-1 et suivants du Code monétaire et financier.

« RGPD » : désigne le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

« Site Internet » : désigne le site internet de Kanta présentant la Plateforme, la Solution et les Services accessibles depuis l'adresse : https://www.kanta.fr/.

« Services » : désignent les services fournis par Kanta au Client via la Plateforme, tels que décrits à l'Annexe 1 et précisés dans le Bon de commande.

« Solution » : désigne la solution logicielle de respect des obligations réglementaires des experts-comptables développée et exploitée par KANTA.

« Tableau de Bord » : désigne l'espace personnel du Client auquel celui-ci et/ou ses Utilisateurs accèdent depuis leur Compte.

« Utilisateur » : désigne toute personne physique autorisée par le Client et sous sa responsabilité à accéder et à utiliser les Services au moyen d'un Compte.

kanta

ARTICLE 2. OBJET ET DOCUMENTS CONTRACTUELS

2.1. Objet. Les présentes CGS ont pour objet de définir les conditions dans lesquelles Kanta fournit au Client l'accès à la Solution et aux Services, ainsi que les droits et obligations de chaque Partie.

2.2. Documents contractuels. Le Contrat est constitué des documents suivants, par ordre de prévalence décroissant en cas de contradiction :

(**a**) le(s) Bon(s) de commande ;

(**b**) les présentes CGS ;

(**c**) les Annexes aux présentes CGS :

- Annexe 1 : description des Services
- Annexe 2 : niveau des Services
- Annexe 3 : accord de traitement des données personnelles
- Annexe 4 : plan d'assurance sécurité

2.3. Conflits. En cas de contradiction entre les stipulations des documents contractuels, les stipulations du document de rang supérieur prévaudront. Le Bon de commande prévaut donc sur les CGS et les Annexes.

Le Contrat exprime l'intégralité de l'accord des Parties et annule et remplace tout accord, lettre, offre ou autre document écrit ou oral antérieur ayant le même objet.

En cas d'invalidité d'une ou plusieurs stipulations du Contrat en vertu d'une loi, d'un règlement ou en application d'une décision définitive d'une juridiction compétente, celle-ci sera sans aucune conséquence sur la validité et l'effectivité des autres stipulations du Contrat.

ARTICLE 3. LICENCE

3.1. Mise à disposition. Kanta met la Solution à disposition du Client sous forme électronique en mode SaaS.

3.2. Licence d'utilisation. Kanta concède au Client, pour la durée du Contrat, une licence non exclusive, non transférable, non cessible et sans redevance supplémentaire au-delà du Prix de l'Abonnement, d'accès et d'utilisation de la Solution et des Services via la Plateforme pour ses seuls besoins Clients internes, dans le respect des termes du Contrat.

3.3. Utilisateurs autorisés. Le Client peut désigner ses collaborateurs, salariés ou prestataires en qualité d'Utilisateurs, dans la limite du nombre de postes prévu au Bon de commande. Chaque Compte Utilisateur est strictement personnel et ne peut être utilisé que par un seul Utilisateur. Tout contournement de cette règle pourra donner lieu à la facturation de postes supplémentaires ou à la résiliation du Contrat aux torts du Client. Le Client est responsable de l'ensemble des usages des Services réalisés par ses Utilisateurs et du respect des présentes CGS par ces derniers. Le Client s'engage à notifier Kanta sans délai de tout accès ou usage non autorisé dont il aurait connaissance.

ARTICLE 4. ACCÈS AUX SERVICES

4.1. Accès aux Services. Le Client accède aux Services, tel que décrits en Annexe 1 et dont le périmètre varie en fonction de l'Abonnement souscrit, tel que précisé dans le Bon de commande depuis la Plateforme de Kanta.

4.2. Comptes. Le premier accès aux Services s'effectue au moyen du Compte du Client créé sur la Plateforme. Le Client désigne un ou plusieurs administrateurs, responsables de la création des Comptes Utilisateurs, de la gestion des droits d'accès et de la supervision des Utilisateurs, y compris de leur affectation aux dossiers des Clients Finaux.

Le Client peut désigner en qualité d'Utilisateurs ses collaborateurs, salariés ou prestataires, dans la limite du nombre de postes prévu au Bon de commande. Chaque Compte Utilisateur est strictement personnel et ne peut être utilisé que par un seul Utilisateur. Tout partage de Compte Utilisateur ou contournement de cette règle pourra donner lieu à la facturation de postes supplémentaires et, le cas échéant, à la résiliation du Contrat dans les conditions prévues à l'article 14.

4.3. Sécurité des accès. La double authentification (MFA) est obligatoire pour l'ensemble des Utilisateurs. Le Client veille à ce que chaque Utilisateur crée des mots de passe robustes, uniques et strictement confidentiels.

Le Client est responsable de la sécurité et de la confidentialité des Identifiants de ses Utilisateurs ainsi que de l'ensemble des usages des Services réalisés au moyen de ces Identifiants. Toute référence au Client dans les présentes CGS s'applique, en tant que de besoin, à ses Utilisateurs.

4.4. Accès non autorisé. Le Client s'engage à notifier Kanta sans délai de tout accès ou usage non autorisé dont il aurait connaissance. La responsabilité de Kanta ne saurait être engagée en cas d'accès frauduleux résultant d'un manquement du Client ou de ses Utilisateurs à leurs obligations au titre du présent article. Kanta se réserve le droit de suspendre l'accès au Compte Utilisateur concerné et de prendre toute mesure conservatoire appropriée.

ARTICLE 5. UTILISATION ET ÉVOLUTION DES SERVICES

5.1. Utilisation des Services. Le Client s'engage à utiliser les Services conformément à leur destination, au Contrat et aux Lois Applicables. Le Client se porte fort du respect des présentes stipulations par ses Utilisateurs et répond de tout manquement de ces derniers comme du sien propre.

Le Client et ses Utilisateurs s'interdisent notamment :

- de concéder une sous-licence, revendre, distribuer, mettre à disposition ou exploiter commercialement tout ou partie des Services, de la Plateforme ou de la Solution auprès de tiers ;
- de copier, modifier, adapter, traduire, désassembler, décompiler ou procéder à de l'ingénierie inverse de la Solution, sauf dans les cas expressément autorisés par les Lois Applicables ;
- de contourner, désactiver ou interférer avec les dispositifs de sécurité ou d'authentification de la Plateforme ;
- de procéder ou tenter de procéder à des intrusions dans les systèmes de Kanta, ou d'accéder à des données ou fonctionnalités auxquelles le Client n'est pas autorisé à accéder ;
- d'imposer une charge disproportionnée sur les infrastructures de Kanta ou de mener toute action de nature à interrompre, suspendre, ralentir ou empêcher le bon fonctionnement de la Plateforme ou des Services ;
- d'utiliser les Services à des fins illicites, frauduleuses ou portant atteinte aux droits des tiers ou à l'ordre public ;
- d'excéder le nombre d'Utilisateurs autorisés dans le Bon de commande ou de partager des Identifiants en violation de l'article 4.2 ;
- plus généralement, de commettre tout acte de nature à porter atteinte aux droits et intérêts financiers, commerciaux ou moraux de Kanta ou des autres utilisateurs de la Plateforme.

5.2. Évolution de la Solution et des Services. Kanta se réserve le droit de faire évoluer la Solution et les Services afin de créer de nouvelles fonctionnalités ou d'améliorer les fonctionnalités existantes.

Kanta s'engage à ce que les évolutions de la Solution et des Services n'entraînent pas de dégradation substantielle des fonctionnalités existantes. Toute modification significative sera communiquée au Client dans un délai raisonnable préalable à sa mise en production.

Si une évolution entraîne une modification tarifaire, Kanta en informera le Client dans un délai raisonnable permettant à ce dernier de décider de la poursuite du Contrat aux nouvelles conditions. Le Client sera en droit de résilier le Contrat dans les conditions prévues à l'article 14.2.

5.3. Services Tiers. Le Client peut être amené à connecter des services tiers à la Plateforme.

Le Client est seul responsable de l'activation de ces connexions et de tout traitement de données, en ce compris les Données Personnelles, résultant de l'utilisation de ces services tiers dans le cadre du Contrat. Il lui appartient de s'assurer que le recours à ces services tiers est conforme aux Lois Applicables et, le cas échéant, à ses obligations déontologiques, notamment en matière de secret Client.

Kanta ne saurait être tenue responsable du fonctionnement, de la disponibilité ou de la sécurité des services tiers, ni du traitement des données opéré par leurs fournisseurs. En cas d'interruption ou de modification d'un service tiers affectant les Services, Kanta en informera le Client dans les meilleurs délais.

ARTICLE 6. CONDITIONS FINANCIÈRES

6.1. Abonnement. En contrepartie de l'accès et de l'utilisation des Services, le cas échéant à compter de la Période d'Essai, le Client s'acquitte du prix de l'Abonnement indiqué dans le Bon de commande (le « **Prix de l'Abonnement** »). Sauf indication contraire dans le Bon de commande, le Prix de l'Abonnement est exprimé hors taxes et soumis à la TVA au taux en vigueur. Il inclut le prix des redevances pour la licence d'utilisation de la Solution.

6.2. Règlement. Le Prix de l'Abonnement est facturé mensuellement, sauf stipulation contraire prévoyant une facturation annuelle dans le Bon de commande. Les factures sont payables à réception par le Client. Le règlement s'effectue par prélèvement automatique SEPA, sauf mode de paiement alternatif expressément convenu dans le Bon de commande. Le Client s'engage à fournir ses coordonnées bancaires (IBAN et BIC) et à signer le mandat de prélèvement SEPA correspondant, sous format papier ou électronique, préalablement à la première échéance. À compter de la mise en place du mandat SEPA, le Client accepte que l'ensemble du Prix de l'Abonnement soit régi par une autorisation de prélèvement commune et unique.

6.3. Retard et défaut de règlement. Toute somme non réglée à son échéance produit de plein droit et sans qu'une mise en demeure soit nécessaire : (a) des pénalités de retard calculées au taux annuel égal à trois (3) fois le taux d'intérêt légal en vigueur, appliqué sur le montant TTC restant dû, à compter du jour suivant la date d'échéance jusqu'à la date de paiement effectif ; (b) une indemnité forfaitaire de quarante (40) euros pour frais de recouvrement, conformément aux articles L. 441-10 et D. 441-5 du Code de commerce. Lorsque les frais de recouvrement réellement exposés sont supérieurs à ce montant forfaitaire, Kanta pourra demander une indemnisation complémentaire sur justificatifs.

Si le retard de paiement excède trente (30) jours à compter de la date d'échéance, Kanta se réserve le droit, à sa seule discrétion et après notification préalable au Client, de suspendre l'accès à la Plateforme et aux Services jusqu'au règlement intégral des sommes dues, majorations comprises. Cette suspension ne saurait ouvrir droit à indemnisation au profit du Client ni le décharger de ses obligations de paiement au titre du Contrat.

