Accord sur le traitement des données

Remarques préliminaires

Le présent accord (accord) concrétise les obligations du client et du sous-traitant (ensemble les parties) en ce qui concerne les prescriptions de la loi suisse sur la protection des données (LPD) et du règlement général sur la protection des données de l'UE (RGPD UE). Il complète à cet égard les accords contractuels relatifs aux services fournis par le sous-traitant au client. Il peut s'agir d'un seul ou de plusieurs contrats entre le sous-traitant et le client (contrat).

L'accord s'applique dans la mesure où les conditions suivantes sont remplies :

Le client intervient soit en tant que responsable du traitement, soit en tant que sous-traitant dans le champ d'application de la LPD et/ou du RGPD de l'UE et

(a) le client fait appel à DAUF SA dans le cadre du contrat en tant que sous-traitant ou sous-traitant pour le traitement de données personnelles ou de données à caractère personnel qui relèvent du champ d'application de la LPD et/ou du RGPD de l'UE (données personnelles).

1. L'objet, la nature, la finalité et la durée du traitement des données

L'objet du traitement des données, sa nature, sa finalité et sa durée sont définis dans le contrat. Les catégories de données personnelles traitées, les catégories de personnes concernées par le traitement des données et les mesures techniques et organisationnelles (MTO) à prendre sont décrites dans le contrat et/ou dans les annexes 1 et 2 du présent accord.

Dans la mesure où le responsable du traitement de la commande assume d'autres services pour le client au cours de la collaboration ultérieure, le présent accord s'applique également à ces services.

2. Directives

(a) Respect des instructions : Le sous-traitant est tenu de traiter les données personnelles exclusivement conformément aux dispositions du contrat et du présent accord et de suivre les

instructions du client lors de leur traitement. Les obligations divergentes découlant du droit applicable (p. ex. obligations légales ou ordres contraignants des autorités compétentes) sont réservées.

(b) Légalité du traitement des données : le client est responsable de la légalité du traitement des données en soi, y compris de l'admissibilité du traitement des commandes/sous-commandes.

(c) Donner des instructions : Les instructions du client sont documentées dans le contrat et par le présent accord. Le client peut à tout moment donner par écrit des instructions supplémentaires au responsable du traitement. De telles instructions individuelles nécessitent l'accord préalable de l'exécuteur de la commande et doivent être documentées. Le responsable du traitement des commandes accepte ces instructions dans la mesure où elles sont réalisables et raisonnables dans le cadre des services convenus dans le contrat. Si de telles instructions entraînent des coûts supplémentaires pour le responsable du traitement des commandes ou une modification de l'étendue des prestations, la procédure de modification prévue dans le contrat s'applique.

(d) Licéité des instructions : Le responsable du traitement informe immédiatement le client s'il estime qu'une instruction est contraire à la LPD ou au RGPD. Dans ce cas, le sous-traitant peut suspendre l'application de la directive jusqu'à ce qu'elle soit confirmée ou modifiée par le client. Les parties conviennent que le client est seul responsable du traitement des données personnelles conformément aux instructions. Le responsable du traitement peut à tout moment partir du principe que les instructions du client concernant les droits d'accès aux données personnelles ou leur remise à ce dernier sont conformes à la loi.

3. Autres obligations du sous-traitant

(a) Limitation des finalités : Le responsable du traitement traite les données personnelles exclusivement dans le but d'exécuter le contrat et conformément aux dispositions convenues dans le contrat et le présent accord. Le sous-traitant se réserve le droit d'anonymiser ou d'agréger les données personnelles, de sorte qu'il ne soit plus possible d'identifier les personnes concernées, et de les utiliser sous cette forme à des fins de conception, de développement et d'optimisation en fonction des besoins, ainsi que pour fournir le service convenu conformément au contrat.

(b) Mesures techniques et organisationnelles (MTO) : le sous-traitant prend des MTO appropriées, et en tout cas au moins celles décrites à l'annexe 2, pour protéger les données personnelles. Le sous-traitant est autorisé à adapter les MTD pendant la durée du contrat, pour

autant que le niveau de sécurité ne soit pas abaissé. En cas de contradiction, les MTD plus spécifiques prévues dans le contrat priment sur celles de l'annexe 2.

