**ACCORD DE TRAITEMENT DE DONNEES**

**ENTRE**

**Opinum SA**, société de droit belge, immatriculée sous le numéro 0561.807.172, dont le siège social est situé rue Emile Francqui 9 à 1435 Mont-Saint-Guibert, Belgique. (**Sous-traitant)**

agissant en qualité de sous-traitant

**ET**

**Client**, toute société et entité juridique, personne physique ou morale agissant en son nom, à titre non privé, autrement qu'à titre privé (B2B), qui s'est inscrite pour l'utilisation des services conformément aux conditions de vente, chaque **Partie** et collectivement les **Parties.**

**Le présent DPA fait partie intégrante des conditions de vente d'Opinum. L'adhésion à ces conditions implique donc l'acceptation par le client des dispositions suivantes relatives au traitement des données à caractère personnel.**

**CONDITIONS CONVENUES**

# Definitions and Interpretation

The following definitions and rules of interpretation apply in this DPA.

## Definitions:

**Finalités commerciales:** les services décrits dans le contrat-cadre et/ou toute autre finalité spécifiquement identifiée à l'annexe A.

**Législation sur la protection des données désigne** le GDPR et la législation de mise en œuvre applicable en vertu du droit belge.

**GDPR** désigne le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

**Contrôleur, analyse d'impact de la protection des données, personne concernée, données à caractère personnel, violation de données à caractère personnel, traitement et sous-traitant** ont la même signification que dans le GDPR.

## Le présent DPA est soumis aux dispositions de l'accord-cadre et y est intégré.

## En cas de conflit ou d'ambiguïté entre:

### toute disposition contenue dans le corps du présent DPA et toute disposition contenue dans les annexes, la disposition contenue dans le corps du présent DPA prévaudra ; et

### toute disposition du présent DPA et les dispositions de l'accord-cadre, les dispositions du présent DPA prévalent.

# Types de données à caractère personnel et finalités du traitement

## Le Responsable du traitement conserve le contrôle des Données à caractère personnel et reste responsable de ses obligations de conformité en vertu de la Législation sur la protection des données applicable, y compris la fourniture de tous les avis requis et l'obtention de tous les consentements requis, ainsi que des instructions de traitement qu'il donne au Sous-traitant. Le Responsable du traitement informe le Sous-traitant de toute législation nationale et/ou sectorielle supplémentaire obligatoire qui s'applique au traitement par le Sous-traitant à la suite du traitement par le Responsable du traitement.

## L'Annexe A décrit la nature et la finalité du traitement, la (les) durée(s) de conservation et les catégories de données à caractère personnel et les types de personnes concernées que le sous-traitant peut traiter pour atteindre les finalités de l'entreprise.

# Obligations du sous-traitant

## Le sous-traitant ne traitera les données personnelles que dans la mesure et de la manière nécessaires aux fins commerciales, conformément aux instructions écrites du contrôleur. Le sous-traitant ne traitera pas les données personnelles à d'autres fins ou d'une manière qui n'est pas conforme au présent DPA ou à la législation sur la protection des données. Le sous-traitant doit informer rapidement le contrôleur si, à son avis, les instructions du contrôleur ne sont pas conformes à la législation sur la protection des données.

## Le sous-traitant maintiendra la confidentialité de toutes les données personnelles et ne divulguera pas les données personnelles à des tiers, sauf si le contrôleur ou le présent DPA autorise spécifiquement la divulgation, ou si la loi l'exige. Si une loi, un tribunal, un régulateur ou une autorité de surveillance exige que le sous-traitant traite ou divulgue des données personnelles, le sous-traitant doit d'abord informer le contrôleur de l'exigence légale ou réglementaire et donner au contrôleur la possibilité de s'opposer ou de contester l'exigence, à moins que la loi n'interdise une telle notification.

## Le sous-traitant aidera raisonnablement le contrôleur à respecter les obligations de conformité du contrôleur en vertu de la législation sur la protection des données, en tenant compte de la nature du traitement du sous-traitant et des informations dont il dispose, y compris en ce qui concerne les droits des personnes concernées, les évaluations de l'impact sur la protection des données et les rapports et consultations avec les autorités de contrôle en vertu de la législation sur la protection des données.

