



## **Annexe 1 – Traitement des commandes (Article 28 du RGPD)**

Entre XXXXXXXXXXXXXXXXXXXX – responsable - ci-après dénommé le donneur d'ordre – et

Fairmas GmbH, EUREF-Campus 13, 10829 Berlin – sous-traitant - ci-après dénommé le mandataire.

### **1. Objet et durée du contrat**

#### **(1) Objet**

L'objet de la commande résulte des contrats de service suivants auxquels il est fait référence ici (ci-après les contrats de service).

#### **(2) Durée**

La durée du présent CONTRAT (terme) correspond à la durée des contrats de service dans tous les cas, tant que le mandataire traite les données personnelles du donneur d'ordre (y compris les sauvegardes).

- (3) Dans la mesure où d'autres conventions conclues entre le donneur d'ordre et le mandataire aboutissent à d'autres accords relatifs à la protection de données à caractère personnel, le présent CONTRAT sur le traitement des commandes prévaut, sauf convention expresse contraire des parties.

### **2. Spécification du contenu de la commande**

#### **(1) Type et finalité du traitement prévu des données**

Le type et la finalité du traitement des données à caractère personnel par le mandataire pour le donneur d'ordre sont décrits dans le(s) contrat(s) de service mentionné(s) au point 1.

#### **(2) Type de données**

Font l'objet du traitement des données personnelles les types et catégories de données suivants (énumération / description des catégories de données)

- Données de base personnelles (titre, prénom, nom)
- Données de communication (téléphone, e-mail)
- Données de base du contrat (relation contractuelle, intérêt produit et/ou contractuel)
- Historique du client
- Données de facturation et de paiement
- Données de planification et de contrôle
- Données financières de l'entreprise
- Informations sur les salaires et revenus

#### **(3) Catégories de personnes concernées**

Les catégories de personnes concernées par le traitement comprennent :

- Clientèle
- Salariés
- Interlocuteurs

### **3. Mesures techniques et organisationnelles**

- (1) Dans son domaine de responsabilité, le mandataire prend toutes les mesures techniques et organisationnelles nécessaires conformément à l'article 32 RGPD pour protéger les données à caractère personnel et remet la documentation au donneur d'ordre pour contrôle. Si elles sont acceptées par le donneur d'ordre, les mesures documentées deviennent la base du présent CONTRAT.

- (2) Si le contrôle / un audit du donneur d'ordre révèle un besoin d'ajustement, celui-ci doit être mis en œuvre d'un commun accord.



(3) Les mesures techniques et organisationnelles convenues sont soumises au progrès technique et au développement. À cet égard, le mandataire est autorisé à mettre en œuvre d'autres mesures adéquates à l'avenir. Ce faisant, les mesures définies doivent avoir au minimum le niveau de sécurité convenu à l'annexe 1. Le donneur d'ordre doit être informé immédiatement de tout changement important à documenter par le mandataire.

(4) Travail mobile

Travail à domicile et télétravail : le traitement des données faisant l'objet du présent CONTRAT est autorisé en dehors du ou des établissements du mandataire et dans des appartements privés.

#### 4. Droits des personnes concernées

(1) Le mandataire soutient le donneur d'ordre dans son domaine de responsabilité et, dans la mesure du possible, au moyen de mesures techniques et organisationnelles appropriées afin de répondre aux demandes des personnes concernées en ce qui concerne leurs droits en matière de protection des données et de les mettre en œuvre. Il ne peut pas accéder, transporter, corriger, supprimer ou restreindre le traitement des données traitées dans la commande de sa propre autorité, mais uniquement conformément aux instructions documentées du donneur d'ordre. Dans la mesure où une personne concernée s'adresse directement au mandataire à cet égard, le mandataire transmettra immédiatement cette demande au donneur d'ordre.

(2) Dans la mesure où l'étendue des prestations de services comprend les droits à l'information, à la correction, à la limitation du traitement, à la suppression et à la portabilité des données, ceux-ci doivent être assurés directement par le mandataire conformément aux instructions documentées du donneur d'ordre.