Le défaut de paiement non régularisé dans un délai de trente (30) jours suivant la réception d'une mise en demeure adressée par Kanta par lettre recommandée avec accusé de réception ou par tout moyen conférant date certaine constitue un manquement grave du Client au Contrat, susceptible d'entraîner la résiliation du Contrat dans les conditions prévues à l'article 14.

Les sommes facturées restent intégralement dues nonobstant la résiliation du Contrat.

6.4. Révisions tarifaires. Le Prix de l'Abonnement est révisé de plein droit, une fois par an à la date anniversaire du Contrat, par application du dernier indice Syntec publié à la date de la révision, sauf clause contraire indiquée au Bon de Commande.

Kanta notifie au Client le nouveau prix résultant de l'indexation au moins trente (30) jours avant sa date d'anniversaire. Le Client dispose d'un délai de trente (30) jours calendaires à compter de la réception de la notification pour refuser la révision tarifaire par l'envoi d'une notification écrite à Kanta. Dans ce cas, le Contrat prendra fin de plein droit à la date d'anniversaire du Contrat, sans indemnité de part ni d'autre. Pendant ce même délai, le Client peut solliciter un échange avec son interlocuteur Kanta, étant précisé qu'une telle sollicitation ne vaut pas, en elle-même, refus de la révision et ne suspend pas le délai de trente (30) jours. À défaut de notification de refus adressée à Kanta dans le délai de trente (30) jours, le Prix révisé est réputé définitivement accepté par le Client et s'applique à compter de la date d'effet indiquée dans la notification, sans qu'il soit nécessaire de signer un avenant au Bon de commande.

ARTICLE 7. DÉCLARATIONS

7.1. Déclarations de Kanta. Kanta déclare et garantit : (**i**) disposer de tous les droits nécessaires pour fournir les Services, en ce compris l'ensemble des droits de propriété intellectuelle sur la Solution ; (**ii**) que les Services seront fournis conformément aux pratiques professionnelles généralement reconnues et conformément aux Lois Applicables.

7.2. Déclarations du Client. Le Client déclare et garantit : (**i**) avoir valablement conclu le Contrat et disposer du pouvoir légal de le faire ; (**ii**) que la conclusion du Contrat ne contrevient à aucune obligation préexistante du Client.

ARTICLE 8. GARANTIES

8.1. Général. Sous réserve des stipulations particulières du présent article relatives aux Modules LAB et PLM et des engagements de niveaux de service définis à l'Annexe 2, les Services sont fournis « en l'état » et « selon disponibilité », sans garantie d'aucune sorte dans les limites les plus larges autorisées par les Lois Applicables. Kanta exclut expressément toute garantie, expresse ou implicite, y compris, sans que cette liste soit limitative, toute garantie implicite de qualité marchande ou d'adéquation à un usage particulier. Le Client reconnaît que Kanta ne garantit pas que la Plateforme et les Services fonctionneront de manière ininterrompue et sera exempte d'erreurs ou exempte de virus, et qu'aucune information ou conseil obtenu par le Client auprès de Kanta ou au travers des Services ne saurait créer une garantie non expressément stipulée au Contrat. Kanta ne saurait être tenue responsable des difficultés ou impossibilités d'accès à la Plateforme ou aux Services ayant pour origine des circonstances extérieures à Kanta, la force majeure, des perturbations des réseaux de télécommunication, ou le fait du Client ou de ses Utilisateurs.

8.2. Services LAB et PLM. Pour les Clients ayant souscrit au Service LAB, Kanta garantit que la Solution intègre les fonctionnalités permettant de répondre aux exigences de la Réglementation LCB-FT, fondées notamment sur les quatre critères d'analyse de la norme NPLAB (caractéristiques du client, activité, localisation, missions effectuées par le Client), intégrant l'évaluation des risques, la détermination du niveau de vigilance et la documentation des diligences.

Pour les Clients ayant souscrit au Service PLM, Kanta garantit que la Solution intègre les fonctionnalités permettant d'assister le Client dans le respect de la Réglementation Déontologique au moyen notamment : (**i**) d'un dispositif de traçabilité de l'acceptation et du maintien de mission, incluant la génération de campagnes de maintien de mission sur la base des dates de clôture renseignées par le Client ; (**ii**) d'un processus de vérification de la procédure de confraternité en cas de reprise de dossier ; (**iii**) de la fourniture de modèles de lettres de mission élaborés au regard des normes de l'Ordre des experts-comptables en vigueur à la date de leur mise à disposition et (**iv**) de questionnaires d'acceptation des missions et de vérification du Bénéficiaires Effectifs permettant au Client d'identifier les risques pesant sur son indépendance et à s'assurer qu'il ne se trouve pas dans une situation de conflit d'intérêt.

8.3. Limitation de la garantie. Les Services LAB et PLM ne constituent, dans la mesure applicable, que des outils destinés à assister le Client dans le respect de ses différentes obligations de conformité dont il demeure seul responsable et ne sauraient en aucun cas se substituer à l'analyse, au jugement Client et à la responsabilité propre du Client. En particulier s'agissant de la conformité LAB, le Client n'est pas exonéré de respecter ses obligations légales et réglementaires, et notamment : (**i**) de mettre en place les procédures et mesures de contrôle interne requises par la Réglementation LCB-FT ; (**ii**) de déterminer et d'appliquer le Niveau de Risques approprié à l'égard de ses Clients et Bénéficiaires effectifs ; (**iii**) d'effectuer, le cas échéant, les déclarations de soupçon auprès de TRACFIN et (**iv**) de documenter les diligences réalisées tout au long de la Relation d'Affaires. Kanta ne fournit aucune prestation de conseil juridique, déontologique ou réglementaire. Les fonctionnalités de conformité déontologique ne constituent pas et ne doivent pas être interprétées comme un avis Client. La fiabilité des résultats produits par la Solution dépend directement de l'exactitude, de l'exhaustivité, des paramètres renseignés et de la mise à jour des données saisies ou importées par le Client ou ses Utilisateurs. Kanta ne saurait être tenue responsable de tout résultat erroné, incomplet ou inadapté résultant de données inexactes, incomplètes ou obsolètes. Kanta ne garantit pas non plus la conformité de la Solution à des réglementations sectorielles spécifiques, à des positions individuelles des instances ordinales ou à des interprétations doctrinales qui ne sont

pas publiquement accessibles. En cas de modification du cadre normatif applicable, Kanta ne saurait être tenue responsable pendant le délai raisonnablement nécessaire à l'adaptation de la Solution, ni des conséquences d'une utilisation de la Solution pendant cette période transitoire. Le Client demeure seul et intégralement responsable de la décision d'accepter, de maintenir ou de mettre fin à une mission, du respect effectif de la procédure de confraternité, de l'adéquation de ses lettres de mission à sa situation particulière, de l'appréciation de son indépendance et de l'absence de conflit d'intérêts, ainsi que, plus généralement, de l'ensemble de ses obligations déontologiques et de mise en conformité LAB.

ARTICLE 9. DONNÉES

9.1. Propriété des Données du Client. Le Client conserve l'intégrité de ses droits de propriété sur ses Données, en ce compris les Données de ses Clients. Kanta n'acquiert aucun droit de propriété sur les Données du Client du fait du Contrat.

9.2. Traitement des Données du Client. Kanta traite les Données du Client aux seules fins de la fourniture des Services et conformément aux instructions documentées du Client. Le Client assume l'entière responsabilité : (**i**) de la nature, du contenu, de l'exactitude, de l'intégrité et de la licéité des Données du Client transmises, saisies ou importées sur la Plateforme ; (**ii**) de l'information préalable de ses Clients et, le cas échéant, de l'obtention de toute autorisation ou base légale nécessaire à l'importation et au traitement de leurs données sur la Plateforme ; (**iii**) du paramétrage de son Compte, de l'exactitude des informations fournies à ce titre et du respect des délais de transmission des informations nécessaires à la fourniture des Services.

Kanta peut être amenée à traiter des Données Personnelles relatives aux Clients Finaux et à leurs Bénéficiaires Effectifs. Pour ces traitements, le Client agit en qualité de responsable de traitement au sens du RGPD et Kanta en qualité de sous-traitant. Les obligations respectives des Parties sont définies à l'Annexe 3 « Accord de Traitement des Données Personnelles ». Kanta traitera également les données des Utilisateurs aux fins de la gestion de leurs Comptes Utilisateurs, de la fourniture et de l'amélioration des Services. Pour ces traitements, Kanta agit en qualité de responsable de traitement. Ces traitements sont soumis à la politique de protection des Données Personnelles de Kanta, accessible depuis la page d'accueil de la Plateforme.

9.3. Sécurité des Données du Client. Kanta prendra toutes précautions utiles et adéquates pour préserver la sécurité et l'intégrité des Données du Client. Kanta met à ce titre en œuvre les mesures techniques et organisationnelles décrites à l'Annexe 4 « Plan d'Assurance Sécurité ».

9.4. Hébergement des Données du Client. Kanta héberge les Données du Client sur la Plateforme pendant toute la durée de l'Abonnement. Pendant cette durée, le Client peut à tout moment accéder à ses Données, les consulter et les exporter au moyen des fonctionnalités mises à disposition sur la Plateforme. Cette conservation ne constitue pas un archivage légal au sens des dispositions applicables. Il appartient au Client de mettre en œuvre, par ses propres moyens et sous sa seule responsabilité, les mesures de sauvegarde et d'archivage nécessaires au respect de ses obligations légales, notamment l'obligation de conservation de cinq (5) ans.

kanta

ARTICLE 10. PROPRIÉTÉ INTELLECTUELLE

10.1. Propriété de Kanta. La Solution et l'ensemble des éléments qui les composent (Plateforme, logiciels, bases de données, textes, graphismes, images, marques, logos, etc.) est et demeure la propriété exclusive de Kanta. Le Contrat ne confère au Client aucun droit de propriété intellectuelle sur la Solution.

10.2. Propriété du Client. Les Données, documents, informations et tout autre élément du Client soumis à un droit de propriété intellectuelle communiqués par le Client ou ses Utilisateurs à Kanta dans le cadre de l'utilisation des Services, sont et demeure la propriété exclusive du Client, Kanta n'acquérant aucun droit à leur égard, à l'exception d'un droit d'utilisation strictement limité aux besoins de l'exécution de ses obligations contractuelles.

10.3. Garanties d'éviction – Indemnisation. Chaque Partie (la « **Partie Garante** ») s'engage à garantir, défendre et indemniser l'autre Partie (la « **Partie Protégée** ») contre toute réclamation, action ou demande émanant d'un tiers relevant du périmètre défini au présent article (ci-après une « **Réclamation** »).

