

---

## Convention de traitement des données en sous-traitance

---

### Remarques préliminaires

La présente convention concrétise les obligations des donneurs d'ordre et des sous-traitants (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 (RGPD) de l'UE. Elle complète à cet égard les accords contractuels entre HCI Solutions SA (sous-traitant) et le client (donneur d'ordre). Il peut s'agir d'un ou de plusieurs contrats entre HCI Solutions SA et le client. Des détails précis sur les «contrats» figurent dans les annexes.

Dans le cadre des prestations, le donneur d'ordre met des données personnelles à la disposition du sous-traitant à des fins de traitement sur mandat; soit le sous-traitant collecte des données personnelles sur mandat du donneur d'ordre, soit il a accès, dans le cadre de l'exécution de son mandat, à des données personnelles dont le donneur d'ordre est responsable. Afin de garantir le respect des exigences de la loi suisse sur la protection des données (LPD) et du règlement général sur la protection des données (RGPD de l'UE), les parties concluent la présente convention de traitement des données en sous-traitance (l'**accord**).

---

### 1. Objet du contrat

- (a) Objet: Dans la convention, les parties règlent uniquement la relation de sous-traitance en vertu de la législation sur la protection des données. Elles n'ont pas l'intention d'étendre ou de restreindre le catalogue de prestations convenu dans la convention de service.
- (b) Règlement des conflits: En cas de contradictions entre des dispositions contractuelles, l'ordre suivant s'applique: les annexes de la présente convention prévalent sur la convention et cette dernière prime dans son ensemble la convention de service. Si les parties concluent ou ont conclu un autre contrat de sous-traitance pour une prestation, les exigences les plus strictes s'appliquent.
- (c) Définitions: Dans la présente convention, les termes en gras sont utilisés avec la signification qui leur est attribuée. Les termes juridiques tels que «données personnelles», «traitement», etc. ont la signification définie dans le droit applicable en matière de protection des données.

---

**2. Objet et durée du traitement des commandes**

- (a) Traitement des commandes: Le sous-traitant traite des données personnelles inclus «données sensibles» en rapport avec les prestations pour le compte du donneur d'ordre (ensemble **des données de commande**). L'objet du traitement des commandes, sa nature et sa finalité découlent de la convention de service. Les catégories de personnes concernées par le traitement des commandes et les catégories de données personnelles concernées sont décrites à l'annexe 1.
- (b) Autres prestations: Dans la mesure où le sous-traitant assure d'autres prestations pour le donneur d'ordre au cours de la collaboration ultérieure, la présente convention s'applique également à ces prestations.
- (c) Durée: La présente convention prend effet au moment de sa signature ou, si elle est postérieure, à l'entrée en vigueur de la convention de service, mais au plus tard au moment du premier accès du sous-traitant aux données de commande. Elle prend fin à la résiliation de la convention de service, mais au plus tôt avec la suppression de toutes les données de commande traitées pour le compte du donneur d'ordre.
- (d) Position du donneur d'ordre: Le donneur d'ordre est conscient qu'il est responsable légalement de la licéité de la collecte et du traitement des données de commande et du respect des droits des personnes concernées en relation avec les prestations.

---

**3. Obligations du sous-traitant**

- (a) Respect des instructions:
  - (i) Le sous-traitant est tenu d'utiliser les données de commande exclusivement aux fins des prestations et de suivre les instructions du donneur d'ordre lors de leur traitement. Sont réservées les obligations divergentes du droit applicable (p. ex. directives contraignantes des autorités compétentes).
  - (ii) Le droit d'émettre des instructions est limité par la convention de service et par la présente convention. Les instructions doivent être données sous forme de texte. Le donneur d'ordre est tenu de documenter toutes les instructions de manière appropriée.

