



Conditions générales de vente "Planik"

Version 1.6, fr, 01.09.2023



Planik est une application qui facilite la création des horaires du personnel (ci-après «Planik»). Planik est un produit de la société Planik SA (ci-après „Planik”) et est proposé sous forme de Software-as-a-Service. Les conditions générales de vente («CGV») ci-dessous définissent l'utilisation de Planik par le client.

La forme masculine a été choisie pour des raisons de lisibilité ; néanmoins, les données se réfèrent à des membres de tous les sexes.



1	Objet du contrat.....	3
2	Droit de mise à disposition pour les utilisateurs.....	4
3	Obligations du client.....	4
4	Responsabilité du client concernant son contenu.....	4
5	Prestation de services par les tiers.....	5
6	Rémunération.....	5
7	Entreprise.....	6
8	Garantie et responsabilité.....	7
9	Confidentialité et protection des données.....	8
10	Résiliation.....	8
11	Modification du contrat.....	8
12	Dispositions finales.....	9

Annexe 1 : Accord sur le traitement des données de commande selon l'art. 9 LPD

1	Objet et durée du marché.....	10
2	Lieu de traitement des données.....	10
3	Type de données.....	11
4	Catégories de personnes concernées.....	11
5	Obligations du contractant.....	11
6	Mesures techniques et organisationnelles.....	13
7	Relations de sous-traitance.....	13
8	Droits de contrôle du mandant.....	13
9	Copies, effacement et restitution de données personnelles.....	14

Addendum I: Mesures techniques et organisationnelles

1	Confidentialité.....	16
2	Intégrité.....	17
3	Disponibilité et résistance au stress.....	17
4	Procédures de contrôle, d'évaluation et de suivi réguliers.....	17
5	Contrôle de la mission : le contractant met notamment en œuvre les mesures suivantes :.....	18



1 Objet du contrat

1.1 Contenu du contrat

Planik fournit Planik au client moyennant des frais d'utilisation. La maintenance et le Hosting de Planik, le support en fonction du module choisi par le client, sont également compris dans la redevance d'utilisation.

1.2 Éléments du contrat

Un contrat entre Planik et le client consiste en général d'un contrat d'utilisation, les présentes CGV ainsi que la politique de confidentialité de Planik. Ces CGV font partie intégrante du contrat d'utilisation. En cas de contradiction entre les différents documents contractuels, les dispositions s'appliquent dans l'ordre indiqué ci-dessus. Toutes les CGV existantes du client sont exclues.

1.3 Conclusion du contrat

Le contrat entre Planik et le client est conclu par la signature du contrat d'utilisation. Le début des obligations de service ou du droit d'utilisation est déterminé par le contrat d'utilisation.

2 Droit de mise à disposition pour les utilisateurs

Planik cède au client le droit personnel, non transférable et non exclusif d'utiliser Planik en ligne pendant la durée du contrat, dans la mesure prévu par le contrat.

Le client n'a pas le droit d'accorder d'autres et/ou de sous-licences. Il n'est pas autorisé à mettre Planik à la disposition de tiers, à éditer, modifier ou reproduire indépendamment, développer, décrypter ou exploiter Planik d'une manière qui s'écarte de la description d'utilisation de Planik, sans le consentement de Planik. Le client n'a pas droit à une copie de travail de Planik et donc pas de droit à une copie de sauvegarde.

Les droits des données et du contenu saisi par le client lui restent acquis. Tous les droits de propriété intellectuelle sur Planik, les modules associés, les modèles, les extensions, les add-ons, les plugins, la documentation, etc. et les droits sur les développements spécifiques aux clients restent la propriété de Planik.

3 Obligations du client

3.1 Paiement dans les délais

Le client s'engage à payer le montant convenu dans les délais.

3.2 Utilisation et informations de connexion

Le client s'engage à utiliser Planik et les données d'accès exclusivement dans le cadre du contrat et uniquement pour la durée d contrat d'utilisation. Il s'engage, ainsi que ces employés, à traiter les données d'accès de manière confidentielle et prudente.

3.3 Obligation de révision et de procédure d'approbation

Le client a l'obligation d'inspecter tout travail effectué ou livré pour le client dans les 7 jours suivant la notification de la livraison par Planik. Le client est tenu de notifier à Planik par écrit (y compris par courrier) tout défaut dès sa découverte, mais au plus tard dans les 7 jours. Sans la signalisation de ces défauts à Planik dans les 7 jours, le travail effectué ou les



marchandises livrées seront considérés comme ayant été approuvés par Planik et acceptés par le client.

3.4 Personne de contact

Le client doit désigner une personne de contact capable de prendre des décisions et un suppléant envers Planik.

