# Accord relatif au traitement des données conformément à l'art. 28 du Règlement général sur la protection des données (RGPD)

Entre

**NOM COMPLET DE LA SOCIÉTÉ**

et

**WEBFLEET SOLUTIONS B.V.**

## 1. Définitions

Le présent Accord de traitement des données (y compris les Annexes, « l'**ATD** ») est conclu entre Webfleet Solutions B.V. (« **Webfleet Solutions** ») et [INSÉRER LE NOM DE L'ENTREPRISE] (le « **Client** »).

Les termes définis dans le contrat de fourniture du Service et des Produits WEBFLEET conclu entre Webfleet Solutions et le Client (le « **Contrat** ») ont la même signification lorsqu'ils sont utilisés dans le présent ATD.

En outre, les définitions s'appliquent telles que définies dans le Règlement 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du Traitement des Données personnelles et à la libre circulation de ces données (Règlement général sur la protection des données ou « **RGPD** »).

## 2. Nature, objet et durée du présent ATD

Dans le cadre de la fourniture du Service et des Produits WEBFLEET au Client, Webfleet Solutions peut traiter les Données personnelles en tant que Sous-traitant pour le compte du Client agissant en tant que Responsable du traitement. Aux fins du présent ATD, le Client est désigné comme « **Responsable du traitement** » et Webfleet Solutions comme « **Sous-traitant de données** ».

L'objet du présent ATD est (i) de décrire les travaux à effectuer par le Sous-traitant de données dans le cadre du Contrat et (ii) d'inclure dans le présent ATD certaines stipulations requises en vertu du RGPD.

Le présent ATD s'applique à compter de la date de signature et reste en vigueur et de plein effet jusqu'à la résiliation du Contrat.

## 3. Portée des travaux

Pour le Responsable du traitement, le but de la collecte, du traitement et de l'utilisation des Données personnelles est de fournir le Service et les Produits WEBFLEET tels que décrits dans le Contrat, qui en fait partie intégrante. Le traitement et l'utilisation des Données personnelles ont lieu dans un État membre de l'Espace économique européen. Tout transfert de données vers un pays tiers est soumis à l'approbation écrite préalable du Responsable du traitement et, en l'absence de toute autre garantie appropriée conformément à l'Article 46 du RGPD, nécessite la conclusion des Clauses types figurant à l'Annexe 2 par les Parties conformément à l'Article 46, paragraphe 2, points (c) et (d) du RGPD.

Le traitement des Données personnelles par le Sous-traitant de données a lieu dans le cadre (i) du Contrat et (ii) du présent ATD et uniquement dans la mesure où le Responsable du traitement a donné instruction au Sous-traitant de le faire en relation avec le Contrat. Le Sous-traitant de données traite les Données personnelles au nom du Responsable du traitement. Les modifications apportées au traitement des Données personnelles dans le cadre de l'ATD sont soumises à une convention mutuelle. Le Sous-traitant de données n'utilisera pas les Données personnelles à d'autres fins que celles décrites dans le présent ATD et/ou dans toute autre condition applicable.

## 4. Transfert des pouvoirs

Le Responsable du traitement, représenté par le signataire comme indiqué sur le Contrat ou son Délégué à la protection des données, sert de point de contact unique pour le Sous-traitant de données aux fins du présent ATD. De même, le Sous-traitant de données a autorisé les personnes suivantes à agir en son nom :

- Délégué à la protection des données du Sous-traitant de données (privacy@webfleet.com)
- Équipe du support client du Sous-traitant de données

## 5. Types de données et catégories de personnes concernées

Le Responsable du traitement a défini que les **catégories de Données** personnelles suivantes seront recueillies, traitées et utilisées par le Sous-traitant de données en vertu du présent ATD :

☐ Données de communication (par exemple, les numéros de téléphone, adresses électroniques, adresses IP, positions GPS précises de la connexion, données sur l'utilisation et le trafic)