- (b) Lieu du traitement des données: Le traitement des données s'effectue en principe en Suisse. Toute communication de données pertinentes par HCI Solutions à l'étranger ou à une organisation internationale n'est autorisée que dans le respect de la loi sur la protection des données et en particulier des dispositions des articles 16 et suivants ou du chapitre V du RGPD de l'UE. En revanche, dans la mesure où une telle communication de données pertinentes est souhaitée par le client ou effectuée pour son compte, le respect des dispositions correspondantes incombe exclusivement au client.
- (c) Obligation de restitution et de suppression: Les données de commande doivent être restituées ou supprimées à la fin du contrat, conformément aux dispositions contractuelles ou aux instructions du donneur d'ordre. Le sous-traitant utilise les procédures usuelles de la branche pour la suppression des données de commande.

---

#### 4. Obligations d'assistance

- (a) Sécurité des données: Le sous-traitant assiste le donneur d'ordre de manière appropriée pour satisfaire à ses obligations légales de garantir une sécurité appropriée des données et de signaler les violations de la protection des données, ainsi que pour la réalisation volontaire ou obligatoire d'analyses d'impact relatives à la protection des données. Le chapitre 5(b) s'applique en cas de violation de la protection des données.
- (b) Droits des personnes concernées: Si une personne concernée s'adresse au sous-traitant dans le cadre de droits en matière de protection des données (p. ex. avec une demande d'information ou de suppression), ce dernier transmet immédiatement la demande correspondante au donneur d'ordre. Il soutient le donneur d'ordre de manière appropriée pour le traitement de telles demandes, ainsi que pour les obligations de renseigner vis-à-vis des autorités. Cela inclut, si nécessaire, l'assistance dans la compilation des données et informations nécessaires.
- (c) Contact: Pour les questions relatives à la protection des données, il convient en premier lieu de contacter les personnes suivantes:
  - (i) **Donneur d'ordre**: Personne de contact indiquée dans le contrat entre le donneur d'ordre et HCI Solutions SA.
  - (ii) **Sous-traitant**: HCI Solutions SA, Untermattweg 8, case postale, 3000 Berne 1  
E-mail: [dataprotection@hcisolutions.ch](mailto:dataprotection@hcisolutions.ch), téléphone: +41 58 851 26 00

---

5. **Sécurité des données**

- (a) Mesures de sécurité: Le sous-traitant prend des mesures techniques et organisationnelles appropriées, mais dans tous les cas au moins celles décrites à l'annexe 2, pour protéger les données de commande (**Mesures de sécurité**). Pendant la durée de la convention, le sous-traitant est autorisé à adapter les mesures de sécurité, pour autant que le niveau de sécurité ne soit pas abaissé.
- (b) Signalement de violations:
- (i) En cas de violations de la sécurité concrètement supposées ou constatées qui entraînent la destruction, la perte, l'altération ou la divulgation de données personnelles, qu'elles soient contraires à la loi, au contrat, aux instructions ou involontaires, le sous-traitant en informe le donneur d'ordre le plus rapidement possible, en fournissant au moins les informations suivantes (celles-ci pouvant être transmises de manière échelonnée si elles ne sont pas connues immédiatement):
- une description de la nature de la violation, en indiquant, si possible, les catégories et le nombre approximatif de personnes et de catégories concernées et le nombre approximatif d'ensembles de données concernés et, en cas de divulgation à des personnes non autorisées, les personnes ou les groupes de personnes concernés;
  - le nom et les coordonnées d'un autre point de contact du sous-traitant pour toute information complémentaire;
  - les conséquences probables de la violation;
  - les mesures prises ou envisagées pour remédier à la violation ou pour éliminer ou atténuer ses conséquences.
- (ii) Le sous-traitant est tenu de fournir au donneur d'ordre, sur demande, d'autres renseignements pertinents concernant la violation de la sécurité, dans la mesure où cela est possible sans violer ses obligations contractuelles et légales de confidentialité.