#### 5. Assurance de la qualité et autres obligations de l'entrepreneur

(1) En plus du respect des dispositions de cette commande, le mandataire a des obligations légales conformément au RGPD; à cet égard, il garantit le respect des prescriptions suivantes :

- a) La préservation de la confidentialité conformément aux articles 28, al. 3, phr. 2, let. b, 29, 32, al. 4 RGPD. Lors de l'exécution des travaux, le mandataire ne fait intervenir que des employés qui sont engagés à la confidentialité et qui ont déjà pris connaissance des dispositions relatives à la protection des données pertinentes. Le mandataire et toute personne subordonnée à celui-ci qui a légitimement accès aux données à caractère personnel ne peuvent traiter ces données que conformément aux instructions du donneur d'ordre, y compris aux compétences accordées dans le présent CONTRAT, à moins qu'ils ne soient légalement tenus de les traiter.
- b) Sur demande, le donneur d'ordre et le mandataire coopèrent avec l'autorité de surveillance dans l'exercice de leurs fonctions.
- c) Informer immédiatement le donneur d'ordre des contrôles et mesures de l'autorité de surveillance, dans la mesure où ils se rapportent au présent CONTRAT. Cela s'applique également si une autorité compétente enquête dans le cadre d'une procédure administrative d'infraction ou d'une procédure pénale concernant le traitement de données à caractère personnel lors du traitement des commandes auprès du mandataire.
- d) Dans la mesure où le donneur d'ordre est confronté à un contrôle de l'autorité de surveillance, à une procédure administrative d'infraction ou à une procédure pénale, à une réclamation en responsabilité d'une personne concernée ou d'un tiers, à une autre réclamation ou à une demande d'informations dans le cadre du traitement de la commande chez le mandataire, le mandataire doit le soutenir au mieux de ses capacités.
- e) Le mandataire contrôle régulièrement les processus internes ainsi que les mesures techniques et organisationnelles afin de garantir que le traitement dans son domaine de responsabilité est effectué conformément aux exigences de la loi applicable en matière de protection des données et que la protection des droits de la personne concernée est assurée.



- f) Vérifiabilité des mesures techniques et organisationnelles prises vis-à-vis du donneur d'ordre dans le cadre de ses compétences de contrôle conformément au chiffre 8 du présent CONTRAT.
  - g) Le mandataire signale immédiatement au donneur d'ordre les violations de la protection des données à caractère personnel de manière à ce que le donneur d'ordre puisse respecter ses obligations légales, en particulier conformément aux articles 33, 34 RGPD. Il élabore une documentation pour l'ensemble du processus, qu'il met à la disposition du donneur d'ordre pour d'autres mesures.
  - h) Le mandataire soutient le donneur d'ordre dans son domaine de responsabilité et, dans la mesure du possible, dans le cadre des obligations d'information existantes vis-à-vis des autorités de surveillance et des personnes concernées et lui fournit sans délai toutes les informations pertinentes dans ce contexte.
  - i) Dans la mesure où le donneur d'ordre est tenu de procéder à une analyse d'impact sur la protection des données, le mandataire le soutient en tenant compte du type de traitement et des informations dont il dispose. Cela s'applique également à une éventuelle obligation de consulter l'autorité de surveillance compétente en matière de protection des données.
- (2) Le présent CONTRAT ne dispense pas le mandataire de se conformer à d'autres exigences du RGPD.