☐ Données du véhicule, notamment la plaque d'immatriculation, la distance parcourue, le temps de conduite, l'heure de la journée, la vitesse du véhicule et du moteur, la charge et la température du moteur, les manœuvres de freinage / de virage / d'accélération, la tension de la batterie, les protocoles de données sur les accidents (pendant 45 secondes avant et 15 secondes après un accident) ; données de diagnostic relatives à l'appareil, aux capteurs ou services du véhicule

☐ Données de planification et de contrôle

☐ Informations fournies par des tiers (par exemple, des agences de crédit ou des annuaires publics)

☐ Données spécifiques (informations sur la race et l'origine ethnique, les opinions politiques, les croyances religieuses ou philosophiques, l'appartenance à un syndicat, la santé ou la sexualité)

☐ Autre:

Le Responsable du traitement a défini les **catégories de personnes concernées** suivantes auprès desquelles les Données personnelles telles que définies ci-dessus seront recueillies, traitées et utilisées par le Sous-traitant de données en vertu du présent ATD :

☐ Clients

☐ Parties intéressées

☐ Abonnés

☐ Employés

☐ Fournisseurs

☐ Autre:

## 6. Obligations du Sous-traitant de données

En vertu du présent ATD, le Sous-traitant de données doit :

(i) traiter les Données personnelles uniquement au nom du Responsable du traitement et conformément à ses instructions ;
(ii) veiller à ce que seul un personnel dûment formé ait accès aux Données personnelles et soit tenu de les garder confidentielles ;
(iii) fournir au Responsable du traitement la coopération (y compris l'accès à ses installations) que celui-ci peut raisonnablement demander ;
(iv) mettre en œuvre les mesures techniques et organisationnelles de protection des Données personnelles requises par le RGPD ;
(v) informer immédiatement le Responsable du traitement de toute activité et mesure de surveillance prise par l'autorité compétente qui supervise la législation applicable en matière de protection des données ;
(vi) soutenir le Responsable du traitement en ce qui concerne ses obligations de fournir des informations sur la collecte, le traitement ou l'utilisation des Données personnelles d'une personne concernée ;
(vii) veiller à ce que les Données personnelles ne soient en aucun cas utilisées, manipulées, distribuées, copiées ou traitées à d'autres fins que l'exécution des obligations contractuelles expressément convenues dans le présent ATD et découlant de celui-ci ; et
(viii) assister le Responsable du traitement en cas de violation des données afin de lui permettre de signaler toute violation conformément à l'Article 28, paragraphe 3, point (f), et aux Articles 33 et 34 du RGPD.

## 7. Traitement secondaire des données

Le Sous-traitant de données engage des sous-traitants secondaires pour fournir certains services en son

nom. Le Responsable du traitement consent à ce que le Sous-traitant de données engage des sous-traitants secondaires pour traiter les Données personnelles dans le cadre du Contrat. Le Sous-traitant de données est responsable des actes, erreurs ou omissions des sous-traitants secondaires qui l'amènent à enfreindre l'une de ses obligations en vertu du présent ATD. Actuellement, le Sous-traitant de données a conclu des accords avec les sous-traitants secondaires suivants qui ont accepté de protéger les Données personnelles d'une manière durablement similaire aux normes énoncées dans le présent ATD :

| Société | Adresse / Pays | Services |
|---|---|---|
| TomTom International B.V. | De Ruijterkade 154<br>(1011 AC) Amsterdam<br>Pays-Bas | Le logiciel du système TomTom qui fournit des services en direct aux clients WEBFLEET, notamment des informations sur la circulation, des caméras de sécurité, des services de recherche locale et d'état des routes, des informations météorologiques et des prix du carburant. |
| Webfleet Solutions Development Germany GmbH | Inselstrasse 22, 04103<br>Leipzig, Allemagne | Traitement sécurisé des données basé sur les exigences des normes ISO/IEC 27001:2013, des données de l'ingénierie, du service informatique et des centres de données en liaison avec la plateforme de services Webfleet Solutions, que Webfleet Solutions Development Germany GmbH fournit à Webfleet Solutions B.V. et à ses clients<br><br>**Coordonnées**<br>M. Christian Volkmer<br>Projekt 29 GmbH & Co. KG<br>http://www.projekt29.com<br>Trothengasse 5, 93047 Regensburg, Allemagne<br>Tél. +49 (0) 941- 2986930, fax +49 (0) 941- 29869316,<br>privacy@webfleet.com |
| DAKO Systemtechnik und Service GmbH & Co. KG | Brusseler Str. 7-11, 07747<br>Jena, Allemagne | WEBFLEET Tachograph Manager |
| Google Dublin,<br>Google Ireland Ltd. | Gordon House<br>Barrow St.<br>Dublin 4, Irlande | Google Analytics Premium (conformément à la Politique de confidentialité Webfleet Solutions)<br>https://www.webfleet.com/fr_fr/webfleet/legal/privacy/<br><br>API Google Maps :<br>https://www.google.com/help/terms_maps.html |