La Partie Garante prend en charge, à ses frais exclusifs, la défense contre toute Réclamation et le paiement de toute somme mise à la charge de la Partie Protégée par une décision de justice définitive, ainsi que les honoraires d'avocats et frais de procédure raisonnables, sous réserve que : (**i**) la Partie Protégée notifie la Partie Garante dans les meilleurs délais de toute menace ou notification relative à une Réclamation ; (**ii**) la Partie Garante dispose du contrôle exclusif de la défense et de la faculté de choisir ses conseils, étant précisé qu'elle ne pourra, sans le consentement écrit préalable de la Partie Protégée, conclure de transaction impliquant une reconnaissance de responsabilité de la Partie Protégée ou imposant à celle-ci des obligations non pécuniaires et ; (**iii**) la Partie Protégée coopère pleinement avec la Partie Garante dans le cadre de la défense. Les stipulations du présent article constituent le recours exclusif de la Partie Protégée au titre des Réclamations qui y sont visées. En outre, si l'utilisation de la Solution ou des Services fait l'objet, ou est susceptible de faire l'objet selon l'appréciation raisonnable de Kanta, d'une Réclamation de propriété intellectuelle, Kanta pourra, à sa discrétion et à ses frais : (**i**) obtenir pour le Client le droit de continuer à utiliser la Solution et les Services ; (**ii**) remplacer ou modifier tout ou partie de la Solution ou des Services de sorte qu'ils cessent de porter atteinte aux droits du tiers, sans dégradation substantielle des fonctionnalités ; (**iii**) si les options (i) et (ii) ne sont pas raisonnablement réalisables, résilier le Contrat et rembourser le cas échéant au Client *prorata temporis* les sommes payées d'avance pour l'accès et l'utilisation aux Services dont il sera privé.
La garantie de Kanta ne s'applique pas lorsque la Réclamation de propriété intellectuelle résulte, en tout ou partie : (i) de la conformité à des spécifications, données ou instructions fournies par le Client ; (ii) d'une modification de la Solution ou des Services par toute personne autre que Kanta et (iii) de l'utilisation de la Solution ou des Services en violation du Contrat.

ARTICLE 11. CONFIDENTIALITÉ

11.1. Obligations. La partie destinataire des Informations Confidentielles (**i**) traitera les Informations Confidentielles avec le même degré de protection que ses propres informations confidentielles, et en tout état de cause avec un niveau de protection raisonnable ; (**ii**) utilisera les Informations Confidentielles aux seules fins de l'exécution du Contrat ; (**iii**) ne reproduira, copiera ou dupliquera les Informations Confidentielles, en tout ou partie, par quelque moyen et sous quelque forme que ce

soit, en dehors de ce qui est strictement nécessaire à l'exécution du Contrat ; (**iv**) ne divulguera les Informations Confidentielles qu'aux seuls membres de son personnel et, le cas échéant, à ses sous-traitants autorisés au titre du Contrat, ayant un besoin légitime d'en connaître pour l'exécution du Contrat, et qui sont eux-mêmes soumis à des obligations de confidentialité au moins aussi protectrices que celles du présent article ; (**v**) prendra toutes les mesures nécessaires pour prévenir toute divulgation non autorisée. Kanta reconnaît expressément que les Données du Client sont, par nature, directement liées à l'activité réglementée du Client et revêtent un caractère hautement confidentiel.

11.2. Divulgation autorisée. Nonobstant les stipulations qui précèdent, une Partie pourra divulguer des Informations Confidentielles : (**i**) lorsque cette divulgation est exigée par une disposition légale ou réglementaire, par une décision de justice ou par une injonction d'une autorité administrative ou judiciaire compétente, sous réserve que la Partie Destinataire en informe la Partie Divulgatrice dans les meilleurs délais et, dans la mesure du possible, préalablement à la divulgation ; limite la divulgation au strict nécessaire ; et s'efforce d'obtenir un traitement confidentiel des informations divulguées ; (**ii**) à ses conseils juridiques, commissaires aux comptes ou auditeurs, soumis à des obligations légales de secret Client ; (**iii**) dans le cadre d'un différend entre les Parties, devant les juridictions compétentes ou les arbitres, dans la stricte mesure nécessaire à l'exercice de ses droits.

11.3. Durée. Les obligations de confidentialité prévues au présent article s'appliquent pendant toute la durée du Contrat et survivront pendant une durée de cinq (5) ans après son expiration ou sa résiliation, quelle qu'en soit la cause.

ARTICLE 12. RESPONSABILITÉ

12.1. Force majeure. Aucune Partie ne sera tenue responsable de l'inexécution de ses obligations si cette inexécution résulte d'un cas de force majeure au sens de l'article 1218 du Code civil. La Partie affectée en informera l'autre Partie dans les meilleurs délais. Si la force majeure persiste au-delà de quatre-vingt-dix (90) jours, chaque Partie pourra résilier le Contrat de plein droit, sans indemnité.

12.2. Responsabilité. Kanta exécute ses obligations selon une obligation de moyens dès lors que les Services sont fournis avec le concours du Client. Sa responsabilité ne pourra donc être engagée qu'en cas de faute prouvée par le Client. Elle sera responsable des conséquences résultant de ses fautes, erreurs ou omissions ainsi que de celles de son personnel et de ses sous-traitants, causant un dommage direct à l'autre Partie, à l'exclusion de tout dommage indirect.

Dans l'hypothèse où la responsabilité de Kanta serait engagée par suite de l'inexécution ou de la mauvaise exécution du Contrat, sauf en cas de manquement à ses obligations du respect de la confidentialité ou de la propriété intellectuelle, le montant de l'indemnisation globale et cumulée, toutes causes confondues, principal, intérêts et frais, à laquelle le Client pourrait prétendre, sera limitée aux sommes effectivement versées par le Client à Kanta au cours des douze (12) derniers mois précédant la survenance du dommage. Les limitations de responsabilité continueront de s'appliquer même en cas de résolution ou de résiliation de l'Abonnement par le Client ou Kanta, pour quelque cause que ce soit.

ARTICLE 13. ASSURANCE

Kanta déclare maintenir en vigueur, pendant toute la durée du Contrat, une police d'assurance de responsabilité civile professionnelle souscrite auprès d'une compagnie d'assurance notoirement solvable et couvrant les risques liés à l'exécution du Contrat.

ARTICLE 14. DURÉE ET FIN DU CONTRAT

14.1. Durée du Contrat. Le Contrat entre en vigueur à la date de signature du Bon de commande pour la durée définie dans celui-ci (la « **Période Initiale** »). À défaut de précision dans le Bon de commande, la Période Initiale du Contrat est de douze (12) mois. À défaut de stipulation contraire dans le Bon de Commande, le Contrat sera tacitement reconduit par périodes successives de douze (12) mois. Le Client souhaitant ne pas renouveler le Contrat devra en notifier à Kanta par lettre recommandée avec accusé de réception ou par e-mail avec accusé de réception, au moins trois (3) mois avant l'échéance en cours. À compter du premier renouvellement, les conditions tarifaires pourront faire l'objet d'une discussion entre les Parties.

14.2. Résiliation du Contrat. Chaque Partie peut résilier le Contrat de plein droit en cas de manquement grave de l'autre Partie à l'une de ses obligations, non remédié dans un délai de trente (30) jours suivant la réception d'une mise en demeure adressée par lettre recommandée avec accusé de réception détaillant le manquement concerné. Chaque Partie peut résilier le Contrat si l'autre Partie fait l'objet d'une procédure de sauvegarde, de redressement ou de liquidation judiciaire, dans la mesure permise par les Lois Applicables.

14.3. Effets de la résiliation. À la date de prise d'effet de la résiliation ou de l'expiration du Contrat, quelle qu'en soit la cause tous les droits et licences concédés au Client au titre du Contrat prennent fin et l'ensemble des Comptes Utilisateurs sont clôturés entrainant par la même occasion l'arrêt des Services.

Le Client pourra procéder à l'export de ses Données au moyen des fonctionnalités d'export disponibles sur la Plateforme. Au terme du Contrat, Kanta procédera à la suppression définitive des Données du Client dans un délai maximum de trente (30) jours, sauf obligation légale ou défense de ses droits imposant une conservation plus longue.

En cas de résiliation pour manquement du Client, aucun remboursement des mensualités du Prix de l'Abonnement déjà versées ne sera effectué. En outre, le Client sera redevable envers Kanta, outre les factures non payées à la date de résiliation, d'une indemnité correspondant à la totalité des mensualités restant à facturer au titre des Services jusqu'à la date d'échéance de la Période Initiale ou le cas échéant, de la Période de renouvellement en cours.

Pour toute autre cause de résiliation, notamment la résiliation pour manquement de Kanta ou pour force majeure, Kanta remboursera le cas échéant, au Client les sommes versées au titre du Prix de l'Abonnement, au prorata de la période restant à courir à compter de la date de prise d'effet de la résiliation.

Les articles suivants survivront à la résiliation du Contrat : article 6 « Conditions financières », article 8 « Garanties », article 9 « Données », article 10 « Propriété intellectuelle », article 11 « Confidentialité », article 12 « Responsabilité », et article 15 « Dispositions diverses ».

ARTICLE 15. DISPOSITIONS DIVERSES

15.1. Sous-traitance. Kanta pourra être amenée à faire appel à des tiers dans le cadre de l'exécution des Services disposant de garanties identiques à celles de Kanta et dont Kanta restera responsable vis-à-vis du Client.

15.2. Cession. Chaque Partie peut, sans le consentement de l'autre Partie, céder le Contrat à toute société affiliée ou dans le cadre d'une fusion, d'un changement de contrôle ou d'une vente de la totalité ou de la quasi-totalité de ses actifs, sous réserve : (i) d'en informer l'autre Partie préalablement ; et (ii) que le cessionnaire accepte de remplir les obligations du Contrat et de prendre les mêmes garanties que Kanta.

15.3. Référence commerciale. Kanta peut utiliser le nom, le logo et les marques commerciales du Client uniquement pour l'identifier en tant qu'utilisateur des Services sur son Site internet et dans ses supports marketing, sous réserve du respect des directives d'utilisation des marques communiquées par le Client**.**

15.4. Indépendance des parties. Kanta et le Client agissent en tant que contractants indépendants. Aucune disposition du Contrat ne saurait être interprétée comme constituant un partenariat, une coentreprise, une relation d'agence ou une relation d'emploi entre les Parties.

15.5. Divisibilité. Si une disposition du Contrat est jugée nulle ou inapplicable, elle sera réputée n'avoir jamais existé, sans affecter la validité des autres dispositions. Les Parties s'engagent à remplacer la disposition nulle par une disposition reflétant aussi fidèlement que possible l'intention initiale.