3.5 Accès à Internet et choix du navigateur

Le client est responsable de son propre accès à Internet pour l'utilisation de Planik. En outre, le client est responsable de l'utilisation d'un navigateur pour lequel la version actuelle de Planik a été testée. La liste des navigateurs testés peut être consultée à l'adresse www.planik.ch. Planik garantit au client que Planik prend en charge toutes les versions de navigateur qui ont une part de marché supérieure à 10% et qui n'ont pas plus de deux ans.

4 Responsabilité du client concernant son contenu

Le client est et reste le propriétaire des données enregistrées dans Planik. Il est seul responsable de la qualité, de la mise à jour et de l'exactitude des contenus. Il est également responsable du respect des dispositions légales en matière de sécurité industrielle, de protection des données et des exigences réglementaires à l'égard de ses employés et des tiers.

Le client est entièrement responsable de l'exportation régulière des données des plans et de l'archivage du contenu.

5 Prestation de services par les tiers

Planik a le droit d'engager des tiers pour fournir des services contractuels.

6 Rémunération

6.1 Frais et leur adaptation

Les frais d'utilisation mensuels de Planik, comprenant les prestations définies d'assistance, de maintenance et de hosting, sont payables annuellement pendant 12 mois à l'avance.

Les prix à payer par le client sont basés sur le montant indiqué dans le contrat d'utilisation signé ou sur la liste de prix respective pour les prestations correspondants. Planik peut ajuster les frais convenus dans le contrat d'utilisation à la prochaine date de résiliation possible conformément à l'article 10 des présentes CGV, sous réserve d'un préavis de 4 mois. Si le client n'est pas d'accord avec l'augmentation, il doit résilier le contrat conformément à l'article 10 des présentes CGV.

Au cas où Planik n'a pas été notifié de tous les principes techniques et organisationnels nécessaires à la préparation d'un devis ou si ceux-ci ont changé après la préparation du devis, Planik se réserve expressément le droit d'augmenter la rémunération spécifiée dans le contrat d'utilisation.

6.2 Prestations non comprises dans les frais

Tout service supplémentaire fourni par Planik qui n'est pas explicitement mentionné dans le contrat d'utilisation signé ou dans l'offre signée sera facturé séparément.



Les services qui sont fournis pour éliminer des dysfonctionnements, les pertes de données, etc., qui sont dues à une utilisation inadaptée ou à une mauvaise manipulation par le client ou qui sont survenus du côté du client en raison d'une intervention non autorisée de tiers, d'un accident ou d'un cas de force majeure ne sont pas non plus couverts par les frais d'utilisation. Ces services correspondants seront facturés séparément au client.

6.3 Modalités de paiement

Le client doit payer les factures pour les services rendus à la date d'échéance indiquée sur la facture ou dans le délai de paiement spécifié. Si aucune date d'échéance ou délai de paiement n'est spécifié, un délai de paiement de 30 jours à compter de la date de la facture est applicable.

A l'expiration du délai de paiement, le client est automatiquement en défaut, c'est-à-dire sans lettre de rappel. Planik est autorisé de facturer des intérêts sur le montant restant dû au taux de 5% par an.

En cas d'indisponibilité de Planik pendant 24 heures, le client peut réclamer les frais d'utilisation pour la durée de l'indisponibilité. La compensation d'autres créances par le client est exclue.

En cas de retard de paiement, Planik se réserve le droit de suspendre immédiatement l'accès à Planik et de résilier le contrat sans préavis après trois rappels. Une éventuelle indisponibilité de Planik due à un retard de paiement ne libère pas le client de l'obligation de payer. Dans tous les cas, Planik se réserve le droit de facturer un supplément de 30chf par rappel.

7 Entreprise

7.1 Problèmes de calcul automatique des horaires du personnel avec Planik «Smart»

Le client reconnaît qu'en raison des propriétés mathématiques des problèmes de planification (NP-intégrité du problème), il ne peut être garanti que le calcul automatisé des horaires sera toujours de qualité constante. Si le client estime que la qualité d'un plan est insuffisante, il peut assigner manuellement les services à distribuer aux employés.

7.2 Travaux de maintenance

Planik optimise le fonctionnement, les performances et la qualité de Planik grâce à des travaux de maintenance sur Planik ou sur les serveurs exécutant Planik.

Le client accepte des restrictions d'utilisation qui découlent des travaux de maintenance. Planik préfère effectuer les travaux de maintenance en dehors des heures de pointe (entre 18h00 et 8h00). Le client sera informé à l'avance de toute interruption prolongée due à des travaux de maintenance.