Le Responsable du traitement consent par la présente à la mise en service des sous-traitants secondaires répertoriés ci-dessus.

Le Sous-traitant de données ne peut engager un nouveau sous-traitant secondaire ne figurant pas dans la section relative au Traitement secondaire des données qu'après (i) une autorisation spécifique ou générale du Responsable du traitement, et (ii) que le traitement secondaire repose sur un accord contractuel dans lequel sont imposées des obligations en matière de protection des données similaires à celles prévues dans le présent ATD.

Le transfert de Données personnelles du Responsable du traitement vers le sous-traitant secondaire et le début du traitement des données par le sous-traitant secondaire ne sont effectués qu'une fois que toutes les exigences ont été satisfaites. Si le sous-traitant secondaire fournit le service convenu en dehors de l'UE/EEE, le Sous-traitant de données doit veiller au respect de la Réglementation de l'UE en matière de protection des données par des mesures appropriées. Toute externalisation supplémentaire par le sous-traitant secondaire nécessite le consentement exprès du Responsable du traitement.

## 8. Droits et obligations du Responsable du traitement

**Droits de surveillance** : Le Responsable du traitement est autorisé à nommer un tiers auditeur indépendant possédant les qualifications professionnelles requises et lié par une obligation de confidentialité pour (i) inspecter le respect par le Sous-traitant de données du présent ATD, (ii) de la législation applicable en matière de protection des données, et (iii) pour vérifier la véracité et l'exhaustivité des déclarations soumises par le Sous-traitant de données en vertu du présent ATD. L'auditeur doit être raisonnablement acceptable pour le Sous-traitant de données. Le droit du Responsable du traitement de procéder à un audit est subordonné à la notification écrite au Sous-traitant de données au moins quatre (4) semaines à l'avance

dudit audit.

Le Sous-traitant de données doit traiter rapidement et correctement toutes les demandes du Responsable du traitement relatives à son traitement des Données personnelles soumises au présent ATD et appartenant aux personnes concernées.

**Rectification, suppression et blocage des données** : sur instruction du Responsable du traitement, le Sous-traitant de données rectifie, supprime ou bloque les Données personnelles.

Dans la mesure où la loi le permet, le Sous-traitant de données informe sans délai le Responsable du traitement lorsqu'il reçoit une demande d'une personne concernée qui souhaite exercer son droit d'accès, son droit de rectification, de limitation de traitement, d'effacement (« droit à l'oubli »), de portabilité des données, son droit de s'opposer au traitement ou son droit de ne pas faire l'objet d'une décision individuelle automatisée. Le Responsable du traitement assumera tous les coûts découlant de la fourniture de cette assistance par le Sous-traitant.

## 9. Obligations d'information

Si le Sous-traitant de données ne peut pas se conformer ou prévoit qu'il ne peut pas respecter ses obligations telles que définies dans le présent ATD, pour quelque raison que ce soit, celui-ci s'engage à informer rapidement le Responsable du traitement de son incapacité à se conformer, auquel cas le Responsable du traitement est en droit de suspendre le transfert de données.