---

**6. Mandataires secondaires**

(a) Admissibilité:

- (i) Pour la fourniture des prestations, le sous-traitant est autorisé à mettre des données de commande à la disposition de mandataires secondaires dans la mesure où le sous-traitant respecte les dispositions de la présente convention, et en particulier du chapitre 6, et qu'il a conclu avec ces mandataires secondaires une convention dont le contenu correspond pour l'essentiel à la présente convention.
- (ii) Par **mandataire secondaire**, on entend ici tout prestataire de services dont les prestations se rapportent directement au traitement de données de commande. Les fournisseurs de prestations annexes telles que les services de télécommunication, les services postaux / de transport, les prestations de maintenance ou l'élimination de supports de données ne sont pas des mandataires secondaires. Toutefois, même en cas de prestations annexes externalisées, le sous-traitant est tenu de conclure des accords contractuels appropriés et conformes à la loi.

(b) Approbation:

- (i) Une liste des mandataires secondaires existants à la date du début du contrat et autorisés par la présente, ayant accès aux données de commande, se trouve à l'annexe 3. Le sous-traitant informe le donneur d'ordre des modifications envisagées des rapports avec les mandataires secondaires dans un délai d'un mois. Après notification par le sous-traitant, le donneur d'ordre peut faire opposition à l'implication du mandataire secondaire concerné pour des raisons importantes relevant du droit de la protection des données. L'opposition du donneur d'ordre doit être formulée par écrit et indiquer les motifs de l'opposition.
- (ii) Le sous-traitant ne peut confier à un mandataire secondaire la réalisation de certaines activités de traitement que si:
  - Le sous-traitant a effectué toutes les vérifications et évaluations appropriées et nécessaires et s'est assuré de la fiabilité et des capacités du mandataire secondaire à cet égard:
    - (i) qu'il garantit le niveau de protection des données personnelles exigé par les lois sur la protection des données et
    - (ii) qu'il remplit les obligations du sous-traitant en vertu du présent contrat;

- le sous-traitant impose contractuellement au mandataire secondaire les mêmes obligations que celles prévues par le présent contrat, et notamment offre des garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées;
  - le mandataire secondaire met fin à ses activités de sous-traitance dès que le présent contrat prend fin.
- (c) Documentation: Sur demande, le sous-traitant transmet au donneur d'ordre une copie de sa/ses convention/s avec des mandataires secondaires (y compris, le cas échéant, les garanties appropriées), afin que le donneur d'ordre puisse vérifier le respect de la présente convention par le sous-traitant. Les parties des conventions qui ne sont pas pertinentes à cet égard peuvent être noircies.
- (d) Responsabilité: Le sous-traitant est responsable envers le donneur d'ordre du respect des obligations des mandataires secondaires.

---

## **7. Droits de contrôle**

- (a) Droit de contrôle: Le sous-traitant est tenu de fournir au donneur d'ordre, sur demande, des informations afin de documenter le respect des obligations convenues. Le donneur d'ordre a le droit de vérifier le respect des obligations découlant de la présente convention par le sous-traitant. Le sous-traitant est tenu de participer de manière appropriée aux contrôles. Lors de la planification et de la réalisation du contrôle, le donneur d'ordre tient compte des besoins et des exigences de sécurité du sous-traitant et est tenu de respecter les obligations de confidentialité du sous-traitant. Le chapitre 8(b) s'applique aux faits constatés dans le cadre de l'audit.
- (b) Organisme de contrôle externe: Le donneur d'ordre a le droit de faire effectuer le contrôle selon le chapitre 7 par un organisme externe compétent et soumis à la confidentialité. Les coûts du contrôle incombant au donneur d'ordre sont à la charge du donneur d'ordre.

---

## **8. Confidentialité**

- (a) Données de commande: Le sous-traitant s'engage à traiter les données de commande de manière strictement confidentielle et à ne les rendre accessibles qu'aux

personnes au sein de son organisation qui ont besoin d'accéder aux données de commande pour remplir leurs obligations. Il s'assure que toutes les personnes ayant accès aux données de commande sont soumises à une obligation de confidentialité légale ou contractuelle les concernant.