15.6. Notifications. Toute notification au titre du Contrat devra être adressée par écrit : (a) par courrier recommandé avec accusé de réception à l'adresse de l'autre Partie indiquée dans le Bon de commande ; ou (b) par courrier électronique à l'adresse indiquée dans le Bon de commande. Les notifications sont réputées remises dès leur envoi par courrier électronique, ou à la date indiquée sur l'accusé de réception.

15.7. Modifications des CGS. Kanta se réserve le droit de modifier à tout moment les présentes CGS afin de tenir compte des évolutions techniques, fonctionnelles, commerciales, réglementaires ou jurisprudentielles applicables à la Solution, aux Services ou à son activité. Toute modification est notifiée au Client par écrit, par tout moyen, au moins trente (30) jours avant son entrée en vigueur. Si la modification est substantielle pour le Client, ce dernier pourra, dans ce délai de trente (30) jours à compter de la notification, résilier le Contrat de plein droit par notification écrite à Kanta, sans indemnité ni pénalité, la résiliation prenant effet à la date d'entrée en vigueur de la modification. À défaut de résiliation notifiée dans ce délai, la modification est réputée définitivement acceptée par le Client et intégrée au Contrat. Les modifications rendues nécessaires par une évolution des Lois Applicables sont d'application immédiate et opposables au Client dès leur notification, sans ouvrir droit à résiliation.

15.8. Non-renonciation. Le fait qu'une Partie ne fasse pas valoir une violation par l'autre Partie d'une disposition du Contrat ne saurait être interprété comme une renonciation à cette disposition.

15.9. Intégrité de l'accord. Le Contrat constitue l'intégrité de l'accord entre les Parties et remplace tout accord antérieur, oral ou écrit, relatif à son objet.

ARTICLE 16. LOI APPLICABLE, JURIDICTION ET LITIGES

16.1. Les présentes sont soumises au droit français.

16.2. Les Parties conviennent de faire leurs meilleurs efforts pour résoudre à l'amiable toute contestation susceptible de résulter de l'interprétation, de l'exécution et/ou la validité du présent Contrat.

16.3. À défaut, tout différend portant sur la validité, l'exécution ou l'interprétation des présentes, sera soumis à la compétence exclusive des tribunaux du ressort de la Cour d'appel de Caen, auquel il est fait expressément attribution de compétence, même en cas de référé ou de pluralité de défendeurs.

kanta

ANNEXE 1 – SERVICES

Les Services décrits dans la présente Annexe sont fournis en fonction de l'Abonnement souscrit par le Client, tels que précisés dans le Bon de commande. Certains services communs aux deux modules sont optionnels et ne sont fournis que sous réserve de leur souscription expresse dans le Bon de commande.

Module 1 – LAB (Lutte Anti-Blanchiment)	
Services	**Description**
Évaluation de la conformité LAB – FT	Identification et vérification d'identité des Clients et Bénéficiaires Effectifs : récupération automatique des documents d'entreprise (registre des Bénéficiaires Effectifs, statuts juridiques, justificatif d'immatriculation) à partir du numéro SIRET. Évaluation et classification des Niveaux de risque de la Relation d'affaires lors de l'acceptation et en cours de mission, formalisée par un Rapport LAB-FT disponible et régulièrement mis à jour sur le Tableau de Bord et, selon l'Abonnement souscrit, les diligences conditionnelles à accomplir et les mesures de vigilance à mettre en place. Détermination du niveau de vigilance : attribution automatique du niveau de vigilance (standard ou renforcée) selon l'exposition aux risques.
Pilotage des risques de conformité LAB-FT	Mise à disposition d'un Tableau de Bord présentant la cartographie des Clients avec leur statut, leur Niveau de Risque, le collaborateur affecté et les actions à mettre en place en fonction du niveau de vigilance - selon l'Abonnement souscrit - que le Client pilote à l'aide des fonctionnalités lui permettant d'actualiser les fiches clients et Bénéficiaires, de moduler les Niveaux de Risque et de valider les Relations d'Affaire.
Veille réglementaire	Veille intégrée, automatique et permanente de la réglementation LCB-FT, des procédures internes et plus largement de toute réglementation en lien avec la Solution, la Plateforme et les Services.

Module 2 – PLM (Prospects et Lettres de Mission)	
Services	**Description**
Gestion de la prospection commerciale	Assistance au suivi du Prospect depuis le premier contact jusqu'à la signature de la lettre de mission intégrant : (**i**) un tableau de bord interactif de type Kanban permettant le suivi de chaque étape du cycle commercial (prise de contact, découverte, proposition commerciale, conversion en client) ; (**ii**) un dispositif de traçabilité de la prise de connaissance globale préalable à l'acceptation de chaque mission. Pour les missions récurrentes, la Solution génère automatiquement des campagnes de maintien de mission, fondées sur les dates de clôture comptable, afin de permettre au Client d'examiner périodiquement si des circonstances nouvelles sont de nature à remettre en cause le maintien de la relation d'affaires ; (**iii**) une analyse de risque intégrée dès la phase de prospection, comprenant la récupération automatique des documents essentiels, le cas échéant, la vérification de la procédure de confraternité, le déclenchement d'une première analyse LAB.
Edition automatisée et signature des lettres de mission	Édition automatisée de modèles de lettres de mission conformes aux normes de l'Ordre des experts-comptables, la possibilité de les personnaliser avec les conditions générales du Client et leur signature électronique. La signature électronique est assurée par un prestataire tiers spécialisé et dûment certifié, dont le service est intégré à la Plateforme à des fins de facilité d'usage. Kanta n'intervient ni dans la fourniture ni dans la sécurisation de ce service de signature ; les conditions d'utilisation de celui-ci relèvent exclusivement de la relation entre le Client et ledit prestataire.

Gestion automatisée du Portefeuille Client	Importation, récupération et mise à jour du Portefeuille Client et, le cas échéant, l'identification des données manquantes, l'audit du Portefeuille Client, la génération automatique des fiches clients et Bénéficiaires Effectifs et, l'alerte en cas de péremption d'un document Client.
Services communs	
Gestion des droits d'administration et d'accès des Utilisateurs	Mise à disposition d'un outil de gestion des droits d'administration des dossiers Clients, des droits d'affectation aux dossiers Clients et des droits d'accès à la Plateforme et aux Services.
Veille réglementaire	Veille intégrée, automatique et permanente des évolutions législatives et réglementaires applicables aux Services, en particulier la Réglementation LCB-FT et la Réglementation Déontologique. Les mises à jour de la Solution qui en résultent sont déployées dans le cadre de la maintenance évolutive définie à l'Annexe 2, dans un délai raisonnablement nécessaire à compter de l'entrée en vigueur des textes concernés.
Formation (Optionnel)	Formation des Utilisateurs à l'utilisation des Services, au moyen du dispositif de E-Learning développé par Kanta et mis à la disposition du Client et de ses Utilisateurs sur la Plateforme.
Support (Optionnel)	Assistance à distance en cas de problème sur la Plateforme, la Solution et les Services, depuis le Tableau de Bord ou en adressant un courriel à l'adresse : support@kanta.fr ou au moyen de la ligne téléphonique dédiée, selon les horaires, canaux et niveaux de priorité définis à l'Annexe 2.

ANNEXE 2 – NIVEAUX DE SERVICES (SLA)

ARTICLE 1. DISPONIBILITÉ

Kanta s'engage, au titre d'une obligation de moyen, à maintenir un taux de disponibilité mensuel des Services de 99,5 % (le « **Niveau de disponibilité** »).

Ce Niveau de disponibilité est calculé sur une période d'un mois calendaire par application de la formule suivante :

$$Taux\ de\ disponibilité\ = \frac{(t_{mois} - t_{interruption} + t_{exclusion})}{t_{mois}}$$

où :

- t_{mois} est le temps moyen mensuel en minutes d'accessibilité ;
- $t_{interruption}$ est le temps cumulé en minutes d'Interruption des Services pendant le mois considéré calculé par Kanta;
- $t_{exclusion}$ est le temps cumulé en minutes d'interruption des Services pendant le mois considéré calculé par Kanta qui est exclu des engagements de Niveau de disponibilité de Kanta au titre des stipulations contractuelles.

Calcul du paramètre $t_{interruption}$:

Le Niveau de disponibilité des Services est calculé par Kanta au moyen de tests automatisés effectués à intervalles réguliers par Kanta dont les résultats sont accessibles sur le site status.kanta.fr.

En cas d'incident, la durée d'indisponibilité sera mesurée à partir du moment où l'incident a été signalé par le Client ou détecté par Kanta jusqu'au moment où l'incident est résolu et que les Services sont de nouveau disponibles pour le Client.

Cas d'exclusion :

Le Niveau de disponibilité des Services peut être perturbé dans les cas ci-dessous qui ne seront en outre pas pris en compte pour le calcul du Niveau de disponibilité. Ces temps de coupure cumulés sont représentés par le paramètre $t_{exclusion}$ dans la formule de calcul :

- Force majeure conformément à l'article 1218 du Code civil ;
- En raison de défaillance avérée des environnements et infrastructures du système du Client ;
- Opérations de maintenance programmées, dûment notifiées au Client ;
- Maintenance d'urgence rendue nécessaire pour prévenir ou corriger un incident critique de sécurité ou de disponibilité ;
- Interventions, paramétrages ou intégrations réalisés par le Client ou par un tiers non autorisé par Kanta ;

- Utilisation non conforme des Services par le Client ou ses Utilisateurs ;
- Indisponibilités dues à des attaques informatiques externes (cyberattaques, déni de service, virus, etc.) lorsque Kanta a mis en œuvre les mesures de sécurité raisonnablement attendues.
- Indisponibilité résultant d'un défaut ou d'un retard de transmission par le Client d'une demande de mise à niveau pour la seule durée de retard imputable à ce défaut.

Pénalités :

Si, sur une période de douze (12) mois glissants, le Niveau de Disponibilité constaté est inférieur au seuil contractuel pendant au moins trois (3) mois, le Client bénéficie d'une remise sur le Prix de l'Abonnement, calculé selon le barème suivant :

Taux Disponibilité constaté				**Remise en pourcentage du Prix de l'Abonnement du Client**
<	99,50%	>	99,00%	5%
<	99,00%	>	98,50%	15%
<	98,50%	>	98,00%	20%

Lorsque, au cours d'une même période de douze (12) mois glissants, plusieurs mois présentent des Niveaux de Disponibilité relevant de niveaux de remise différents, seule la remise correspondant au niveau le moins élevé s'applique, à l'exclusion de tout cumul.

Les remises s'appliquent sur les facturations au titre des mois affectés par un niveau de disponibilité ressortant du barème ci-dessus.