Le Responsable du traitement informera rapidement le Responsable du traitement de :

(i) toute demande juridiquement contraignante de divulgation des Données personnelles par une autorité chargée de l'application de la loi, sauf interdiction contraire, telle que l'interdiction, en vertu du droit pénal, de préserver la confidentialité d'une enquête policière ;
(ii) tout accès accidentel, non autorisé ou tout autre événement constituant une violation des données personnelles ; et
(iii) toute demande reçue directement des personnes concernées sans répondre à cette demande, à moins qu'elle n'ait été autrement autorisée à le faire ; et
(iv) toute violation réelle ou présumée de la sécurité impliquant des Données personnelles en contactant le Responsable du traitement. En cas de violation de la sécurité, le Sous-traitant de données prend immédiatement toutes les mesures correctives appropriées et doit fournir rapidement au Responsable du traitement toutes les informations pertinentes et l'assistance demandée par ce dernier concernant la violation réelle ou présumée de la sécurité. La notification d'une violation de la sécurité des données au Responsable du traitement comprendra au minimum :
    a. une description de la violation de la sécurité, y compris la date et l'heure de sa découverte et (si possible) les catégories et le nombre approximatif de personnes concernées, ainsi que les catégories et le nombre approximatif d'enregistrements de données personnelles concernés ;
    b. des informations sur les conséquences (probables) de la violation de la sécurité ;
    c. une description des mesures prises par le Sous-traitant de données pour remédier à la violation de la sécurité, y compris, le cas échéant, des mesures visant à atténuer ses effets négatifs éventuels et à limiter les conséquences de la violation de la sécurité des données ; et
    d. le temps prévu pour résoudre la faille de sécurité.

## 10. Affectation

Le Sous-traitant de données ne doit pas céder le présent ATD sans le consentement écrit préalable du Responsable du traitement. Lorsque le Sous-traitant de données cède le présent ATD, avec le consentement du Responsable du traitement, il ne doit le faire qu'au moyen d'un accord écrit avec le cessionnaire, qui se verra imposer les mêmes obligations que celles qui sont imposées au Sous-traitant de données en vertu du présent ATD.

## 11. Conséquences de la résiliation

Les parties conviennent qu'à la résiliation des stipulations du Contrat, le Sous-traitant de données et le sous-

traitant secondaire doivent, au choix du Responsable du traitement, (i) restituer à ce dernier toutes les Données personnelles transférées, y compris tout support de stockage de données fourni au Sous-traitant et les copies de celles-ci, ou (ii) détruire toutes les Données personnelles et certifier au Responsable du traitement que celles-ci ont bien été détruites, à moins que la législation imposée au Sous-traitant de données ne l'empêche de restituer ou de détruire tout ou partie des Données personnelles transférées. Dans ce cas, le Sous-traitant de données confirme qu'il garantira la confidentialité des Données personnelles transférées et qu'il ne les traitera plus activement.

## 12. Confidentialité

Toute information de quelque nature que ce soit (technique, commerciale, financière, opérationnelle ou autre) et sous quelque forme que ce soit (orale, écrite, enregistrée ou autre), y compris les Données personnelles (ci-après dénommées, les « **Informations confidentielles** »), qui peut être divulguée sous quelque forme ou manière que ce soit par une partie à l'autre partie, dans le cadre ou à la suite du présent ATD, est considérée comme étant de nature confidentielle. Les Données relatives à la base de données, aux procédures et aux informations sur les clients du Responsable du traitement sont considérées comme des informations privées et confidentielles.

## 13. Autre

Le présent ATD s'applique en plus des conditions du Contrat. En cas de conflit entre le présent ATD et le Contrat, le présent ATD prévaudra.

Le présent ATD est exclusivement régi par la loi et la juridiction qui régissent le Contrat.

Si les Clauses contractuelles types (CCT) ont été exécutées parce que des données sont traitées en dehors de l'EEE, le Contrat est également complété par les clauses supplémentaires figurant à l'Annexe 2.

Les parties conviennent que le présent ATD ainsi que le Contrat constituent un contrat et/ou un autre acte juridique conformément à l'Article 28 du RGPD, qui lie le Sous-traitant de données à l'égard du Responsable du traitement et qui définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de Données personnelles et les catégories de personnes concernées ainsi que les obligations et les droits du Responsable du traitement.

CONVENU par les Parties, par l'intermédiaire de leurs représentants dûment autorisés, à la date à laquelle les deux parties ont signé le présent ATD.