7.3 Support

Les services d'assistance de Planik comprennent le traitement des demandes des clients et les rapports d'erreur envoyé par écrit ou par téléphone, ainsi que l'analyse des problèmes relatifs et le dépannage d'erreurs simples par Planik.

Planik s'engage à contacter le client dans un délai de 2 jours ouvrables suivant la réception de la demande.



Planik se garde le droit de demander le client de saisir le problème lui-même en ligne dans un système de notification d'erreurs avant tout traitement part de Planik.

7.4 Disponibilité

Aucune garantie ne peut être donnée que Planik et l'assistance seront disponibles à tout moment ou que des dysfonctionnements et des interruptions ne se produiront pas. Cependant, Planik réagira aussi rapidement que possible à toute défaillance de Planik. Les autres dysfonctionnements sont prise en charge dans le cadre du support.

7.5 Nouvelles versions, options et modules

Planik peut mettre fournir une mise à jour ou développement complet de Planik ou de modules individuels en tant que nouvelle version de la solution. Le client s'engage à utiliser la nouvelle version ou la mise à jour.

Planik peut proposer des options et des modules sous forme d'extensions payantes. Le client n'est pas obligé de les acheter. Planik se réserve le droit d'intégrer une option ou un module en tant que mise à jour ou nouvelle version de la solution sans frais supplémentaires.

Planik se réserve le droit de modifier des procédures et le comportement de Planik dans le cadre du processus d'innovation. Planik ne garantit donc pas, que toutes les fonctions restent inchangées. Si les fonctions essentielles sont modifiées de telle manière que la fonctionnalité de Planik n'est plus garantie pour un client, celui-ci a le droit de résilier le contrat avec effet immédiat.

7.6 Sauvegarde des données

Planik ne peut pas facilement rétablir une base de clients sécurisée. Toutefois, Planik offre la possibilité de mettre à niveau les services des plans souhaités à un niveau de secours moyennant des frais.

8 Garantie et responsabilité

8.1 Garantie

Planik garantit au client pour la durée du contrat d'utilisation que Planik dispose les spécifications convenues lorsqu'il est utilisé correctement conformément au présent contrat d'utilisation et qu'il ne s'en écarte pas au point d'annuler ou de considérablement réduire leur utilité, et qu'aucun droit d'auteur de tiers concernant le logiciel n'est violé lorsque Planik est utilisé par le client conformément au contrat. Toute autre garantie est exclue.

En particulier, les obligations de garantie de Planik ne s'appliqueront pas dans la mesure où un écart par rapport à l'utilisation autorisée du client telle que décrite dans le contrat d'utilisation s'est produit ou est dû à des circonstances dont Planik n'est pas autrement responsable.

En cas de défaut dont Planik est responsable en vertu de la garantie, le client n'a droit, dans un premier temps, qu'à la réparation gratuite du défaut par Planik.

Le client doit fournir une assistance raisonnable à Planik pour analyser les causes et les conditions de la défaillance pour la résoudre.



Si Planik n'est pas en mesure de corriger avec succès le défaut invoqué dans la garantie, le client n'aura droit, selon le libre choix de Planik, qu'à une des options suivantes :

- a) une solution de contournement ; ou
- b) le remplacement par un autre logiciel ayant une portée fonctionnelle équivalente ; ou
- c) le retrait du contrat d'utilisation et le remboursement des frais d'utilisation déjà payés moins la période d'utilisation déjà effectuée.

Toute autre demande d'indemnisation de dommage est exclue.

En cas de survenance d'un défaut dont Planik n'est pas responsable, le client remboursera à Planik le temps passé à remédier à ce défaut au taux horaire inscrit dans la liste de prix actuelle de Planik, plus les frais et la TVA.

8.2 Responsabilité de Planik

Les données saisies par le client dans Planik sont transmises sous forme cryptée via une connexion de haute sécurité. Malgré l'utilisation des normes de sécurité élevées pour protéger les données par Planik, la transmission de données sur Internet n'est pas totalement sûre. Planik ne peut donc pas garantir la sécurité des données contre les attaques pirates, les virus, les chevaux de Troie et autres influences de tiers.

8.3 Responsabilité du client et indemnisation

Le client est seul responsable des plans de déploiement du personnel qu'il a établi, des données personnelles traitées et du respect des dispositions légales et réglementaires applicables. Le client s'engage à indemniser pleinement Planik contre toute réclamation faite par ses contractants, employés, autorités ou tiers à cet égard, ainsi que les dommages et les frais (y compris les frais de justice et d'avocat), et à assumer la responsabilité de toute action en justice de ce type.