L'application de remises devra être effectuée sous forme d'avoir émis par Kanta dans les 30 jours de la survenance d'un cas d'application des remises ci-dessus.

kanta

ARTICLE 2. SUPPORT ET ASSISTANCE

2.1. Maintenance

Maintenance programmée. Kanta effectue les opérations de maintenance programmée durant les créneaux de faible utilisation des Services, soit entre 20h et 6h (heure de Paris). Les opérations de maintenance courante, en ce compris les mises à jour mensuelles de l'infrastructure serveur et les mises en production de nouvelles versions de la Solution, n'entraînent en principe pas d'interruption perceptible des Services et ne font pas l'objet d'une notification préalable au Client. Seules les opérations de maintenance susceptibles d'entraîner une interruption des Services font l'objet d'une notification au Client, par courrier électronique ou par publication sur la Plateforme, au moins soixante-douze (72) heures à l'avance. Cette notification précise la nature de l'intervention, le créneau prévu et la durée estimée d'indisponibilité.

Maintenance d'urgence. En cas de nécessité liée à la prévention ou à la correction d'un incident critique de sécurité ou de disponibilité, Kanta peut procéder à une maintenance d'urgence sans respecter le délai de notification prévu ci-dessus. Kanta informe le Client dans les meilleurs délais de la nature de l'intervention et de son impact sur la disponibilité des Services, par tout moyen approprié et notamment via le site status.kanta.fr.

Incidence sur la disponibilité. Les périodes d'indisponibilité résultant d'une maintenance programmée dûment notifiée ou d'une maintenance d'urgence sont exclues du calcul du Niveau de Disponibilité conformément au paragraphe « Cas d'exclusion » ci-dessus. Kanta s'engage à faire de son mieux pour maintenir la disponibilité des Services pendant les périodes de maintenance et à en minimiser au maximum l'impact.

Maintenance évolutive. Kanta peut, à sa discrétion, apporter des améliorations à la Solution, indépendamment des opérations de maintenance programmée ou d'urgence visées ci-dessus. Ces évolutions, qui peuvent donner lieu à la mise à disposition de nouvelles versions de la Solution, sont déployées automatiquement sur la Plateforme sans intervention du Client.

2.2. Support

Kanta répond aux demandes de support du Client concernant l'utilisation et le fonctionnement des Services par téléphone, via le Service Desk ou encore par email à l'adresse support@kanta.fr. Le support est disponible entre 9h et 18h du lundi au jeudi et de 9h à 16h45 le vendredi (« **les Heures de Support** »).

2.3. Gestion des incidents

Kanta s'engage, au titre d'une obligation de moyens, à remédier aux incidents affectant le bon fonctionnement des Services conformément aux délais de réponse définis au paragraphe ci-après.

Pour les besoins du présent article, une « Anomalie » désigne tout écart, défaut ou non-conformité affectant la Solution, la Plateforme ou les Services par rapport au Contrat, à la Documentation ou aux spécifications fonctionnelles et techniques applicables. Constituent notamment, sans que cette liste soit limitative, des Anomalies : les incidents d'exploitation, les bogues, les pannes, les erreurs de

programmation, les indisponibilités non planifiées, les défauts de performance significatifs ainsi que toute dégradation notable des fonctionnalités attendues.

Kanta n'est pas tenue de fournir de support ni de maintenance corrective dans les cas suivants : (**i**) le dysfonctionnement résulte d'une utilisation des Services non conforme au Contrat ou aux instructions de Kanta ; (**ii**) le dysfonctionnement est imputable à un équipement, un logiciel, un réseau ou une infrastructure relevant de la responsabilité du Client ou de ses Utilisateurs ; (**iii**) le dysfonctionnement est imputable à un service tiers connecté à la Plateforme par le Client en application de l'article 5.3 des CGS ; (**iv**) l'incident n'est pas suffisamment documenté par le Client pour permettre à Kanta d'en vérifier la réalité et d'en effectuer le diagnostic ; (**v**) la demande est formulée en dehors des horaires de support définis au paragraphe 2.3 ; (**vi**) un cas de force majeure.

Une modification des fonctionnalités de la Solution et des Services telle que fournie par une mise à jour ou une mise à niveau ou une Nouvelle Version n'est pas considérée comme une Anomalie.

Les Anomalies ont quatre niveaux de priorité :

Priorité	Description
P1 (Urgent)	Anomalie rendant la Solution ou les Services totalement inaccessibles ou inutilisables
P2 (Élevée)	Perte grave d'une fonctionnalité essentielle ou restriction importante de l'utilisation des Services
P3 (Normal)	Anomalie ponctuelle ou localisée sans impact significatif sur l'utilisation des Services
P4 (Faible)	Gêne d'utilisation, défaut mineur n'ayant aucun impact fonctionnel sur l'utilisation des Services

En cas d'Anomalie, le Client doit informer immédiatement Kanta via l'adresse support@kanta.fr,. La déclaration de l'Anomalie doit inclure les informations suivantes : (**i**) la description détaillée de l'Anomalie et de ses effets sur l'utilisation des Services ; (**ii**) l'heure et la date de l'Anomalie ; (iii) les détails sur la localisation géographique et le navigateur utilisé pour accéder aux Services ; (iv) tout autre renseignement jugé pertinent par le Client.

Kanta s'engage, dans le cadre d'une obligation de moyen à respecter le niveau de service de support ci-après détaillé (« **Niveau de service de support** »). Ainsi Kanta devra, pendant les Heures de Support applicables faire ses meilleurs efforts pour, répondre, résoudre ou traiter les Anomalies sur la base des indicateurs suivants :

- **Garantie de temps d'intervention** (ou « **GTI** ») pour la prise en compte de la demande de résolution d'une Anomalie identifiée par le Client : il s'agit du délai entre le signalement de la demande par le Client et la prise en charge par Kanta pour analyse.

- **Garantie de temps de résolution** (ou « **GTR** ») pour la mise en place des correctifs proposés par Kanta : il s'agit du délai entre le signalement par le Client de l'Anomalie ou du problème et la mise en place par Kanta d'une solution définitive permettant le rétablissement d'une situation opérationnelle.

Niveau de Priorité	GTI	GTR
P1	4 heures	8 heures
P2	8 heures	24 heures
P3	12 heures	72 heures
P4	24 heures	72 heures

Kanta peut demander au Client l'accès temporaire à son Compte ou à ses données aux seules fins de la résolution de l'Anomalie. En cas de défaut de coopération du Client ou de refus d'accès, les délais de réponse et de résolution définis au paragraphe 2.3 sont suspendus jusqu'à l'obtention des éléments ou accès demandés.

2.4. Notification des incidents. Kanta s'engage à informer le Client de toute Anomalie affectant la disponibilité des Services dans un délai de vingt-quatre (24) heures, via le site status.kanta.fr. La notification inclut une description de l'Anomalie, de ses effets sur l'utilisation des Services et des actions en cours pour le résoudre. Kanta fournit des mises à jour régulières sur l'avancement de la résolution jusqu'au rétablissement des Services. En cas de Dysfonctionnement affectant la sécurité des Données Personnelles, Kanta notifie le Client dans les conditions prévues à l'Annexe 3.

2.5. Suivi de la disponibilité. Le site status.kanta.fr permet au Client de suivre en temps réel et de manière historisée la disponibilité des Services, les incidents en cours et les opérations de maintenance planifiées. Sur demande du Client, Kanta fournit des informations complémentaires relatives à un incident spécifique. En dehors de cette hypothèse, Kanta n'est pas tenue de fournir de rapports périodiques systématiques sur les incidents.

ANNEXE 3 – ACCORD DE TRAITEMENT DES DONNÉES PERSONNELLES

Le présent Accord de Traitement des Données Personnelles y compris ses annexes (ci-après le « **DPA** ») fait partie intégrante du Contrat et réglemente les traitements de données à caractère personnel effectués par Kanta, en qualité de sous-traitant, pour le compte du Client, en qualité de responsable de traitement, dans le cadre de l'utilisation des Services. Les termes définis dans le Contrat ont le même sens dans le présent DPA.

ARTICLE 1. OBJET ET STATUT DES PARTIES

Kanta agit en qualité de sous-traitant pour l'ensemble des Données Personnelles qu'elle traite pour le compte du Client dans le cadre de l'exécution du Contrat, y compris dans le cadre des prestations de support et de maintenance prévues à l'Annexe 2. Le Client agit en qualité de responsable de traitement à l'égard des Données Personnelles relatives à ses Clients et à leurs Bénéficiaires Effectifs. Le présent article définit les obligations respectives des Parties en matière de protection des Données Personnelles. La description des traitements, les catégories de Données Personnelles concernées et les catégories de personnes concernées sont précisées à l'annexe du présent DPA.

ARTICLE 2. OBLIGATION DU CLIENT

Le Client s'engage à respecter l'ensemble de ses obligations au titre du RGPD, notamment : (**a**) tenir un registre des activités de traitement ; (**b**) réaliser, le cas échéant, une analyse d'impact ; (**c**) informer les personnes concernées du traitement de leurs données ; (**d**) ne traiter les Données Personnelles que pour les finalités prévues au Contrat ; (**e**) fournir à Kanta les instructions documentées nécessaires à l'exécution des traitements.

ARTICLE 3. OBLIGATION DE KANTA

Kanta s'engage à (**a**) traiter les Données Personnelles uniquement sur instruction documentée du Client ; (**b**) garantir la confidentialité des Données Personnelles et s'assurer que les personnes autorisées à les traiter s'engagent à respecter cette confidentialité ; (**c**) mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer la sécurité des traitements ; (**d**) assister le Client dans le respect de ses obligations (réponse aux demandes d'exercice des droits, notification des violations, analyses d'impact) ; (**e**) notifier le Client dans les meilleurs délais (et au plus tard dans les 48 heures) en cas de violation de données personnelles ; (**f**) supprimer les Données Personnelles au terme du Contrat sauf si la loi en exige autrement ou en cas de litige ; (**g**) mettre à disposition du Client toute information nécessaire pour démontrer le respect des obligations prévues au présent DPA.

ARTICLE 4. SOUS-TRAITANCE

Kanta est autorisée à recourir à des sous-traitants pour l'exécution des Services. Kanta s'assure que ses sous-traitants présentent des exigences équivalentes à celles prévues dans le présent DPA et reconnait qu'il sera responsable envers le Client du respect des obligations du sous-traitant en vertu du DPA. La liste des sous-traitants est fournie en Annexe B du présent DPA.

Kanta informera le Client de tout changement de sous-traitant et lui laissera un délai raisonnable pour émettre toute objection raisonnablement formulée et raisonnablement fondée, en rapport à la protection des données et au respect de la législation sur la protection des données.

ARTICLE 5. TRANSFERTS INTERNATIONAUX

Les Données Personnelles sont traitées et hébergées en France. En cas de transfert hors UE/EEE, Kanta mettra en place les garanties appropriées (clauses contractuelles types, décisions d'adéquation) et en informera préalablement le Client.