Pour et au nom de :

| | |
|---|---|
| **Webfleet Solutions B.V.** | **Nom complet de la société** |
| _____ | _____ |
| Nom : | Nom : |
| Fonction: | Fonction: |
| Date : | Date : |

## Annexe 1 : Mesures techniques et opérationnelles

### 1. Introduction

La disponibilité de la plateforme de services Webfleet Solutions, y compris la meilleure protection possible des données des clients, est une priorité absolue et sous-tend toutes les relations commerciales fructueuses et à long terme. Par l'intermédiaire de notre société affiliée, Webfleet Solutions Development Germany GmbH en Allemagne, nous veillons à ce que la plateforme de services Webfleet Solutions respecte et dépasse les normes les plus récentes en matière de sécurité et de protection des données, y compris en matière de protection des données personnelles et confidentielles. Ces normes comprennent l'exploitation d'un système de gestion de la sécurité de l'information (SGSI) conformément à la norme ISO/IEC 27001:2013. Des investissements continus et complets dans des solutions matérielles et logicielles de pointe, la sécurité et la protection des données personnelles dès la conception, des technologies récentes et des processus, politiques et audits associés garantissent le respect et l'amélioration continue des mesures de protection.

Le Sous-traitant de données devra avoir nommé un délégué à la protection des données. Cette personne veille au respect de la réglementation et des autres lois et règlements mondiaux pertinents relatifs à la protection des données

**Contact pour la protection des données personnelles :**
Webfleet Solutions B.V.
Data Protection Officer
privacy@webfleet.com
De Ruijterkade 154
(1011 AC) Amsterdam
Pays-Bas

### 2. Présentation des mesures techniques et organisationnelles (MTO)

Le Sous-traitant de données doit mettre en œuvre et maintenir des mesures techniques et organisationnelles (MTO) conformément à l'Article 32 du RGPD comme indiqué ci-dessous et dans l'environnement client en ligne de la plateforme de services Webfleet Solutions afin d'assurer un niveau de sécurité approprié au risque pour le champ de responsabilité du Sous-traitant de données. Les MTO sont soumis à des progrès techniques et à des développements ultérieurs. En conséquence, le Sous-traitant se réserve le droit de modifier les MTO à condition que la fonctionnalité et la sécurité des Produits et du Service WEBFLEET ne soient pas dégradées.

## Confidentialité (art. 32, paragraphe 1, point (b) du RGPD)

### (i) Contrôle d'accès aux bâtiments / bureaux / centre de données

Le Sous-traitant de données a mis en œuvre les mesures suivantes, sans toutefois s'y limiter, pour empêcher l'accès non autorisé aux systèmes de traitement des données dans lesquels des données personnelles sont traitées :

- ☒ Système d'alarme
- ☒ Système de contrôle d'accès automatique
- ☒ Capteurs photoélectriques / détecteurs de mouvement
- ☒ Gestion des clés (délivrance des clés, etc.)
- ☒ Enregistrement des visiteurs
- ☒ Sélection rigoureuse des agents de sécurité
- ☒ Protection des fondations des installations
- ☒ Système de verrouillage par carte à puce / transpondeur
- ☒ Système de verrouillage manuel (utilisation limitée pour les salariés clés en cas de défaillance des systèmes de contrôle d'accès
- ☒ Surveillance vidéo aux points d'entrée (bureaux et centres de données)
- ☒ Serrures de sécurité
- ☒ Gestion des visiteurs aux bureaux d'accueil
- ☒ Sélection minutieuse du personnel de nettoyage
- ☒ Port visible des badges d'accès obligatoire
- ☒ Un contrôle d'accès séparé, spécifique et documenté des centres de données et des salles de serveurs est mis en place pour les personnes autorisées. L'accès des personnes autorisées est documenté à l'aide de leur nom et de leur numéro de carte ou de jeton. Pour les centres de données, des systèmes de contrôle d'accès distincts sont mis en place.