## 6. Sous-traitance

- (1) Par relations de sous-traitance au sens du présent règlement, on entend des prestations de services qui se rapportent directement à la fourniture de la prestation principale. Cela n'inclut pas les services auxiliaires auxquels le mandataire a recours, par exemple les services de télécommunications, les services postaux / de transport, les services de nettoyage ou les services de surveillance. Les services de maintenance et d'inspection constituent une relation de sous-traitance s'ils sont fournis pour des systèmes informatiques fournis dans le cadre d'une prestation de service fournie par le mandataire conformément au présent CONTRAT. Cependant, le mandataire est tenu de conclure des accords contractuels appropriés et conformes à la loi pour assurer la protection des données et la sécurité des données du donneur d'ordre, même dans le cas de services auxiliaires externalisés, ainsi que de prendre des mesures de contrôle.
- (2) Conformément à l'article 28, al. 2, phr. 2 RGPD, le donneur d'ordre donne au mandataire l'autorisation générale de faire appel à d'autres sous-traitants pour le traitement des données du donneur d'ordre (sous-traitants).

L'aperçu actuel des autres mandataires est publié par le mandataire sur le site Web suivant et peut y être consulté par le donneur d'ordre à tout moment sous forme actuelle.

<https://fairmas.com/fr/data-protection-software/>

En outre, le donneur d'ordre peut à tout moment demander la liste des autres mandataires (sous-traitants) par écrit ou par e-mail à [datenschutz@fairmas.com](mailto:datenschutz@fairmas.com).

En option, le donneur d'ordre peut être activement informé par le mandataire des modifications apportées à la liste des autres mandataires (sous-traitants). Pour ce faire, il s'impose d'indiquer une adresse e-mail générique ci-dessous : \_\_\_\_\_

L'obligation d'information susmentionnée est caduque si aucune adresse e-mail n'est spécifiée ou si l'adresse e-mail susmentionnée ne peut pas être jointe.

L'accord contractuel individuel avec les autres mandataires (sous-traitants) peut être soumis au donneur d'ordre à sa demande, sachant que les clauses commerciales sans référence à la loi sur la protection des données en sont exclues.

- (3) Le transfert de données à caractère personnel du donneur d'ordre au sous-traitant et les premiers travaux ne sont autorisés que si toutes les conditions pour une sous-traitance sont remplies. Le respect et la mise en œuvre des mesures techniques et organisationnelles chez le sous-traitant sont contrôlés en amont du traitement des données à caractère personnel, puis régulièrement par le mandataire en tenant compte du risque du sous-traitant. Le mandataire doit mettre les résultats du contrôle à la disposition du donneur d'ordre sur demande. En outre, le mandataire doit s'assurer



que le donneur d'ordre peut exercer ses droits en vertu du présent contrat (en particulier ses droits de contrôle) directement vis-à-vis des sous-traitants.

- (4) Si le sous-traitant fournit le service convenu en dehors de l'UE/EEE, le mandataire doit garantir l'admissibilité en vertu de la loi sur la protection des données en prenant les mesures correspondantes. Cela s'applique également si des prestataires de services au sens du chiffre 1, phrase 2, doivent intervenir.
- (5) Une externalisation suivante par le sous-traitant nécessite le consentement exprès du donneur d'ordre principal (au moins sous forme de texte).

Toutes les dispositions contractuelles de la chaîne contractuelle doivent également être imposées au sous-traitant suivant.

## 7. Transferts internationaux de données

- (1) Tout transfert de données à caractère personnel vers un pays tiers ou vers une organisation internationale nécessite une instruction documentée du donneur d'ordre et présuppose le respect des exigences relatives au transfert de données à caractère personnel vers des pays tiers conformément au chapitre V du RGPD.

Le traitement des données convenu par contrat a lieu exclusivement dans un État membre de l'Union européenne ou dans un autre État partie à l'accord sur l'Espace économique européen.

- (2) Dans la mesure où le donneur d'ordre ordonne un transfert de données à des tiers dans un pays tiers, il est responsable du respect du chapitre V du RGPD.