ARTICLE 6. SÉCURITÉ

Kanta mettra en œuvre et maintiendra des mesures techniques et organisationnelles appropriées nécessaires pour répondre aux exigences de l'article 32 du RGPD afin de garantir la sécurité, la confidentialité et l'intégrité des Données Personnelles du Client contre la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé(e), de manière accidentelle ou illicite, à ces Données Personnelles du Client.

Kanta s'assurera que son personnel autorisé à traiter les Données Personnelles du Client est soumis à des obligations de confidentialité appropriées.

Kanta met à la disposition du Client les informations raisonnablement nécessaires pour démontrer le respect de ses obligations au titre du présent DPA et de la réglementation applicable en matière de protection des données. Le Client peut, à ses frais, faire réaliser un audit des conditions de traitement des Données Personnelles par un auditeur tiers indépendant, soumis à des obligations de confidentialité appropriées et qui ne soit pas un concurrent de Kanta. Le Client adresse à Kanta un préavis écrit d'au moins trente (30) jours ouvrés avant la date envisagée de l'audit et veille à ce que celui-ci ne perturbe pas le fonctionnement normal des activités de Kanta. Les audits sont limités à un (1) par année civile, sauf en cas de violation avérée de Données Personnelles ou de demande émanant d'une autorité de contrôle.

ARTICLE 7. RESPONSABILITÉ

Le Client est responsable des dommages résultant de ses manquements en qualité de responsable de traitement. Kanta est responsable des dommages résultant de ses manquements propres à ses obligations de sous-traitant ou aux instructions du Client.

Sous réserve des limitations et exclusions de responsabilité prévues dans le Contrat, chaque Partie indemnisera et maintiendra l'autre Partie indemne contre toute responsabilité, amendes, réclamations, demandes, dépenses et coûts (y compris les frais juridiques raisonnables) encourus par l'autre Partie résultant de ou en relation avec : (a) toute violation par l'autre Partie de ses obligations en vertu de la *Législation sur la Protection des Données* ; et/ou (b) lorsque Kanta est la partie indemnisée, Kanta agissant conformément à toute instruction, politique ou procédure du Client.

Annexe A – Description des traitements

Nature des traitements : collecte, hébergement, enregistrement, structuration, conservation, consultation, extraction, utilisation, communication par transmission, rapprochement, limitation et effacement de données à caractère personnel.

Finalités : exécution des Modules LAB et/ou PLM souscrits par le Client ;

Catégories de personnes concernées : Clients Finaux, Bénéficiaires Effectifs.

Types de données : données d'identification (nom, prénom, date de naissance, adresse, numéro de pièce d'identité), données professionnelles (SIRET, activité, chiffre d'affaires).

Durée du traitement : durée du Contrat, sauf obligation légale de conservation plus longue ou litige.

kanta

Annexe B – Liste des sous-traitants

Prestataire	Localisation	Garanties	Rôle
Scaleway	France (UE)	N/A (UE/EEE)	Hébergement infrastructure et bases de données
Google	France (UE)	N/A (UE/EEE)	Hébergement infrastructure et bases de données

ANNEXE 4 – PLAN D'ASSURANCE SÉCURITÉ

Dernière mise à jour : 12/02/2026

La PSSI, ou Politique de Sécurité des Systèmes d'Information, se définit comme un document de référence reflétant la vision stratégique et les objectifs d'une organisation en matière de sécurité des systèmes d'information (SSI) et définissant les règles de sécurité à adopter. La PSSI constitue donc une démarche à la fois stratégique, validée par la direction et opérationnelle, qui impacte tous les acteurs des systèmes d'information en service.

Sommaire

kanta

Approbation de la direction

Cette Politique de Sécurité des Systèmes d'Information (PSSI) est approuvée par la direction de Kanta.

Elle s'applique à l'ensemble des collaborateurs, prestataires et partenaires impliqués dans la gestion, le traitement et la protection des données clients.

Vision & Périmètre

Vision

Chez Kanta, la sécurité fait partie du fonctionnement normal de nos produits et de nos processus. Nous protégeons les données de nos clients à chaque étape, en appliquant des pratiques techniques et organisationnelles reconnues.

Périmètre d'application

Ce document couvre :

- L'ensemble des services, applications, API et infrastructures exploitées par Kanta pour ses clients
- Les environnements de développement, test et production
- Les utilisateurs internes, prestataires, partenaires accédant aux systèmes ou données
- Les données hébergées, traitées ou stockées pour le compte de nos clients.

Partenariats de Confiance

Kanta travaille avec des partenaires et fournisseurs qui respectent les mêmes exigences de sécurité que nous. Cette cohérence crée une chaîne de confiance solide, du client jusqu'à nos prestataires techniques.

Responsabilité Sociale et Éthique

Kanta traite la protection des données comme une responsabilité éthique, pas seulement réglementaire. Le respect de la vie privée guide nos décisions techniques et nos relations avec les clients.

Adaptabilité et Résilience

L'approche de Kanta vise la résilience et l'adaptabilité : anticiper les nouveaux risques, ajuster nos dispositifs et maintenir la disponibilité de nos services quelles que soient les circonstances.

kanta

Gouvernance & Responsabilités

La sécurité de l'information chez Kanta repose sur une gouvernance claire, partagée entre la direction technique et les fonctions de conformité.

Cette organisation associe la rigueur d'un cadre groupe, le Visma Security Program (VSP), et la proximité opérationnelle d'une équipe tech impliquée au quotidien.
La sécurité est intégrée dans les activités courantes de Kanta : chaque membre de l'équipe technique est acteur de la protection des données, de la prévention des incidents et de la conformité.

Le comité technique sécurité, composé des dix membres du pôle technique, se réunit chaque semaine pour suivre les sujets liés à la sécurité applicative, à la protection des données et à la conformité RGPD.

Tableau des rôles et responsabilités

Rôle	Responsabilités principales	Appui / collaboration
CTO (Responsable Sécurité)	Supervise la stratégie et la mise en œuvre de la sécurité des systèmes d'information. Définit les priorités, valide les choix techniques et garantit la conformité aux exigences internes et groupe.	Visma Security Program (VSP)
Tech Lead	Met en œuvre les pratiques de sécurité dans le développement et l'exploitation. Suit la correction des vulnérabilités et pilote les améliorations continues.	CTO / Comité technique
Comité technique sécurité (10 pers.)	Participe activement à la veille, à la mise à jour des politiques et à la validation des actions de sécurité. Revue hebdomadaire des incidents, vulnérabilités et évolutions.	CTO / Tech Lead
DPO	Audite le respect du RGPD, supervise les analyses d'impact et le traitement des demandes liées aux données personnelles.	Legal Counsel / Leto
Legal Counsel	Gère la conformité juridique et	DPO / Leto

Rôle	Responsabilités principales	Appui / collaboration
	contractuelle en matière de sécurité et de protection des données. Coordonne les audits contractuels avec le partenaire Leto.	
Groupe Visma – Visma Security Program (VSP)	Fournit le cadre, les outils et les audits sécurité du groupe. Le VSP encadre les sociétés du groupe selon des standards élevés (sécurité cloud, tests continus, formation, réponse incident).	Programme groupe Visma
Prestataire externe	Réalise un test d'intrusion annuel indépendant (approche grey box) pour vérifier la résistance de l'application Kanta, y compris depuis un compte client simulé.	CTO / Tech Lead

Cadre groupe – Visma Security Program (VSP)

Kanta applique les exigences du **Visma Security Program**, programme de sécurité de référence du groupe Visma.

Le VSP fournit un ensemble de services de sécurité avancés (analyse de code, scanning de vulnérabilités, formation, bug bounty interne) et s'appuie sur une culture de transparence et de responsabilisation : *"Security works for you."*

Les standards du programme sont alignés sur les meilleures pratiques du secteur (OWASP, ISO 27001, NIST) et mesurés par un **Security Maturity Index** commun à toutes les entités Visma. Vous pouvez consulter les détails du programme et des certifications sur le Trust Center de Visma.

En complément du VSP, Kanta bénéficie de l'appui opérationnel des **services de sécurité du groupe Visma**. Ces équipes spécialisées interviennent notamment en cas d'incident de sécurité majeur pour fournir un **soutien à la gestion de crise**, à la **remédiation technique** et à la **communication coordonnée**.

Elles travaillent en lien direct avec les responsables de Kanta afin d'assurer une réponse rapide, documentée et conforme aux procédures groupe.

kanta

Contrôle d'accès & Authentification

La sécurité des accès constitue un pilier central de la politique de sécurité de Kanta.
Elle repose sur des mécanismes d'authentification robustes, adaptés au profil des utilisateurs (clients, partenaires, collaborateurs internes) et sur une gestion stricte des droits d'accès selon le principe du moindre privilège.
Cloisonnement des données. Kanta assure un cloisonnement logique strict des Données de chaque Client au sein de la Plateforme, de sorte qu'aucun Client ne puisse accéder aux données d'un autre Client. Ce cloisonnement est mis en œuvre par des mécanismes applicatifs de séparation des structures de données au sein de l'infrastructure commune, complétés par des contrôles d'accès garantissant l'étanchéité entre les environnements de chaque Client.

Authentification et accès des clients (plateforme Kanta)

Domaine	Description	Responsable	Évolution prévue
Authentification principale	Système d'authentification basé sur JWT, utilisé par la majorité des clients de la plateforme Kanta.	CTO / Tech Lead	Maintenu, avec renforcement sécurité.
Authentification forte (2FA)	Le second facteur d'authentification (2FA) intégré au système JWT, afin de renforcer la sécurité des comptes clients. Code par e-mail pour les collaborateurs et code via application dédiée pour les valideurs	CTO / Comité technique	Revue annuelle
Keycloak (SSO / fédération d'identité)	Service d'authentification basé sur Keycloak, utilisé pour les grands comptes disposant de fédération d'identité. Permet l'intégration SSO via les annuaires clients.	CTO / Tech Lead	Déploiement sur demande client
Politique de mot de passe	Règles de complexité appliquées côté SaaS : minimum 12 caractères, majuscules, minuscules, chiffres et symboles. Vérification automatique de robustesse.	Tech Lead	Revue annuelle

Domaine	Description	Responsable	Évolution prévue
Gestion des droits et habilitations	Attribution des droits selon le principe du moindre privilège, suppression des accès inactifs et traçabilité complète des actions sensibles.	CTO / Comité technique	Continu

Authentification et accès des collaborateurs (environnement interne)

Domaine	Description	Responsable	Évolution prévue
Identité et authentification centralisées	Les comptes collaborateurs sont gérés dans **Google Workspace** (groupe Visma). **Keycloak** s'appuie sur cette identité Google pour authentifier l'accès aux outils internes, dont le **Backoffice Kanta**. Le **MFA** est obligatoire pour tous les comptes.	CTO / RH / Visma	Continu
Automatisation des habilitations (Primo)	La gestion des habilitations est automatisée par **Primo**, l'outil interne de provisioning utilisé pour la création, la gestion et la suppression des comptes utilisateurs et ordinateurs. Les rôles et profils définis permettent d'attribuer ou de révoquer automatiquement les droits lors de l'onboarding ou de l'offboarding.	CTO / Tech Lead	Continu

Gestion des secrets et mots de passe internes

Historiquement, l'usage des coffres-forts de mot de passe est répandu chez Kanta mais pas structuré.