### (ii) Contrôle d'accès aux systèmes

Le Sous-traitant de données a mis en œuvre les mesures suivantes, sans toutefois s'y limiter, pour empêcher l'utilisation des systèmes de traitement des données par des personnes non autorisées :

- ☒ Attribution des droits d'utilisation
- ☒ Attribution des mots de passe
- ☒ Authentification par nom d'utilisateur / mot de passe
- ☒ Utilisation de systèmes de prévention des intrusions
- ☒ Utilisation de pare-feu matériels
- ☒ Création de profils d'utilisateurs
- ☒ Mesures supplémentaires : pare-feu pour les applications Web, analyses régulières de la vulnérabilité, tests de pénétration réguliers, gestion des correctifs, exigences minimales en matière de complexité des mots de passe et de changement forcé des mots de passe, utilisation de scanners de virus
- ☒ Affectation de profils d'utilisateurs aux systèmes informatiques
- ☒ Utilisation de la technologie VPN
- ☒ Chiffrement des supports de stockage mobiles
- ☒ Utilisation d'une administration centrale des smartphones (par exemple : effacement à distance des smartphones)
- ☒ Chiffrement des disques durs sur les ordinateurs portables
- ☒ Utilisation d'un pare-feu logiciel (clients de bureau)

### (iii) Contrôle d'accès aux données

Le Sous-traitant de données a mis en œuvre les mesures suivantes, sans toutefois s'y limiter, afin (i) de garantir que les utilisateurs autorisés d'un système de traitement des données ne puissent accéder qu'aux données pour lesquelles ils sont autorisés, et (ii) d'empêcher que les données personnelles soient lues sans autorisation pendant que les données sont utilisées, en mouvement ou au repos :

- ☒ Création d'un concept d'autorisation
- ☒ Nombre d'administrateurs réduit au « strict
- ☒ Chiffrement des disques (bandes de sauvegarde pour le stockage hors site ou les ordinateurs portables)

nécessaire »
☒ Enregistrement de l'accès aux applications, notamment lors de la saisie, de la modification et de la suppression des données
☒ Nettoyage sécurisé des supports avant leur réutilisation
☒ Utilisation de broyeurs ou de services de destruction de documents (si possible avec un sceau de confidentialité)

☒ Gestion des droits par les administrateurs de système
☒ Politique en matière de mots de passe, y compris la longueur des mots de passe, la gestion des changements de mots de passe
☒ Stockage sécurisé des supports de données
☒ Enregistrement de la destruction de supports sécurisés
☒ Destruction conforme des supports de données (DIN 66399)

### (iv) Traitement séparé des données

Le Sous-traitant de données a mis en œuvre, entre autres, les mesures suivantes, afin de garantir que les données recueillies pour différentes finalités puissent être traitées séparément :

☒ Création d'un concept d'autorisation
☒ Fourniture d'enregistrements avec des attributs de finalité / des champs de données
☒ Droits sur les bases de données approuvés et documentés

☒ Séparation logique des clients (dans les logiciels)
☒ Pour les données pseudonymes : la séparation du fichier de mappage et le stockage sur un système informatique sécurisé distinct
☒ Séparation de la production et des systèmes d'essai

## Intégrité (art. 32, paragraphe 1, point (b) du RGPD)

### (v) Contrôle du transfert des données

Le Sous-traitant de données a mis en œuvre les mesures suivantes, sans toutefois s'y limiter, pour garantir que les données personnelles ne puissent être lues, copiées ou modifiées pendant la transmission électronique ou pendant le transport ou le stockage sur disque. Ces mesures sont également mises en œuvre pour contrôler et déterminer à quels organismes le transfert de données personnelles fournies par des équipements de communication de données est autorisé :

☒ Création de lignes spécialisées ou de tunnels VPN
☒ Documentation sur les destinataires des données et les délais de fourniture des données, y compris les délais d'effacement convenus
☒ Pour le transport physique, sélection minutieuse du personnel et des véhicules de transport (stockage hors site sur bande)
☒ Chiffrement des disques (bandes de sauvegarde pour le stockage hors site)