(c) Registre des traitements de données : Le responsable du traitement tient un registre de ses traitements de données personnelles conformément aux exigences de l'art. 12, al. 1 LPD et de l'art. 30, al. 2 RGPD. Sur demande, le sous-traitant permet au client de consulter les parties du registre de traitement qui concernent le traitement de données personnelles pertinentes pour les prestations de service qui lui sont fournies.

(d) Confidentialité et discrétion : le sous-traitant veille à ce qu'il soit interdit aux personnes chargées du traitement des données personnelles de les traiter à d'autres fins que celles convenues et en dérogation au présent accord. Il s'assure en outre que toutes les personnes ayant accès aux données personnelles sont soumises à une obligation légale ou contractuelle de confidentialité/de secret professionnel. Dans la mesure où les données personnelles traitées sont soumises au secret professionnel, le responsable du traitement agit en tant qu'auxiliaire et remplit les obligations légales applicables.

(e) Confidentialité et discrétion : le sous-traitant veille à ce qu'il soit interdit aux personnes chargées du traitement des données personnelles de les traiter à d'autres fins que celles convenues et en dérogation au présent accord. Il s'assure en outre que toutes les personnes ayant accès aux données personnelles sont soumises à une obligation légale ou contractuelle de confidentialité/de secret professionnel. Dans la mesure où les données personnelles traitées sont soumises au secret professionnel, le responsable du traitement agit en tant qu'auxiliaire et remplit les obligations légales applicables.

(f) Les obligations d'assistance:

(i) Si une personne concernée s'adresse au responsable du traitement en rapport avec des droits en matière de protection des données (par exemple une demande de rectification, d'information ou d'effacement), le responsable du traitement transmet immédiatement la demande correspondante au client. Il soutient le client de manière appropriée dans le traitement de telles demandes. En cas de travail important, le responsable du traitement des commandes peut exiger une rémunération séparée à convenir au préalable.

(ii) Le sous-traitant aide le client à réaliser une analyse d'impact sur la protection des données, à consulter l'autorité de contrôle, à lui faire des notifications et à lui fournir les données et informations nécessaires. En cas de travail important, le responsable du traitement peut demander une rémunération séparée à convenir au préalable.

(g) Obligation de restitution et de suppression :

(i) Les données personnelles doivent être restituées ou effacées à la fin du contrat conformément aux dispositions contractuelles ou aux instructions du client, à moins que le responsable du traitement ne soit légalement tenu de continuer à conserver les données personnelles. Le sous-traitant utilise les procédures usuelles dans la branche pour la suppression des données personnelles.

(ii) Les documents servant à prouver que les données personnelles ont été traitées conformément au mandat peuvent être conservés par le sous-traitant même après la fin de l'accord, conformément aux dispositions légales.

4. Devoirs et obligations du client

(a) Obligations réglementaires : Le client remplit toutes les obligations réglementaires applicables à son rôle de responsable du traitement des données personnelles. Il est seul responsable de la légalité du traitement des données personnelles et du respect des droits des personnes concernées dans les relations entre les parties. Si le client agit pour sa part en tant que sous-traitant d'un responsable, le sous-traitant est un sous-traitant. Dans ce cas, le client garantit avec chaque instruction qu'il s'agit de l'instruction du responsable. Si des tiers font valoir des prétentions à l'encontre du responsable du traitement en raison du traitement de données personnelles conformément au présent accord, le client libérera le responsable du traitement de toutes ces prétentions.

(b) Mesures techniques et organisationnelles (MTO): le client prend lui-même des mesures techniques et organisationnelles appropriées dans son domaine de responsabilité (par ex. ses systèmes et ses bâtiments) pour protéger les données personnelles.

(c) Obligations d'information:

(i) Le client informe immédiatement le sous-traitant s'il constate une violation de la protection des données dans la prestation de services du sous-traitant.

(ii) Si le sous-traitant est tenu de fournir des informations sur le traitement de données personnelles à une autorité publique ou à une personne, ou de coopérer d'une autre manière avec ces autorités, le client est tenu d'aider le sous-traitant à remplir ces obligations

5. Contact

(a) Client : personne de contact visible dans le contrat entre le client et DAUF SA

(b) Traitement des commandes : DAUF SA, Via Figino 6, 6917 Barbengo, dataprotection@dauf.ch

6. Sous-traitants

(a) Droit de faire appel à des tiers : à moins que le contrat ne contienne des dispositions restrictives concernant le recours à des tiers, le responsable du traitement est autorisé à faire appel à des sous-traitants. Ceci à condition que le sous-traitant conclue un accord avec le sous-traitant afin de garantir le respect des obligations prévues par le présent accord.