9 Confidentialité et protection des données

9.1 Confidentialité

Les parties ainsi que leurs employés et auxiliaires s'engagent à préserver la confidentialité de toute information non généralement connue, qui se rapporte à la sphère d'activité de l'autre partie et qui leur est accessible au cours de la préparation et de l'exécution du présent contrat. Cette obligation reste en vigueur après la fin de la relation contractuelle. Planik peut citer le client comme référence sur consentement.

9.2 Protection des données

Dans le cadre de la fourniture de services informatiques, Planik traite les données du client exclusivement pour l'exécution du contrat. Dans la mesure où Planik traite des données personnelles pour le client en tant que sous-traitant au sens de la législation applicable en matière de protection des données, elle le fait exclusivement de la manière définie dans l'accord sur le traitement des données de commande ("**accord TDC**") conformément à l'annexe 1 des présentes CGV et exclusivement pour les besoins du client.



10 Résiliation

Le contrat est conclu pour une durée indéterminée. La durée minimale du contrat est de 12 mois. Par la suite, chaque partie peut résilier le contrat par lettre recommandée à la fin d'une année civile, moyennant un préavis de 3 mois.

Planik peut résilier le contrat d'utilisation à tout moment pour un motif valable avec effet immédiat. Cela s'applique dans le cas où Planik est utilisé en violation du contrat d'utilisation ou si les présentes conditions générales continuent d'être ignorées malgré un rappel écrit. Dans ce cas, l'obligation de paiement du client reste en vigueur jusqu'à la prochaine date de résiliation ordinaire possible.

Après la résiliation du contrat, le client est lui-même responsable de la sauvegarde de ses données saisies à Planik. À l'expiration de ce délai, les données relatives à Planik seront supprimées par Planik sans autre préavis.

11 Modification du contrat

11.1 Modification des CGV

Planik peut modifier les présentes CGV à tout moment et à sa seule discrétion. Le client sera informé par Planik avant tout ajustement. Si le client n'est pas en accord avec les ajustements, il doit résilier le contrat d'utilisation avec Planik dans les 30 jours suivant la prochaine date de résiliation, conformément à l'article 10 des présentes CGV.

À moins que le client ne résilie le contrat dans les 30 jours suivant cette notification, les CGV modifiées seront considérées comme acceptées et obligatoires dans le délai communiqué par Planik.

11.2 Modifications du contrat d'utilisation

Les modifications ou les ajouts au contrat d'utilisation nécessitent la signature des deux parties pour être juridiquement valables. Cela s'applique également à cette exigence de forme écrite.

12 Dispositions finales

12.1 Transfert de droits à des tiers

Les droits et obligations découlant de la relation contractuelle ne peuvent être cédés ou autrement transférés à des tiers sans le consentement écrit de Planik.

12.2 Nullité partielle

Si certaines dispositions ou parties du contrat s'avèrent invalides, la validité de l'ensemble du contrat n'est pas affectée. Dans ce cas, les parties contractantes doivent adapter le contrat de manière à ce que le but visé par la partie nulle ou inefficace soit atteint dans la mesure du possible.

12.3 Droit applicable et lieu de juridiction

La présente relation contractuelle est soumise au droit matériel suisse, à l'exclusion des conflits de lois et de la Convention des Nations Unies sur les contrats de vente internationale de marchandises. Le lieu de juridiction pour tout litige est Berne, en Suisse. Toutefois,



Planik peut choisir de faire valoir ses droits à sa propre discrétion au domicile ou au siège social du client.



Annexe 1 : Accord sur le traitement des données de commande selon l'art. 9 LPD (accord TDC)

La société Planik AG ("prestataire") propose au client ("donneur d'ordre") la mise à disposition, la maintenance et l'exploitation d'un logiciel basé sur le web pour la planification du personnel et la saisie du temps de travail ainsi que des services d'accompagnement pour son utilisation. Dans ce contexte, le Prestataire traite des données à caractère personnel dont le Client est responsable. Le contractant est donc le sous-traitant du client.

Le présent accord concrétise les obligations des parties contractantes en matière de protection des données.