- (b) Autres informations: En ce qui concerne les faits dont elles ont connaissance dans le cadre de la présente convention, les deux parties sont en outre soumises aux obligations de confidentialité légales qui leur sont applicables et convenues entre elles dans la convention de service.

---

## **9. Dispositions finales**

- (a) Responsabilité: En cas de violation de la présente convention, les règles de responsabilité convenues pour les prestations ou en vigueur de par la loi s'appliquent.
- (b) Communications: Sauf accord contraire, les communications prévues dans la présente convention doivent être faites expressément et sous forme de texte (p. ex. par e-mail ou par courrier postal).
- (c) Modifications et compléments: Par dérogation à d'éventuelles réserves de forme écrite figurant dans le contrat, la présente convention peut également être convenue ou modifiée par voie électronique entre les parties.
- (d) Règlement des litiges: Le droit applicable et le for sont déterminés par la convention de service. Le donneur d'ordre reste toutefois en droit d'exiger des mesures provisionnelles devant tout tribunal compétent et de faire valoir ses prétentions à l'encontre du sous-traitant devant le tribunal de l'action principale en cas de recours par un tiers.

## Annexe 1 – Concrétisation de la Convention de traitement des données en sous-traitance

| Prestation                             | Catégories de données personnelles                                                                                                                                                                                                                                                                                                          | Personnes concernées |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| Compendium.ch                          | Inclus: eMediplan, Documedis CDS.CE, Documedis PCA.CE et Documedis Vac                                                                                                                                                                                                                                                                      | Patientèle           |
| Documedis eMediplan                    | Obligatoire: nom, prénom et date de naissance<br>Facultatif: autres données personnelles et informations de santé                                                                                                                                                                                                                           | Patientèle           |
| Documedis Ordonnance électronique      | Obligatoire: nom, prénom, date de naissance, adresse et médication<br>Facultatif: autres données personnelles                                                                                                                                                                                                                               | Patientèle           |
| Documedis CDS.CE                       | Obligatoire: médication<br>Facultatif: autres données patient (données personnelles et informations de santé), en fonction du contrôle qui doit être effectué.<br>Journaux de données: afin de garantir la sécurité de la patientèle, des données anonymisées sont exigées conformément à l'ordonnance sur les dispositifs médicaux (ODim). | Patientèle           |
| Documedis PCA.CE                       | Obligatoire: nom, prénom et date de naissance<br>Facultatif: autres données patient (données personnelles, informations de santé et médication).<br>Journaux de données: afin de garantir la sécurité de la patientèle, des données anonymisées sont utilisées conformément à l'ordonnance sur les dispositifs médicaux (ODim).             | Patientèle           |
| pharmaVISTA                            | Inclus: eMediplan, Documedis CDS.CE, Documedis PCA.CE, délivrance de l'ordonnance électronique Documedis et PMC Polymedications Check                                                                                                                                                                                                       | Patientèle           |
| CGP Contrôle de polymédication         | Obligatoire: nom, prénom et date de naissance<br>Facultatif: médicaments et autres données personnelles                                                                                                                                                                                                                                     | Patientèle           |
| VAC Saisie des vaccins / documentation | Obligatoire: nom, prénom et date de naissance<br>Facultatif: vaccinations, réponse aux questions concernant l'état de santé et autres données personnelles                                                                                                                                                                                  | Patientèle           |

## Annexe 2 – Exigences de sécurité

La présente annexe décrit les mesures techniques et organisationnelles prises par le responsable du traitement des commandes HCI Solutions SA afin de garantir un niveau de protection adapté aux risques. Du fait de sa localisation partagée avec Galenica SA, HCI Solutions partage en grande partie des règles de sécurité.