☒ Divulgation de données sous forme anonyme ou pseudonyme
☒ Création d'une vue d'ensemble des opérations régulières de demande et de livraison
☒ Pour le transport physique, conteneurs de transport / emballage sécurisés (stockage hors site sur bande)
☒ Chiffrement TLS de toutes les communications (client Web, API, applications mobiles)

### (vi) Contrôle de la saisie des données

Le Sous-traitant de données a mis en œuvre les mesures suivantes, sans toutefois s'y limiter, pour garantir qu'il est possible de contrôler et de déterminer ultérieurement si des données personnelles ont été introduites, modifiées ou supprimées dans les systèmes de traitement des données, et par qui :

☒ Enregistrement de l'introduction, de la modification et de la suppression des données
☒ Traçabilité de la saisie, de la modification et de la suppression des données par des noms d'utilisateurs individuels (et non par des groupes d'utilisateurs)
☒ Octroi de droits pour la saisie, la modification ou la

☒ Création d'un aperçu des applications autorisées à saisir, modifier ou supprimer des données
☒ Stockage des formulaires, par lesquels les données ont été acquises lors du traitement automatisé

suppression de données sur la base d'un concept d'autorisation

## Disponibilité et résilience (art. 32, paragraphe 1, point (b) du RGPD)

### (vii) Contrôle de la disponibilité

Le Sous-traitant de données a mis en œuvre les mesures suivantes, sans toutefois s'y limiter, pour garantir la protection des données personnelles contre la destruction ou la perte accidentelle :

- ☒ Alimentation sans coupure (UPS)
- ☒ Appareils de contrôle de la température et de l'humidité dans les salles de serveurs
- ☒ Systèmes de détection d'incendie et de fumée
- ☒ Alarme en cas de détection d'une entrée non autorisée dans les salles de serveurs
- ☒ Test de récupération des données
- ☒ Stockage hors site sécurisé des sauvegardes de données
- ☒ Dans les zones inondables : les salles de serveurs doivent se trouver au-dessus du niveau inondable
- ☒ Climatisation des salles de serveurs
- ☒ Blocs d'alimentation de protection dans les salles de serveurs
- ☒ Extincteurs dans les salles de serveurs
- ☒ Création d'un concept de sauvegarde et de récupération
- ☒ Préparation d'un plan d'intervention d'urgence
- ☒ Salles de serveurs positionnées ailleurs que sous les installations sanitaires
- ☒ Deux centres de données en Allemagne dans une configuration active/active pour garantir la résilience

## Processus d'examen, d'analyse et d'évaluation réguliers (art. 32, paragraphe 1, point (d), art. 25, paragraphe 1 du RGPD)

### (viii) Contrôle des commandes

Le Sous-traitant de données a mis en œuvre les mesures suivantes, sans toutefois s'y limiter, afin de garantir que les données personnelles traitées pour le compte d'un Responsable du traitement ne soient traitées que selon les instructions de ce dernier :

- ☒ Sélection des fournisseurs après vérification des antécédents (en particulier la sécurité des données)
- ☒ Instructions écrites à l'attention du fournisseur (par exemple, via un ATD) (RGPD)
- ☒ Dans la mesure nécessaire : s'assurer que les fournisseurs ont désigné des Délégués à la protection des données
- ☒ Des droits de contrôle effectifs sur les sous-traitants
- ☒ Examen préalable de la documentation et des mesures de sécurité prises par le fournisseur
- ☒ Obligation des salariés du fournisseur de maintenir la confidentialité des données (RGPD)
- ☒ Assurer la destruction sécurisée des données après la résiliation du contrat
- ☒ Examen continu des fournisseurs et de leurs activités
- ☒ Gestion de la réponse aux incidents

| | |
|---|---|
| de données ont été convenus | |
| ☒ Gestion de la protection des données (ISMS) | ☒ Protection des données dès la conception et protection des données par défaut (art. 25, paragraphe 2 du RGPD) |

Le Responsable du traitement confirme, en signant l'ATD, qu'il a eu la possibilité raisonnable de prendre connaissance des MTO telles qu'elles figurent dans le présent document et confirme que ces MTO offrent un niveau de protection approprié des Données personnelles du Client compte tenu des risques associés au Traitement de ces données.