- 1 Objet et durée du marché
- 12.4 L'objet de la présente convention (ci-après "commande") découle du contrat d'utilisation auquel il est fait référence ici (ci-après "contrat principal"). Sont également considérés comme contrat principal tous les éléments de ce dernier ainsi que les éventuels avenants au contrat et les offres complémentaires.
- 12.5 Les services à fournir découlent du contrat principal.
- 12.6 La durée du présent mandat correspond à la durée du contrat principal, pour autant qu'aucune obligation dépassant ce cadre ne résulte des dispositions suivantes.
- 12.7 L'Addendum I - Mesures techniques et organisationnelles - fait partie intégrante de ce mandat.
- 13 Lieu de traitement des données
- 13.1 Le traitement de données faisant l'objet du contrat est effectué en Suisse, dans l'UE ou dans un État de l'AELE et dans un État tiers pour lequel il existe une décision d'adéquation du Conseil fédéral ou de la Commission européenne.
- 13.2 Une délocalisation du traitement des données dans un pays tiers pour lequel il n'existe pas de décision d'adéquation du Conseil fédéral n'est possible qu'avec l'accord écrit préalable du mandant. Est assimilée à une délocalisation dans un tel pays tiers la délocalisation dans une solution de cloud computing si son exploitant et/ou l'entreprise qui le contrôle sont soumis au CLOUD Act des États-Unis.
- 13.3 Le contractant s'assure que, dans le cadre de l'externalisation vers un pays tiers ou d'une solution de cloud computing selon le point précédent, il garantit une protection des données appropriée au moyen de garanties suffisantes et qu'il respecte les conditions particulières prévues aux articles 16 et suivants de la LPD. LPD. A cet effet, le contractant conclut par exemple le module nécessaire des clauses contractuelles types de l'UE ("SCC") du 4 juin 2021.
- 13.4 En tout état de cause, avant de procéder à un transfert vers un pays n'ayant pas fait l'objet d'une décision d'adéquation, le contractant doit procéder à une évaluation des risques sous la forme d'une évaluation de l'impact du transfert ("TIA") et déterminer ainsi le risque pour les droits des personnes concernées d'un accès des autorités sans garantie de recours dans le pays concerné. Un transfert ne peut avoir lieu que si le risque correspondant a été jugé



faible au sens de la clause 14 des CSC. L'AIT doit être mise spontanément à la disposition du client avant la transmission.

14 Type de données

Les types/catégories de données suivants font notamment l'objet du traitement des données à caractère personnel :

- données de base sur les personnes (par exemple, nom, adresse, date de naissance, état civil, titre professionnel, appartenance à une entreprise, CV, etc ;))
- Données d'identification électronique (telles que l'adresse IP, la signature électronique, les données de connexion/de protocole, les cookies) ;
- données de communication (par ex. téléphone, e-mail, code PIN, mot de passe, ports, login) ;
- Données de base du contrat (relation contractuelle, intérêt du produit ou du contrat) ;
- Données de décompte du contrat (saisie du temps de travail et données salariales variables) ;

15 Catégories de personnes concernées

Les catégories de personnes concernées par le traitement résultent de l'énumération suivante. Chacune de ces catégories comprend des personnes concernées anciennes, actuelles et potentiellement futures :

- Employés ;
- Employés indépendants / Freelancer ;

16 Obligations du contractant

Le contractant garantit le respect des spécifications suivantes :

- 16.1 Les données à caractère personnel ne doivent pas être traitées à des fins autres que celles spécifiées par le client ;
- 16.2 Le preneur d'ordre s'engage à respecter une stricte confidentialité lors du traitement des données. Lors de l'exécution des travaux, le mandataire ne fait appel qu'à des personnes qui, avant le début du traitement des données, ont été tenues de respecter la confidentialité et ont été familiarisées avec les dispositions pertinentes de la protection des données. L'obligation de confidentialité/de secret professionnel se poursuit également après la fin du mandat ;
- 16.3 Le traitement s'effectue exclusivement conformément à la commande et aux instructions du donneur d'ordre, à moins que le preneur d'ordre ne soit légalement tenu de procéder à un traitement différent ou plus étendu ;
- 16.4 Le preneur d'ordre confirme les instructions orales immédiatement et au moins sous forme de texte ;
- 16.5 Le preneur d'ordre est tenu d'informer immédiatement le donneur d'ordre s'il estime qu'une instruction enfreint les dispositions relatives à la protection des données. Le preneur



d'ordre est en droit de suspendre l'exécution de la directive correspondante jusqu'à ce qu'elle soit confirmée ou modifiée par le donneur d'ordre ;