## 8. Droits de contrôle du donneur d'ordre

- (1) Le donneur d'ordre a le droit de procéder à des contrôles en consultation avec le mandataire ou de les faire effectuer par des auditeurs à nommer au cas par cas. Il a le droit de s'assurer du respect du présent accord par mandataire dans le cadre de ses activités commerciales au moyen de contrôles aléatoires, qui doivent généralement être notifiés en temps utile.
- (2) Le mandataire veille à ce que le donneur d'ordre puisse s'assurer que les obligations du mandataire en vertu de l'article 28 RGPD sont respectées. Le mandataire s'engage à donner au donneur d'ordre les renseignements nécessaires sur demande et, en particulier, à prouver la mise en œuvre des mesures techniques et organisationnelles.
- (3) La preuve des mesures technico-organisationnelles pour le respect des exigences particulières de la protection des données en général ainsi que de celles qui concerne la commande peut être fournie des manières suivantes :
  - par le respect des règles de conduite approuvées conformément à l'art. 40 RGPD
  - par la certification selon une procédure de certification approuvée conformément à l'art. 42 RGPD
  - par des attestations, des rapports ou des extraits de rapports actuels d'organismes indépendants (par exemple experts comptables, révision, délégués à la protection des données, service de sécurité informatique, auditeurs de protection des données, auditeurs de qualité)
  - par une certification appropriée par audit de sécurité informatique ou de protection des données (par exemple protection fondamentale BSI (*Office fédéral de la sécurité des technologies de l'information*)).

## 9. Autorisation de donner des instructions du donneur d'ordre

- (1) Le mandataire traite les données à caractère personnel uniquement sur la base d'instructions documentées du donneur d'ordre, à moins qu'il ne soit obligé de les traiter en vertu du droit de l'État membre ou du droit de l'Union. Le donneur d'ordre confirme immédiatement les instructions verbales (au moins sous forme de texte). Les instructions initiales du donneur d'ordre sont déterminées par le présent contrat.



**Systeme de gestion de la protection des  
donnees  
Fairmas GmbH**

Auteur : S. Meyzis

Date : 01.01.2023

Version : 06

- (2) Le mandataire doit informer immédiatement le donneur d'ordre s'il estime qu'une instruction viole les dispositions relatives à la protection des données. Le mandataire a le droit de suspendre l'exécution de l'instruction correspondante jusqu'à ce que le donneur d'ordre la confirme ou la modifie.

## 10. Suppression et restitution des données à caractère personnel


- (1) Il est interdit de copier ou dupliquer les données à l'insu du donneur d'ordre. Sont exclues les sauvegardes, dans la mesure où elles sont nécessaires pour assurer un traitement correct des données, ainsi que les données nécessaires dans le cadre du respect des obligations légales de conservation.
- (2) Après l'achèvement des travaux convenus par contrat ou plus tôt sur demande du donneur d'ordre – au plus tard à la résiliation du CONTRAT ou des contrats de service – le mandataire doit remettre au donneur d'ordre tous les documents en sa possession, les résultats de traitement et d'utilisation établis ainsi que les bases de données liées à la relation contractuelle ou les détruire avec consentement préalable conformément à la réglementation sur la protection des données. Cela s'applique également au matériel d'essai et de rebut. Le rapport de suppression doit être présenté sur demande.

\_\_\_\_\_  
Date/ Lieu

\_\_\_\_\_  
Date/ Lieu

\_\_\_\_\_  
Mandataire

\_\_\_\_\_  
Donneur d'ordre

	<b>Système de gestion de la protection des données</b> <b>Fairmas GmbH</b>	Auteur : S. Meyzis Date : 01.01.2023 Version : 06
---	---	---

## Annexe 1 – Mesures techniques et organisationnelles

### 1. Confidentialité (art. 32 al. 1 let. b RGPD)

(1) Accès :

Pas d'accès non autorisé aux systèmes de traitement de données, par exemple : cartes magnétiques ou à puce, clés, ouvre-portes électriques, sécurité de l'usine ou gardiens, systèmes d'alarme, systèmes vidéo

(2) Contrôle d'admission

Aucune utilisation non autorisée du système, par exemple : mots de passe (sûrs), mécanismes de verrouillage automatiques, authentification à deux facteurs, cryptage de supports de données