(b) Autorisation : Une liste des sous-traitants existants au début du contrat et autorisés par la présente à accéder aux données personnelles figure à l'annexe 3. Le sous-traitant informe le client des modifications envisagées. Dans un délai d'un mois à compter de la notification par le sous-traitant, le client peut s'opposer au recours au sous-traitant en question pour des raisons importantes liées à la protection des données. L'opposition du client doit être formulée par écrit et comporter les motifs de l'opposition. En présence d'un motif important relevant de la protection des données et si une solution à l'amiable entre les parties n'est pas possible, le client dispose d'un droit de résiliation pour le service concerné par le changement de sous-traitant.

7. Lieu du traitement des données

Toute communication de données personnelles par le sous-traitant à l'étranger ou à une organisation internationale n'est autorisée que si le sous-traitant respecte les dispositions des articles 16 et suivants du RGPD. LPD ou du chapitre V du RGPD de l'UE. En revanche, si une telle communication de données personnelles est souhaitée par le client ou effectuée sur son ordre, le respect des dispositions correspondantes incombe exclusivement au client.

8. Droits de contrôle

(a) Droit de contrôle : le responsable du traitement est tenu de fournir au client, à sa demande, des informations permettant de documenter le respect des obligations convenues. Le client

a le droit de vérifier le respect par le sous-traitant des obligations prévues par le présent accord. Le sous-traitant est tenu de coopérer de manière appropriée à ces contrôles. Lors de la planification et de l'exécution de l'audit, le client tient compte des besoins et des exigences de sécurité du responsable du traitement de la commande et doit respecter les obligations de confidentialité de ce dernier.

(b) Organisme de contrôle externe : le client a le droit de faire effectuer le contrôle visé au point 8(a) par un organisme externe, compétent et tenu à la confidentialité. Les frais de vérification encourus par le client sont à la charge de ce dernier.

(c) Mesures correctives : Si, dans le cadre de l'audit, des violations du présent accord sont constatées et prouvées, le responsable du traitement prend immédiatement les mesures correctives appropriées.

9. Dispositions finales

(a) Champ d'application : dans l'accord, les parties règlent uniquement la relation de traitement des données relevant de la protection des données. Elles n'ont pas l'intention d'étendre ou de restreindre le catalogue de prestations convenu dans l'accord de prestations.

(b) Responsabilité : la responsabilité découlant de la violation du présent accord est régi par les règles de responsabilité convenues pour les services ou applicables en vertu de la loi. Le Client s'engage également à indemniser le Sous-traitant de toute amende infligée au Sous-traitant, dans la mesure où le Client a une part de responsabilité dans l'infraction sanctionnée par l'amende.

(c) Durée : la durée du présent accord est déterminé par la durée de tous les contrats conclus entre le sous-traitant et le client, en vertu desquels le sous-traitant traite des données personnelles pour le client, dans la mesure où le présent accord n'impose pas d'obligations allant au-delà.

(d) Notifications : Les notifications prévues dans le présent Contrat doivent être expresses et sous forme de texte (par exemple, par courrier électronique ou postal), sauf accord contraire.

(e) Modifications et compléments : En dérogation à d'éventuelles réserves de forme écrite dans le contrat, le présent accord peut également être convenu ou modifié par voie électronique entre les parties.

(f) Règlement des litiges : le droit applicable et le for sont déterminés par le contrat. Le client reste toutefois en droit de demander des mesures provisoires devant tout tribunal compétent et de faire valoir ses droits à l'encontre du sous-traitant devant le tribunal saisi de l'action principale en cas de recours d'un tiers.

(g) Règlement des conflits : dans la mesure où le contrat ou des dispositions légales spéciales ne contiennent pas de dispositions plus strictes ou plus étendues, le présent accord prévaut sur le contrat en cas de contradictions. Pour le reste, les dispositions du contrat, y compris les autres dispositions relatives à la protection des données et à la sécurité, restent applicables sans modification.