Pour cela, la gestion des mots de passe et secrets internes est maintenant assurée via **1Password**, solution fournie et diffusée par le groupe **Visma**.
Son déploiement obligatoire pour tous les collaborateurs Kanta est prévu au **Q2 2026**.
L'outil est accompagné d'un programme d'adoption documenté et soutenu par Visma, incluant :

- des **licences personnelles et familiales** offertes pour encourager les bonnes pratiques de sécurité
- des **fonctionnalités avancées** pour les développeurs (stockage d'API keys, intégration CI/CD)
- un support interne dédié pour la configuration et la gestion des coffres.

Infrastructure, Hébergement & Sauvegardes

Hébergement principal

L'infrastructure de production de Kanta est hébergée chez **Scaleway**, dans le datacenter **Paris 1**, garantissant un hébergement **100 % en France** et conforme aux exigences européennes en matière de protection des données.

L'architecture applicative repose sur des instances cloud dédiées et sécurisées, intégrées au sein de l'écosystème du groupe Visma.

Les bases de données de production sont déployées en **haute disponibilité**, avec un **nœud de secours actif** maintenant la continuité de service en cas de défaillance d'un serveur. Cette configuration permet de minimiser les interruptions et d'assurer une résilience accrue.

Sauvegardes des données

Les sauvegardes de données applicatives sont effectuées de manière **horaire entre 6h et 22h en semaine**, permettant la restauration rapide en cas d'incident.

Chaque sauvegarde complète est conservée pendant **7 jours**, assurant un court historique, mais réactif, adapté aux besoins d'un service SaaS en évolution continue.

En complément, des **snapshots journaliers** complets des bases de données sont réalisés chaque soir à **21h30** et conservés durant **14 jours**. Ces snapshots capturent l'état complet du système à un instant donné, facilitant une restauration intégrale si nécessaire.

Sauvegardes des documents

Les documents clients sont stockés dans des **buckets S3 hébergés chez OVHcloud**, également situés en **France**.

Ces données font l'objet d'une **sauvegarde différentielle quotidienne**, effectuée chaque nuit sans limites de rétention.

Ce mécanisme garantit la **non-altération des données**, grâce à l'utilisation des contrôles d'intégrité natifs de S3 et à la vérification automatique des métadonnées.

Tests et vérification

Kanta effectue un **test de restauration complet une fois par an**, afin de valider la fiabilité de ses procédures de sauvegarde.

L'entreprise prévoit d'**augmenter cette fréquence** dans les années à venir, dans une logique d'amélioration continue de la résilience opérationnelle.

Les processus de sauvegarde et de restauration sont documentés et suivis au sein du comité technique.

Continuité & Gestion des Incidents

Kanta adopte une approche proactive de la continuité et de la gestion des incidents.
L'objectif est de garantir la disponibilité de ses services, la protection des données et une reprise rapide en cas de perturbation, tout en assurant une communication claire avec les parties prenantes.
La stratégie de gestion des incidents repose sur trois piliers : **détection rapide**, **coordination efficace**, et **amélioration continue**.

Détection et surveillance

Élément	Description	Responsable / Outil	Statut
Supervision des terminaux	Les postes de travail des collaborateurs Kanta sont protégés par **SentinelOne** managé par Visma assurant une surveillance en temps réel des menaces et comportements suspects. Il est relié au SOC interne de Visma	CTO / Tech Lead / Visma Security Team	En production
Alertes de sécurité	Les alertes remontent automatiquement aux responsables de la sécurité par e-mail ou via le canal choisi. Intégré au **SOC du groupe Visma** avec des équipes groupe dédiées 24/7.	CTO / Comité technique	En cours d'évolution

Surveillance des infrastructures	Les environnements cloud (Scaleway, OVHcloud) font l'objet d'une supervision continue via les outils internes et les mécanismes de reporting du groupe Visma.	CTO / Visma Security Program	Continu

Gestion des incidents de sécurité

Étape	Description	Responsable
Détection et signalement	Tout collaborateur Kanta a le devoir d'alerter immédiatement le service sécurité du groupe Visma en cas d'incident suspect.	Tous les collaborateurs
Analyse et qualification	Le CTO et les responsables sécurité évaluent la gravité et définissent le plan d'action.	CTO / Comité technique
Coordination de la réponse	En cas d'incident majeur, le CTO coordonne la réponse avec les équipes spécialisées de Visma (VSP, VC3).	CTO / Visma Security Services
Communication	Communication interne pilotée par le CTO. La communication externe est coordonnée avec le service sécurité du groupe.	CTO / Visma Security Team
Retour d'expérience (REX)	Tous les incidents sont documentés. Les incidents majeurs font l'objet d'une **task force** et d'un **retour d'expérience** pour prévenir toute récurrence.	CTO / Comité technique

Soutien du groupe Visma

Visma Security Program (VSP)

Kanta bénéficie du cadre, des outils et des audits du **Visma Security Program**, garantissant une approche structurée et mesurable de la sécurité.

Le VSP fournit des services spécialisés (analyse de code, scanning, bug bounty interne, formation, réponse à incident) et contribue à la surveillance globale des actifs critiques.

Visma Cyber Crime Centre (VC3)

Le **VC3** est l'unité du groupe dédiée à la **prévention et à la réponse aux cyberattaques**.

Ses missions incluent :

- la **détection et l'analyse** des menaces ;
- la **gestion de crise** et la coordination des réponses aux incidents majeurs ;
- le **soutien technique** aux entités Visma lors d'investigations post-incident ;
- la **veille de sécurité et le renseignement sur les menaces** pour l'ensemble du groupe.

Kanta peut mobiliser ces services via le CTO en cas d'incident critique, garantissant ainsi une réponse coordonnée, rapide et conforme aux standards du groupe.

Résilience et continuité d'activité

Les systèmes critiques de Kanta sont conçus pour maintenir leur disponibilité grâce à une **infrastructure en haute disponibilité** et des **sauvegardes multi-niveaux** (voir section précédente).
Des **tests de restauration annuels** sont effectués pour valider l'efficacité du dispositif, et leur fréquence sera progressivement augmentée.

Protection des Données & RGPD

La protection des données personnelles constitue un engagement central de Kanta, tant pour ses clients que pour ses collaborateurs.

Conformément au **Règlement Général sur la Protection des Données (RGPD)**, Kanta met en œuvre des mesures organisationnelles et techniques adaptées afin d'assurer la confidentialité, l'intégrité et la disponibilité des informations traitées.

Cette démarche s'inscrit dans un cadre d'amélioration continue, en lien étroit avec la **direction compliance du groupe Visma**, qui challenge et accompagne Kanta dans le renforcement permanent de sa conformité.

Organisation et responsabilités

Rôle	Description	Collaboration
Délégué à la Protection des Données (DPO)	DPO interne à Kanta, responsable de la supervision de la conformité RGPD, du registre des traitements et de la gestion des demandes des personnes concernées.	Collaboration avec le Legal Counsel et le service Compliance Visma
Legal Counsel	Supervise la conformité contractuelle et les aspects juridiques du traitement des données. Pilote la relation avec le partenaire **Leto**.	DPO / Leto
Leto	Fournit la solution SaaS de gestion de conformité et d'audit des contrats. Facilite la gestion quotidienne du RGPD via un **portail clients** et des outils de suivi automatisé.	Legal Counsel / DPO
Service Compliance Visma	Encadre et challenge Kanta dans la mise en œuvre de standards groupe, évalue la maturité et définit des plans d'amélioration.	Direction Kanta / DPO

Outils et processus de conformité

Domaine	Description	Statut
Portail RGPD (Leto)	Portail en ligne permettant aux clients et utilisateurs d'exercer leurs droits (accès, rectification, suppression). Les demandes sont traitées directement dans l'interface Leto par Kanta.	En production
Registre des traitements	Tenu à jour par le DPO et le Legal Counsel, documentant les traitements, finalités, durées et mesures associées.	En place

Analyses d'impact (PIA)	Non obligatoires à ce jour mais prévues dans la feuille de route 2026 pour les traitements sensibles.	À venir
Clauses contractuelles de sous-traitance	Modèle en cours d'élaboration avec le groupe Visma afin d'assurer un cadre commun et conforme pour tous les prestataires (Scaleway, OVHcloud, etc.).	En cours
Sensibilisation RGPD	Le personnel est régulièrement informé des obligations liées à la protection des données et des bonnes pratiques à respecter.	Continu

Suivi et amélioration continue

Le **service compliance du groupe Visma** assure un suivi régulier du niveau de conformité des entités du groupe, dont Kanta.
Cette supervision se traduit par :

- des **revues périodiques** de conformité et de documentation,
- des **plans d'action correctifs** à mettre en œuvre,
- et la **mutualisation des bonnes pratiques** entre sociétés du groupe.

Kanta s'engage à maintenir une conformité dynamique, fondée sur la transparence, la réactivité et la responsabilisation des équipes internes.

Sensibilisation & Culture Sécurité

Chez Kanta, la sécurité n'est pas qu'une affaire d'outils ou de procédures : c'est un réflexe collectif.
Chaque collaborateur joue un rôle actif dans la protection des données, et la sensibilisation continue vise à maintenir une vigilance constante face aux menaces numériques.
L'objectif est de faire de la sécurité un **comportement naturel**, ancré dans le quotidien de l'entreprise.

Sensibilisation interne

Domaine	Description	Fréquence / Modalité
Onboarding	Chaque nouvel arrivant reçoit une présentation des bonnes pratiques de sécurité, des obligations de confidentialité et de l'usage des outils internes.	À chaque arrivée
Réunions hebdomadaires	Les points sécurité et les rappels sur les risques (phishing, MFA, gestion des accès) sont abordés lors des réunions collectives de synchronisation.	Hebdomadaire
Ateliers techniques	Le département technique organise deux ateliers par an centrés sur la sécurité applicative, le durcissement des environnements et la gestion des incidents.	Semestriel
Configuration des outils	Les outils collaboratifs et SaaS utilisés par Kanta sont configurés selon les principes de moindre privilège et de sécurité par défaut, réduisant ainsi les risques liés au facteur humain.	Continu

Formation et accompagnement groupe Visma

En tant que membre du groupe Visma, Kanta bénéficie d'un écosystème de sensibilisation étendu et structuré autour du Visma Security Program (VSP).