- 16.6 Si la législation applicable en matière de protection des données l'exige, le contractant tient un registre de traitement qu'il met immédiatement à la disposition du client sur demande ;
- 16.7 Le preneur d'ordre signale immédiatement au donneur d'ordre les violations de la protection des données. Le preneur d'ordre informe le donneur d'ordre en particulier en détail sur la nature de la violation de la protection des données ainsi que sur la catégorie et le nombre de personnes concernées et le nombre d'ensembles de données concernés. Le preneur d'ordre prend les mesures nécessaires à la sauvegarde des données et à l'atténuation des conséquences négatives éventuelles pour les personnes concernées et se concerta également sans délai avec le donneur d'ordre à ce sujet. En outre, le preneur d'ordre communique immédiatement si la violation de la protection des données entraîne des perturbations importantes dans l'exécution de la commande ou si le preneur d'ordre enfreint les dispositions ou les consignes de protection des données définies dans la présente commande ;
- 16.8 Le fournisseur désigne au client un interlocuteur pour les questions de protection des données qui se posent dans le cadre de la présente commande et, si la législation applicable en matière de protection des données le prescrit, il désigne un responsable de la protection des données interne ou externe à l'entreprise et communique au client les coordonnées correspondantes ;
- 16.9 Le contractant assiste en outre le client dans les évaluations d'impact sur la protection des données et les consultations préalables ;
- 16.10 Le mandataire informe immédiatement le mandant des actes de contrôle et des mesures prises par l'autorité de surveillance, dans la mesure où ils se rapportent au présent mandat ;
- 16.11 Le client et le contractant coopèrent, sur demande, avec les autorités de contrôle dans l'accomplissement de leurs tâches ;
- 16.12 Dans la mesure où le client est soumis à un contrôle de l'autorité de contrôle, à une procédure administrative ou pénale, à une action en responsabilité d'une personne concernée ou d'un tiers ou à toute autre action en relation avec le traitement de la commande auprès du fournisseur, ce dernier apportera son soutien au client dans la mesure du possible ;
- 16.13 Le contractant ne transmet des informations à des tiers ou à des personnes concernées qu'avec l'accord écrit préalable du client. Les demandes directes adressées au contractant sont immédiatement transmises par celui-ci au client ;
- 16.14 Le preneur d'ordre ne peut rectifier, effacer ou limiter le traitement des données traitées dans le cadre de la commande qu'après avoir reçu des instructions documentées du donneur d'ordre. Dans la mesure où une personne concernée s'adresse directement au preneur d'ordre à ce sujet, le preneur d'ordre renverra cette personne au donneur d'ordre et transmettra immédiatement la demande au donneur d'ordre ;
- 16.15 Le sous-traitant contrôle régulièrement les processus internes ainsi que les mesures techniques et organisationnelles afin de garantir que le traitement dans son domaine de responsabilité s'effectue conformément aux exigences de la législation applicable en matière de protection des données.



- 16.16 Si les documents, les données ou le matériel informatique du client se trouvant chez le fournisseur sont menacés par des mesures prises par des tiers (par exemple par une saisie ou une confiscation), par l'insolvabilité ou par d'autres événements, le fournisseur doit en informer immédiatement le client.
- 17 Mesures techniques et organisationnelles
- 17.1 Le mandataire doit assurer la sécurité des données par des mesures appropriées conformément à l'article 8 LPD. Les différentes mesures sont décrites dans l'annexe I ci-après.
- 17.2 Il s'agit de mesures de sécurité des données et de la garantie d'un niveau de protection adéquat en matière de confidentialité, d'intégrité, de disponibilité et de résistance des systèmes. Il est tenu compte de l'état de la technique, des coûts ainsi que de la nature, de l'étendue et des finalités du traitement. Les mesures garantissent notamment la détection en temps réel des violations de la sécurité et de la protection des données.
- 17.3 Le contractant veille notamment à ce que les données traitées dans le cadre de cette mission soient strictement séparées des autres bases de données.
- 17.4 Le mandataire garantit la preuve des mesures techniques et organisationnelles prises vis-à-vis du mandant dans le cadre de ses pouvoirs de contrôle selon le point 8 ci-après.
- 17.5 Les mesures techniques et organisationnelles sont soumises au progrès technique et au développement. Dans cette mesure, le contractant est autorisé à mettre en œuvre des mesures alternatives adéquates. Ce faisant, le niveau de sécurité des mesures définies ne doit pas être inférieur.
- 17.6 Les modifications importantes sont documentées et communiquées immédiatement par écrit au client. Le mandataire informe alors le mandant des mesures concernées par l'adaptation selon l'Addendum I, des motifs de l'adaptation, des systèmes concernés et de l'impact de l'adaptation sur la protection des données personnelles faisant l'objet du contrat.
- 18 Relations de sous-traitance
- 18.1 Aux fins de la présente réglementation, on entend par relations de sous-traitance les prestations de services qui se rapportent directement à la fourniture de la prestation principale.
- 18.2 Le preneur d'ordre est autorisé à faire appel à des sous-traitants pour le traitement des données.
- 19 Droits de contrôle du mandant
- 19.1 Le donneur d'ordre, le cas échéant son autorité de contrôle ainsi que, si le donneur d'ordre agit également en tant que sous-traitant pour eux, ses clients (ci-après "personnes autorisées à contrôler") ont le droit de procéder à des contrôles en concertation avec le preneur d'ordre ou de les faire effectuer par des contrôleurs à désigner au cas par cas. Le droit de contrôle du donneur d'ordre se limite à une fois tous les 12 mois, sauf si le donneur d'ordre peut invoquer une raison importante.
- 19.2 Le donneur d'ordre a le droit de s'assurer du respect du présent contrat par le preneur d'ordre dans son entreprise et dans le centre de données utilisé par ce dernier, ainsi que dans les locaux d'éventuels sous-traitants, par le biais de contrôles ponctuels, qui doivent en règle générale être annoncés à temps (c'est-à-dire dans un délai de 10 jours ouvrables).