### (1) Pseudonymisation et cryptage des données à caractère personnel

- Dans la mesure du possible et en accord avec la finalité du traitement, les données personnelles sont pseudonymisées ou cryptées, avec conservation sécurisée des informations d'attribution ou de la clé.

### (2) Capacité à garantir durablement la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services liés au traitement

**Contrôle d'accès** – *l'accès aux installations dans lesquelles des données personnelles sont traitées doit être interdit aux personnes non autorisées; contrôle des supports de données personnelles* – *la lecture, la copie, la modification ou la suppression de supports de données doit être rendue impossible par les personnes non autorisées:*

- L'accès aux bâtiments de Galenica SA à Berne et Niederbipp est sécurisé par un badge. La procédure d'attribution des badges est décrite dans les documents contrôlés dans le système de gestion de Galenica SA.
- L'accès aux centres de calcul de Galenica SA n'est autorisé que pour les badges autorisés et nécessite en outre la saisie d'un code PIN personnel. Les portes des centres de calcul sont surveillées par le système d'alarme anti-intrusion (EMA), et une alarme retentit lorsqu'une porte reste ouverte pendant plus de 60 secondes. Si la porte reste ouverte pendant 30 secondes de plus, une alarme anti-intrusion est transmise au service technique d'exploitation.
- Les visiteurs doivent s'inscrire et se désinscrire dans un registre des visiteurs. À l'intérieur du bâtiment, les visiteurs sont accompagnés par un collaborateur de Galenica SA.
- Les centres de calcul font l'objet d'une vidéosurveillance. Le délai de conservation et l'accès aux données vidéo sont consignés dans des documents contrôlés dans le système de gestion de Galenica SA.

**Contrôle de l'accès** – *l'accès des personnes autorisées doit être limité aux données personnelles dont elles ont besoin pour l'accomplissement de leur mission; contrôle des utilisateurs* – *l'utilisation de systèmes automatisés de traitement des données au moyen de dispositifs de transmission de données par des personnes non autorisées doit être empêchée; contrôle de l'enregistrement* – *la saisie non autorisée dans la mémoire ainsi que la consultation, la modification ou la suppression non autorisées de données personnelles enregistrées doivent être empêchées:*

- L'accès aux données personnelles repose sur un modèle de droit d'accès aux données basé sur les rôles. Chaque utilisateur reçoit un identifiant unique.
- Il existe des prescriptions relatives à la complexité des mots de passe, dont le respect est techniquement imposé.
- Le réseau du Groupe Galenica est protégé par un pare-feu, un système de détection d'intrusion (Intrusion Detection System, IDS) et une segmentation du réseau.
- Tous les systèmes serveurs et clients exploités par Galenica SA sont équipés de scanners anti-virus mis à jour régulièrement.
- Les systèmes serveurs et clients exploités par Galenica SA sont régulièrement équipés de correctifs.

- En cas d'inactivité de plus de huit minutes d'un client, un économiseur d'écran protégé par mot de passe est activé.
- Il existe une directive interne selon laquelle les postes clients doivent être verrouillés par le système d'exploitation lorsqu'ils quittent temporairement leur poste de travail.
- Les autorisations pour les services informatiques de base (Active Directory, VPN, comptes FTP) ainsi que pour des applications sélectionnées sont vérifiées une fois par an par le Data Governance Manager; les autorisations d'accès éventuellement existantes à tort sont retirées.

**Contrôle des transports** – *lors de la communication de données personnelles ainsi que lors du transport de supports de données, il convient d'empêcher que les données puissent être lues, copiées, modifiées ou effacées sans autorisation; contrôle de la communication* – *les destinataires auxquels des données personnelles sont communiquées au moyen de dispositifs de transmission de données doivent pouvoir être identifiés:*

- Les données personnelles sont protégées de manière appropriée contre les accès et les interventions non autorisés, p. ex. au moyen d'un cryptage de transport, d'une signature, d'une interface protégée ou de toute autre manière. L'identification des destinataires des données personnelles est garantie dans la mesure du possible.
- Si HCI Solutions SA est responsable de la saisie des données de commande, des mesures sont prises pour garantir leur saisie correcte.