Ce programme vise à créer une culture de sécurité partagée dans l'ensemble des entités du groupe, en combinant formation, communication et accompagnement opérationnel.
Les collaborateurs de Kanta ont accès à plusieurs dispositifs proposés par Visma :

- Formations et modules obligatoires : chaque employé suit régulièrement des parcours de formation à la sécurité, à la confidentialité et à la conformité, adaptés à son rôle.

- Canaux Slack dédiés : plusieurs canaux internes favorisent la veille et le partage d'informations sur la cybersécurité, les incidents connus et les bonnes pratiques.

- Webinaires et événements sécurité : le VSP organise des sessions régulières sur des thèmes comme la gestion des vulnérabilités, la prévention du phishing, la conformité RGPD et la sécurité applicative.

Ces dispositifs complètent les initiatives internes de Kanta (réunions hebdomadaires, ateliers techniques, rappels sécurité) et garantissent un alignement constant avec les standards de sécurité et de conformité du groupe Visma.

L'objectif est que chaque collaborateur puisse prendre des décisions éclairées et sécurisées au quotidien, quel que soit son rôle.

Pour plus d'informations, voir le Visma Trust Center.

Amélioration continue

La sensibilisation fait partie intégrante du plan d'amélioration continue de Kanta.
Les retours d'incidents, les évolutions réglementaires et les audits internes alimentent régulièrement les actions de formation et de communication interne.

L'objectif est d'élever progressivement le niveau de maturité sécurité de l'ensemble des collaborateurs, tout en favorisant l'autonomie et la responsabilité individuelle.

Gestion de la Sous-traitance et des Échanges

Sous-traitance technique (opérationnel)

Prestataire	**Rôle**	**Portée / Détail**	**Pilotage**
Scaleway	Hébergement principal	Infra applicative et bases de données en France, HA pour la prod	CTO / Tech Lead
OVHcloud	Sauvegardes documents	Buckets S3 France, sauvegardes différentielles quotidiennes	CTO
Google Workspace (via Visma)	Identité & collaboration	Comptes collaborateurs, MFA obligatoire, base d'identité pour Keycloak	CTO / RH / Visma

Attineos	Test d'intrusion annuel	Grey box sur l'appli Kanta, scénario "compte client"	CTO / Tech Lead
Leto	Conformité RGPD	Portail droits RGPD, audit contrats, workflows de traitement	Legal / DPO
Visma (VSP, services sécurité)	Cadre & soutien sécurité	Outils, audits, gestion de crise, compliance groupe	Direction Kanta / CTO

Échanges de données (clients, partenaires, API)

Domaine	Mesure	Détail (technique modéré)	Statut
Chiffrement en transit	TLS	Accès externes via HTTPS (TLS ≥ 1.2, cible 1.3)	En production
Chiffrement au repos	Stockage	Volumes/buckets chiffrés côté fournisseur; intégrité vérifiée (S3)	En production
Authentification clients (appli)	JWT / Keycloak	JWT historique côté SaaS; SSO Keycloak pour grands comptes	En production
API publique (clients)	Clé API	Clé générée par un admin client, **affichée une seule fois**; stockage côté client	En production
Sécurité API	Journalisation & contrôle	Logs d'appels, **rate-limiter dédié**, alertes d'usage anormal	En production

Habilitations	Moindre privilège	Scopes/permissions applicatives, révocation à l'offboarding	En production
Traçabilité	Logs & rétention	Traçabilité des actions sensibles, corrélation avec supervision	En production

Gouvernance et contrôle

- Les sous-traitants critiques sont **revus annuellement** (tech + conformité).
- Les échanges de données externes sont **journalisés** et **monitorés**; les incidents suivent la procédure décrite dans **"Continuité & Gestion des Incidents"**.
- Tout nouveau prestataire manipulant des données clients passe par une **évaluation sécurité/conformité** (Legal + DPO + CTO).

Protection des Locaux

Les locaux de Kanta hébergent une partie limitée de l'infrastructure technique.
Même si la majorité des ressources est externalisée (hébergement cloud chez Scaleway et OVHcloud), Kanta maintient un haut niveau de sécurité physique pour les postes, les équipements et les supports contenant des données sensibles.

Contrôle des accès physiques

Domaine	Mesure	Description
Accès aux bureaux	Serrure connectée à empreinte digitale	L'accès aux locaux est strictement réservé aux collaborateurs autorisés. L'ouverture par empreinte digitale est consignée dans un **journal d'accès conservé en continu**.

Visiteurs	Accompagnement obligatoire	Toute personne externe est enregistrée et accompagnée par un membre de Kanta pendant sa présence.
Postes de travail	Sécurisation et chiffrement	Tous les postes sont chiffrés, verrouillés automatiquement et protégés par **SentinelOne**, administrés via **Visma**.
Équipements partagés	Usage contrôlé	Les périphériques partagés (imprimantes, écrans, docks) ne stockent aucune donnée.
Stockage physique	Interdiction des supports amovibles	Aucun stockage de données client sur support externe (clé USB, disque portable). Les transferts physiques sont bloqués par politique système.

Protection environnementale

- Les bureaux sont situés dans des locaux sécurisés disposant de **détection incendie**, **contrôle d'intrusion** gérés par **Kanta**.
- L'ensemble des infrastructures critiques (serveurs, bases de données, sauvegardes) est hébergé dans des **datacenters certifiés ISO/IEC 27001** et **ISO/IEC 50001** (Scaleway Paris 1 et OVHcloud France).
- Tout incident physique (intrusion, sinistre, panne) suit la **procédure d'escalade** décrite dans *Continuité & Gestion des Incidents*.

Mobilité et télétravail

- Le télétravail est autorisé uniquement depuis des **postes d'entreprise gérés via Primo**.
- L'accès distant repose exclusivement sur des **services SaaS sécurisés**, aucun VPN n'est utilisé.
- Les connexions sont protégées par **MFA (Google Workspace)** et des règles d'accès conformes aux standards du groupe Visma.

Revue et amélioration

La sécurité physique et environnementale fait l'objet d'une **revue annuelle** conduite par le CTO et le service compliance Visma, incluant :

- la vérification des accès physiques,
- le contrôle du **journal des empreintes digitales**,
- la mise à jour des procédures d'accès et d'effacement à distance.

Gestion des Développements Informatiques

Les développements logiciels de Kanta sont intégralement réalisés en interne par les équipes techniques.
Chaque **squad** est responsable de ses projets, de la qualité de son code et du respect des bonnes pratiques de sécurité applicative.

Cette organisation garantit à la fois agilité et traçabilité sur l'ensemble du cycle de vie logiciel.

Processus de développement

Tous les développements sont gérés via **GitLab**, où chaque fonctionnalité fait l'objet d'une *Merge Request* (MR) soumise à **revue croisée** par un ou plusieurs pairs.

Cette étape permet de prévenir les erreurs, d'améliorer la lisibilité du code et de partager les connaissances entre développeurs.

Les règles de fusion et de revue sont strictes : aucune modification n'est intégrée sans validation d'un autre membre de l'équipe.

Le pipeline de **CI/CD GitLab** automatise les principales étapes de vérification.
Chaque build exécute une série de tests unitaires et fonctionnels, des analyses de code et des contrôles de sécurité intégrés.

Le processus inclut des outils de qualité de code (PHPStan, Pint, CodeSniffer, Insights) ainsi qu'une **analyse de dépendances.**

Ce pipeline garantit que chaque livraison est reproductible, traçable et conforme aux standards internes.

Sécurité applicative

Kanta applique une politique de sécurité continue sur l'ensemble de la chaîne de développement :

- Les environnements de test et de préproduction sont isolés, sans données réelles de clients.

- Les variables sensibles sont gérées par **GitLab CI** avec des secrets protégés et, à terme, seront centralisées dans **1Password** (déploiement prévu début 2026).
- Les images Docker sont construites à partir de bases maîtrisées, puis promues manuellement après validation.
- Les erreurs et exceptions applicatives sont supervisées via **Sentry**, garantissant une traçabilité complète des anomalies.

Vérifications externes et conformité

Un **test d'intrusion annuel** est réalisé par **Attineos** sur l'application Kanta, en mode *grey box*, afin d'évaluer la résistance de la plateforme depuis le point de vue d'un utilisateur légitime.

À noter qu'il est possible que le prestataire change dans le futur.

Les résultats de test permettent de mettre en œuvre un plan de mitigation des risques et alimentent les actions correctives et les améliorations techniques prioritaires effectués par l'équipe technique.

Les pratiques de développement et de livraison sont également **alignées avec le Visma Security Program (VSP)**, garantissant une cohérence avec les exigences de sécurité du groupe.

Amélioration continue

La sécurité logicielle n'est pas figée : elle évolue avec le produit.

Kanta prévoit de renforcer la détection automatisée des vulnérabilités, d'introduire des analyses dynamiques (DAST) sur ses environnements de préproduction et de resserrer les critères de mise en production autour de seuils qualité et sécurité mesurables.

Chaque incident, correction ou évolution est documenté et partagé lors des revues techniques hebdomadaires afin d'améliorer collectivement la maturité de l'équipe.

Feuille de Route Sécurité 2026

La sécurité n'est jamais un état figé. Chez Kanta, elle évolue au même rythme que nos produits, nos outils et nos partenariats.

Chaque changement technique ou organisationnel implique d'ajuster nos pratiques et d'enrichir notre dispositif de protection.

Ce plan d'amélioration vise à maintenir un haut niveau de cohérence et de maîtrise, sans alourdir nos processus.

Il traduit une volonté simple : continuer à faire de la sécurité un réflexe partagé, fondé sur des mesures concrètes, proportionnées et alignées avec les standards du groupe Visma.

Ces actions sont suivies en interne, documentées et revues dans le cadre de nos comités techniques et de nos échanges réguliers avec les équipes sécurité du groupe.

Axes de travail prioritaires

Formation et sensibilisation (Q3 2026)

Renforcer la culture sécurité au sein de l'entreprise : mise en place d'un programme de formation régulier, ateliers internes et intégration des ressources proposées par Visma.
L'objectif est d'assurer un niveau homogène de compétences et de vigilance pour l'ensemble des collaborateurs.

Conformité RGPD (Amélioration continue)

Poursuivre l'amélioration du cadre légal : réalisation d'une analyse d'impact (PIA) et intégration de clauses contractuelles types avec les sous-traitants.
Ces actions garantissent la conformité continue et la traçabilité des engagements pris vis-à-vis des clients.

Refonte du plan de continuité d'activité (Q2 2026)

Revoir le dispositif de continuité pour l'adapter à la croissance de Kanta et à l'évolution de nos services SaaS.

L'objectif est de clarifier les scénarios de crise, d'améliorer la coordination entre les équipes et de renforcer la résilience globale, notamment sur la disponibilité des environnements critiques et la priorisation des services essentiels.