- 19.3 Le mandant et, le cas échéant, les autres personnes autorisées à effectuer des contrôles peuvent notamment demander des renseignements, exiger de consulter les données enregistrées et les programmes de traitement des données et effectuer d'autres contrôles sur place.
- 19.4 Le contractant et, le cas échéant, les autres personnes autorisées à effectuer des contrôles sont tenus d'accorder les accès et les vues nécessaires à l'exécution des contrôles, ainsi que d'indiquer les procédures requises, de fournir les renseignements et de tenir les registres nécessaires à cet effet.
- 19.5 Le contractant s'assure que le client et, le cas échéant, les autres personnes autorisées à effectuer des contrôles peuvent s'assurer à tout moment du respect des obligations du contractant ou de ses sous-traitants découlant de la présente commande.
- 19.6 Le contractant s'engage à fournir à tout moment au client et, le cas échéant, aux autres personnes autorisées à effectuer des contrôles, les renseignements nécessaires sur demande et à prouver notamment la mise en œuvre des mesures techniques et organisationnelles.
- 19.7 La preuve de telles mesures, qui ne concernent pas uniquement le mandat concret, peut être apportée par :
- des attestations, rapports ou extraits de rapports récents d'instances indépendantes (par exemple, commissaires aux comptes, auditeurs, délégués à la protection des données, service de sécurité informatique, auditeurs chargés de la protection des données, auditeurs de qualité) ;
 - une certification appropriée par un audit de sécurité informatique ou de protection des données.
- 19.8 Le contractant est tenu de se faire accorder contractuellement par ses sous-traitants les droits de contrôle du client et, le cas échéant, des autres personnes autorisées à effectuer des contrôles.
- 19.9 Si le contractant estime que des actions concrètes d'audit et de contrôle dépassent le cadre habituel, il doit en informer le client à temps afin qu'un accord préalable sur les coûts puisse être trouvé. La rémunération d'éventuels sous-traitants est du ressort du preneur d'ordre. Le droit à la rémunération est supprimé si les contrôles révèlent des violations de la présente convention par le preneur d'ordre ou ses sous-traitants.
- 20 Copies, effacement et restitution de données personnelles
- 20.1 Aucune copie ou duplication des données n'est effectuée à l'insu du donneur d'ordre. Font exception à cette règle les copies de sécurité, dans la mesure où elles sont nécessaires pour garantir un traitement correct des données, ainsi que les données nécessaires en vue de respecter les obligations légales de conservation.
- 20.2 Le donneur d'ordre décide lui-même à tout moment quelles données il souhaite supprimer dans le logiciel. Une suppression ne signifie pas automatiquement une destruction des données. Les données supprimées sont toujours présentes dans les sauvegardes du système et sont écrasées au bout de deux ans dans le cadre des cycles de sauvegarde. Une destruction définitive peut être commandée par le client contre remboursement des frais.



- 20.3 Les documentations qui servent à prouver que le traitement des données est conforme à la commande et à la réglementation doivent être conservées par le mandataire au-delà de la fin de la commande, conformément aux délais de conservation respectifs. Le mandataire peut les remettre au mandant à la fin de la commande afin de le décharger.



Addendum I - Mesures techniques et organisationnelles

Les mesures techniques et organisationnelles prises par le sous-traitant pour garantir un niveau de sécurité adéquat sont décrites ci-dessous - en tenant compte de la nature, de la portée, du contexte et de la finalité du traitement ainsi que des risques pour les droits et libertés des personnes concernées :

1 Confidentialité

20.4 Contrôle d'accès : le contractant veille à ce qu'aucun accès non autorisé ne soit autorisé aux installations de traitement des données.