Annexe 1 : Concrétisation sur le traitement des données

1. Types de données personnelles

Le traitement de données sur commande peut notamment comprendre les catégories de données personnelles suivantes :

a. *Données de base* (données se rapportant directement à la personne et à ses caractéristiques ; p. ex. prénom, nom, date de naissance, âge, sexe, nationalité, numéro AVS, état civil, informations sur le profil professionnel et l'emploi, historique du client, etc.).
b. *Données relatives à la* santé (données relatives à l'état de santé d'une personne ; p. ex. diagnostics, formes de thérapie, médecin traitant, etc.)
c. *Données contractuelles* (données générées dans le cadre de la conclusion ou de l'exécution d'un contrat ; par exemple, relation contractuelle, intérêt pour le produit ou le contrat, données de facturation et de paiement, etc.)
d. *Données de communication* (par ex. adresse électronique, numéro de téléphone, adresse, contenu de la correspondance, données marginales, etc.)
e. *Données techniques et informations sur l'utilisateur* (données générées dans le cadre de l'utilisation du site web ou de l'application, par ex. adresse IP, données de connexion, numéro de client, numéro personnel, etc.)
f. *Données* comportementales (par exemple, données sur l'utilisation des sites web, informations sur l'utilisation des communications électroniques)
g. *Données de préférence* (données qui renseignent sur les besoins, les intérêts, les préférences, les caractéristiques ou le comportement probable)
h. *Autres données* (p. ex. données en rapport avec des procédures administratives ou judiciaires, dans le cadre de concepts de protection, photos, vidéos et enregistrements sonores, données de réenregistrement)

2. Données personnelles sensibles

Il s'agit de données personnelles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques et biométriques permettant d'identifier une personne physique de manière unique, les données relatives à la santé et les données relatives à la vie privée.

3. Données à caractère secret

Il peut s'agir par exemple de données soumises au secret professionnel ou à l'obligation de discrétion prévue par le droit des assurances sociales.

4. Personnes concernées

Les catégories de personnes suivantes peuvent notamment être concernées par le traitement des données de commande :

a. Clients finaux actuels, anciens et potentiels, pharmacies, drogueries, maisons de retraite et divers,
b. Collaborateurs actuels, anciens et potentiels et autres auxiliaires du client
c. Les partenaires commerciaux, vendeurs, fournisseurs, conseillers, représentants du client qui sont des personnes physiques ainsi que leurs collaborateurs.

Annexe 2 : Mesures techniques et organisationnelles

La présente annexe décrit les mesures techniques et organisationnelles que le sous-traitant doit prendre pour garantir un niveau de protection adapté au risque. Les mesures sont à comprendre de manière générique et s'appliquent à chaque fois que rien d'autre n'est défini dans le contrat. Si le traitement des données est effectué par des sous-traitants auxquels le responsable du traitement fait appel, cette dernière veille, par le biais d'accords contractuels appropriés, à ce que les sous-traitants respectent des mesures comparables.

Il incombe exclusivement au client de juger si les mesures techniques et organisationnelles décrites ci-après sont appropriées pour protéger les données confiées au sous-traitant (notamment les données personnelles sensibles ou les données liées au secret).

Contrôle d'accès

- Les surfaces sont divisées en zones de sécurité plus ou moins sécurisées. Les zones publiques sont accessibles à tout le monde. Pour accéder aux zones sécurisées, il faut un badge, une clé ou un objet similaire. En cas d'utilisation de badges, ceux-ci doivent en principe être personnalisés. Si des badges non personnalisés sont utilisés, les propriétaires temporaires sont enregistrés. La remise de clés ou d'objets similaires aux personnes autorisées est également consignée. La procédure de remise des badges, des clés ou autres sont réglée dans des documents correspondants. Les visiteurs doivent s'enregistrer et sont accompagnés par le personnel responsable dans les zones sécurisées.
- Les centres de données disposent des mesures de protection physique nécessaires pour détecter en temps réel un accès non autorisé et déclencher une alarme correspondante.
- Les centres de calcul disposent des autres mesures de protection nécessaires pour réduire autant que possible les risques dus à des phénomènes naturels tels que la foudre, la pluie, les inondations, etc. de manière qu'ils ne soient plus pertinents pour l'exploitation du centre de calcul.
- Si des centres de données tiers sont utilisés pour le stockage permanent de données dans le cadre des services, il est veillé à ce que les exploitants d'un tel centre de données remplissent des conditions comparables et donc un niveau de sécurité équivalent.
- Les centres de données peuvent être surveillés par vidéo. La durée de conservation et l'accès aux enregistrements sont définis.
- Dans le cas où le client enregistre ses données sur son site, DAUF SA peut donner des recommandations sur la manière dont ces locaux doivent être sécurisés. Il est de la responsabilité du client de prendre les mesures de protection nécessaires.
- Le personnel est sélectionné avec soin.
- Lors de leur entrée en fonction, les nouveaux collaborateurs sont familiarisés avec les règles pertinentes relatives à leur propre sécurité et à la sécurité des données.
- Les collaborateurs en place sont régulièrement formés à la manipulation soigneuse des données et sensibilisés aux risques de sécurité.