**(3) Capacité à rétablir rapidement la disponibilité des données à caractère personnel et l'accès à celles-ci en cas d'incident physique ou technique**

- L'infrastructure informatique de Galenica SA est en grande partie redondante. En particulier, les systèmes de serveurs seront exploités en miroir dans deux centres de données géographiquement séparés, selon les exigences de disponibilité définies.
- Les deux centres de calcul de Galenica SA disposent d'une alimentation électrique double (c.-à-d. redondante), dont l'un est en outre raccordé à ASI et au groupe électrogène de secours.
- Les deux centres de calcul de Galenica SA disposent en outre de deux connexions Internet séparées auprès de fournisseurs différents.
- Les deux centres de données disposent de systèmes de climatisation redondants indépendants l'un de l'autre. Le fonctionnement des redondances est contrôlé régulièrement.
- Les deux centres de calcul disposent d'un concept d'extinction d'incendie à trois niveaux, composé d'une détection par un système de détection précoce des incendies, d'un système d'alarme incendie et d'une extinction active.
- Il existe un concept de sauvegarde de tous les systèmes serveurs, qui est décrit dans les documents contrôlés dans le système de gestion de Galenica SA. Selon le système et le groupe de sauvegarde défini, les sauvegardes sont effectuées périodiquement à des intervalles différents, entre un quart d'heure et une fois par jour. Selon le groupe de sauvegarde, les sauvegardes sont conservées pendant au moins cinq jours et, si une application l'exige, à long terme. Si une application l'exige, les sauvegardes enregistrées sur bande sont périodiquement externalisées sur un autre site géographiquement séparé du Groupe Galenica.
- Il existe un système de gestion des urgences et des crises, qui est décrit dans les documents contrôlés dans le système de gestion de Galenica SA. Il existe notamment un plan d'urgence et de crise pour le scénario. Celui-ci régit la communication et l'information en cas de crise, définit les mesures immédiates et autres mesures réactives en fonction de différents scénarios de panne, décrit les scénarios d'exploitation informatique restreinte, définit les priorités pour le rétablissement du fonctionnement normal et donne des directives sur les tests et la formation à la procédure en cas de crise.

**(4) Procédures permettant de réexaminer, d'évaluer et d'apprécier régulièrement l'efficacité des mesures techniques et organisationnelles visant à garantir la sécurité du traitement**

- Il existe un registre des risques dans lequel sont répertoriés tous les risques identifiés. Le registre des risques est régulièrement soumis à une révision à laquelle participe la direction de HCI Solutions SA. Tous les six mois, la Direction de Galenica SA est également informée des principaux risques tirés du registre des risques informatiques.
- Le plan d'urgence et de crise est actualisé une fois par an.

### Annexe 3 – Mandataires secondaires autorisés

Les personnes suivantes sont considérées comme des mandataires secondaires autorisés au sens du chiffre 6(b) de la convention:

| Nom et siège       | Pays de traitement | Personnes concernées<br>Prestations                  | Tâche/s du mandataire secondaire                                                                                 |
|--------------------|--------------------|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Galenica SA, Berne | Suisse             | Infrastructure informatique et hébergement Documedis | Distribution de l'infrastructure informatique et de l'hébergement des applications Documedis eMediplan et CDS.CE |
| ISS                | Suisse             | MepFlix pour Vac Check                               | Distribution de l'infrastructure informatique et de l'hébergement de l'application Vac Check                     |

Attention : ce document a été traduit de l'allemand. En cas d'ambiguïté ou de divergence d'interprétation, les formulations de la version originale allemande prévalent et doivent être considérées comme prépondérantes.