Le contrôle d'accès au centre de données et aux locaux du contractant ou de ses sous-traitants agréés, dans lesquels les données du client sont stockées ou traitées ou les données d'accès à ces mêmes données sont stockées, se présente comme suit :

- Système de contrôle d'accès via le système de fermeture
- Remise des clés uniquement à un nombre limité de personnes avec une liste de clés ;
- Dispositif de surveillance par système d'alarme et connexion au service de sécurité ;
- Porte d'accès fermée en permanence, accès aux locaux de l'entreprise uniquement après qu'un employé a sonné et ouvert la porte ;

20.5 Contrôle d'accès : le contractant s'assure qu'aucune utilisation non autorisée du système n'a lieu. Pour ce faire, il prend les mesures suivantes :

- Procédure de mot de passe (notamment exigences de complexité, longueur minimale, changement régulier du mot de passe avec gestion de l'historique) ;
- Authentification à deux ou plusieurs facteurs
- Création d'une fiche utilisateur par utilisateur ;
- Protection par mot de passe des supports de données ;
- Utilisation d'un verrouillage d'écran programmé avec protection par mot de passe ;
- si nécessaire, WLAN crypté pour l'utilisation interne, en plus découplé pour les invités dans la DMZ ;
- Concept de pare-feu sophistiqué ;

20.6 Contrôle d'accès : le contractant veille à ce qu'aucune lecture, copie, modification ou suppression non autorisée des données à caractère personnel traitées n'ait lieu au sein du système. Le contractant prend les mesures suivantes :

- Définition et contrôle des droits d'accès différenciés selon les données, les programmes et les types d'accès (concept d'autorisation) ;
- l'installation en temps utile des mises à jour de sécurité nécessaires ;
- Mise à jour permanente de la protection antivirus ;
- Évaluations des accès ;
- Réalisation d'audits de sécurité externes ;
- Gestion et conservation sécurisées des supports/stocks de données ;
- Cryptage / connexion tunnel (VPN = Virtual Private Network) pour un cercle restreint de collaborateurs ;



- 20.7 Contrôle de la séparation : le contractant veille à ce que les données à caractère personnel collectées à des fins différentes soient traitées séparément. Le contractant veille à la mise en œuvre des mesures suivantes :
- "multi-tenant" du logiciel utilisé ;
 - Séparation des fonctions entre la production et les tests ;
- 21 Intégrité
- 21.1 Contrôle de la transmission : le contractant veille à ce que les données à caractère personnel ne soient pas lues, copiées, modifiées ou supprimées sans autorisation lors d'une transmission électronique ou d'un transport. Pour ce faire, il prend les mesures suivantes :
- Rangement dans une zone sécurisée ;
- 21.2 Contrôle de l'introduction : le contractant contrôle régulièrement si et par qui des données à caractère personnel ont été introduites, modifiées ou supprimées dans les systèmes de traitement des données. Pour ce faire, il prend les mesures suivantes :
- Technique de consignation par enregistrement dans une base de données et évaluation du protocole de chaque utilisateur (ID utilisateur unique) ;
 - Instructions claires pour la saisie des données (instructions d'action) ;
 - Consignation dans le système de tickets.
- 22 Disponibilité et résistance au stress
- 22.1 Contrôle de la disponibilité : le contractant veille à ce que les données à caractère personnel soient protégées contre toute destruction ou perte accidentelle ou intentionnelle. Le contractant prend les mesures suivantes :
- Procédure de sauvegarde définie ;
 - Garantie de disponibilité grâce à des systèmes de stockage redondants ;
 - Alimentation électrique ininterrompue (garantie au centre de données sous-traitant)
 - Salle de serveurs sécurisée et climatisée (redondante) (garantie auprès du centre de données sous-traitant) ;
 - Conservation séparée dans l'espace et dans le milieu ;
 - Protection antivirus / pare-feu ;
 - Système de détection de fumée (garanti auprès du centre de données sous-traitant) ;
 - Extincteur à CO2 (garanti auprès du centre de données sous-traitant) ;
 - Plan d'urgence ;
- 22.2 Le contractant veille à ce que les systèmes et les données du client puissent être restaurés rapidement.
- 23 Procédures de contrôle, d'évaluation et de suivi réguliers
- 23.1 Le contractant veille à une gestion adéquate de la protection des données et à une gestion des réponses aux incidents.
- 23.2 Le contractant met en œuvre des paramètres par défaut favorables à la protection des données afin de traiter le moins possible de données à caractère personnel.



24 Contrôle de la mission : le contractant met notamment en œuvre les mesures suivantes :

- Un contrat clair ;
- Passation de marché formalisée ;
- Engagement des employés et des entreprises mandatées (entreprises de services, conseillers fiscaux, experts-comptables, entreprises de sécurité et autres) à respecter la protection des données et la confidentialité ;