(3) Contrôle d'accès

Pas de lecture, copie, modification ou suppression non autorisée au sein du système, par exemple : concepts d'autorisation et droits d'accès basés sur les besoins, journalisation des accès

(4) Contrôle de séparation

Traitement séparé des données collectées à des fins différentes, par exemple multi-tenant, le sandboxing

(5) Pseudonymisation (art. 32 al. 1 let. a RGPD ; art. 25 al. 1 RGPD)

Le traitement des données à caractère personnel de manière à ne plus pouvoir attribuer les données à une personne concernée spécifique sans avoir recours à des informations supplémentaires, à condition que ces informations supplémentaires soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles appropriées

### 2. Intégrité (art. 32 al. 1 let. b RGPD)

(1) Contrôle de partage

Pas de lecture, copie, modification ou suppression non autorisée pendant la transmission ou le transport électronique, par exemple : cryptage, réseaux privés virtuels (VPN), signature électronique

(2) Contrôle d'entrée

Déterminer si et par qui les données à caractère personnel ont été saisies, modifiées ou supprimées dans les systèmes de traitement des données, par exemple : journalisation, gestion des documents

### 3. Disponibilité et résilience (art. 32 al. 1 let. b RGPD)

(1) Contrôle de disponibilité

Protection contre la destruction accidentelle ou intentionnelle ou contre la perte, par exemple : stratégie de sauvegarde (en ligne / hors ligne; sur site / hors site), alimentation sans interruption (ASI), protection antivirus, pare-feu, moyens de signalement et plans d'urgence

(2) Restauration rapide (art. 32 al. 1 let. c RGPD) ;

### 4. Procédure de test, d'analyse et d'évaluation réguliers (art. 32 al. 1 let. d RGPD ; art. 25 al. 1 RGPD)


(1) Gestion de la protection des données

(2) Gestion des réponses aux incidents

(3) Paramètres par défaut pour la protection des données (art. 25, al. 2 RGPD)

(4) Contrôle des commandes

Aucun traitement des données de commande au sens de l'art. 28 RGPD sans instructions correspondantes du donneur d'ordre, par exemple : conception claire du contrat, gestion formalisée des commandes, sélection stricte du prestataire de services, obligation de conviction préalable, contrôles de suivi.

	<b>Système de gestion de la protection des données</b> <b>Fairmas GmbH</b>	Auteur : S. Meyzis Date : 01.01.2023 Version : 06
---	---	---

## Annexe 2 – Sous-traitants

Conformément au point 6 (1) du contrat de traitement des commandes, le mandataire fournit une liste actuelle des sous-traitants sur demande ou à l'adresse Internet qui y est indiquée. La liste suivante n'est donc valable qu'au moment de la signature et sera remplacée par la version mise à jour.

Sous-traitant selon le point 6 du contrat de traitement des commandes entre le donneur d'ordre et le mandataire – État au **01.01.2023**

Société / Sous-traitant	Adresse / Pays	Prestations de service
Host Europe GmbH	Hansestr. 111 51149 Köln Allemagne	Fourniture, exploitation et maintenance de matériel informatique (serveur) et de lignes de données
<i>Responsable en Europe :</i> Microsoft Ireland Operations Ltd.	One Microsoft Way Redmond, Washington 98052 USA  Attn: Data Protection One Microsoft Place South County Business Park, Leopardstown Dublin 18, D18 P521 Irlande	Fourniture, exploitation et maintenance de matériel informatique (serveur) et de lignes de données, y compris la fourniture d'applications logicielles pour la préparation et la représentation de données ainsi qu'assistance et services de conseil
Sendinblue GmbH	Köpenicker Str. 126 10179 Berlin Allemagne	Transmission de messages système et de rapports aux utilisateurs de logiciels et destinataires enregistrés par e-mail ou SMS.
1&1 Internet SE	Elgendorfer Straße 57 56410 Montabaur Allemagne	Réception, stockage et transfert de données de gestion ainsi que transmission de messages système et de rapports aux utilisateurs de logiciels et destinataires enregistrés par e-mail ou SMS.