- Lorsque les collaborateurs quittent DAUF SA, l'identification sur les systèmes et l'accès aux bâtiments sont bloqués.

Contrôle d'accès :

- L'accès aux systèmes de DAUF SA se fait au moyen d'identifiants personnalisés.
- L'accès aux systèmes est toujours protégé au moins par un mot de passe ou une caractéristique d'authentification équivalente et les identifiants d'utilisateur correspondants.
- Il existe des exigences minimales en matière de complexité des mots de passe.
- En cas d'erreur de connexion, l'identification est temporairement bloquée après plusieurs tentatives infructueuses. Il existe un processus de réinitialisation des identifications bloquées.

Contrôle d’accès :

- Les autorisations sur les systèmes sont structurées de manière que seules les données nécessaires à l'accomplissement de la tâche puissent être consultées.
- Si un collaborateur a besoin de droits supplémentaires, il peut commander un rôle supplémentaire. La validation de ce rôle supplémentaire est effectuée par le propriétaire du rôle.
- Pour tous les rôles, il est régulièrement vérifié si les utilisateurs attribués ont encore besoin de ces rôles.
- Le trafic de données entre le réseau du client et DAUF SA est, dans la mesure du possible, crypté. Le cryptage peut se faire de différentes manières.
- Le réseau est protégé par un pare-feu, par un système de détection d'intrusion (IDS) et par une segmentation du réseau.
- Des antivirus sont utilisés et régulièrement mis à jour.
- Les systèmes serveur et client sont régulièrement corrigés.
- Les accès aux données et aux systèmes sont consignés.

Contrôle du transport :

- L'accès aux données pertinentes via Internet se fait toujours par le biais d'une connexion cryptée.

Contrôle de la mémoire :

- Les mémoires permanentes dans les centres de données disposent d'une alimentation électrique redondante et des systèmes nécessaires pour permettre un fonctionnement autonome pendant une période définie.
- Pour se protéger contre les dégâts causés par la fumée ou les incendies, les centres de données disposent de systèmes de détection de fumée et d'incendie.
- En cas de défaut, les supports de données sont rendus physiquement inutilisables ou confiés à un récupérateur certifié afin d'exclure totalement tout accès possible.

- Les supports de données en état de marche sont effacés à l'aide des procédures d'effacement usuelles dans la branche, de manière qu'il soit pratiquement impossible de reconstruire les données qu'ils contiennent. Si une telle procédure n'est pas possible, les supports de données sont rendus physiquement inutilisables ou détruits.

Contrôle de la saisie :

- Les entrées ou les modifications dans les systèmes de traitement des données sont consignées.

Contrôle des disponibilités :

- Des sauvegardes régulières sont effectuées afin d'éviter la perte de données en cas de problème du système.
- Pour garantir la disponibilité des données, les systèmes de stockage sont configurés de manière que plus d'un composant puisse tomber en panne et que les données soient malgré tout toujours disponibles.

Principe de séparation :

- Il est garanti au niveau logique et physique que les données des clients ne peuvent pas être consultées par les autres.

Examen, appréciation et évaluation :

- Des audits sont réalisés périodiquement.
- Les installations de sécurité informatique sont soumises de manière récurrente à un audit de sécurité informatique réalisé par des experts externes.

En cas de divergence, c'est la version allemande qui fait foi.