# Employés du sous-traitant

## Le sous-traitant s'assurera que tous les employés:

### soient informés de la nature confidentielle des données personnelles et soient liés par des obligations de confidentialité et des restrictions d'utilisation en ce qui concerne les données personnelles; et

### soient conscients des devoirs du sous-traitant et de leurs devoirs et obligations personnels en vertu de la législation sur la protection des données et du présent DPA.

# Sécurité

## Le sous-traitant doit mettre en œuvre les mesures techniques et organisationnelles appropriées contre le traitement, l'accès, la divulgation, la copie, la modification, le stockage, la reproduction, l'affichage ou la distribution non autorisés ou illégaux des données à caractère personnel, et contre la perte, la destruction, l'altération, la divulgation ou l'endommagement accidentels ou illégaux des données à caractère personnel, comme décrit plus en détail à l'annexe B.

## Le sous-traitant doit mettre en œuvre les mesures nécessaires pour assurer un niveau de sécurité approprié au risque encouru, y compris, le cas échéant :

### la pseudonymisation et le cryptage des données personnelles ;

### la capacité à assurer la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement ;

### la capacité de rétablir la disponibilité et l'accès aux données à caractère personnel en temps utile en cas d'incident physique ou technique ; et

### un processus permettant de tester, d'apprécier et d'évaluer régulièrement l'efficacité des mesures de sécurité.

# Violation de données à caractère personnel

## Le sous-traitant notifie par écrit au Contrôleur, sans retard injustifié et en tout état de cause dans les 24 heures, s'il a connaissance d'une violation de données à caractère personnel.

## Lorsque le sous-traitant a connaissance d'une violation de données à caractère personnel, il fournit également par écrit au responsable du traitement, dans les meilleurs délais, les informations suivantes :

### la description de la nature de la violation, y compris les catégories et le nombre approximatif de personnes concernées et de données à caractère personnel concernés ;

### les conséquences probables ; et

### la description des mesures prises ou proposées pour remédier à la violation de données à caractère personnel, y compris les mesures visant à en atténuer les effets négatifs éventuels.

## Immédiatement après une violation de données à caractère personnel, les Parties se coordonnent pour enquêter sur la question. Le sous-traitant coopérera raisonnablement avec le Contrôleur dans le traitement de l'affaire par le Contrôleur, y compris :

### en participant à toute enquête ;

### en prenant des mesures raisonnables et rapides pour atténuer les effets et minimiser tout dommage résultant de la violation de données à caractère personnel.

## Le sous-traitant n'informera aucun tiers d'une violation de données à caractère personnel sans avoir obtenu au préalable le consentement écrit du responsable du traitement, sauf si la loi l'exige.

# Transferts transfrontaliers de données à caractère personnel

## Le sous-traitant (ou tout Sous-Traitant) ne doit pas transférer ou traiter autrement les Données Personnelles en dehors de l'Espace Economique Européen (EEE) sans obtenir le consentement écrit préalable du Contrôleur.

## Ce consentement du contrôleur n'est pas nécessaire lorsque le transfert de données personnelles vers des pays situés en dehors de l'EEE est obligatoire en vertu des dispositions de l'UE ou d'un État membre de l'UE.

# Tiers

## Le Processeur ne peut autoriser un tiers (Tiers) à traiter les Données Personnelles que si :

### le contrôleur a la possibilité de s'opposer à la nomination de chaque tiers ultérieur dans un délai de 14 jours après que le sous-traitant a notifié par écrit au contrôleur son intention de nommer un tel tier ultérieur, étant entendu que le contrôleur ne peut s'opposer à une telle nomination que par écrit et sur la base de motifs raisonnables et prouvés ; et

### le sous-traitant conclut un contrat écrit avec le tiers ultérieur qui contient des conditions essentiellement identiques à celles énoncées dans le présent DPA, notamment en ce qui concerne l'obligation de prendre des mesures techniques et organisationnelles appropriées en matière de sécurité des données, et, sur demande écrite du responsable du traitement, fournit au responsable du traitement des copies de ces contrats.

## Les Tiers approuvés au début du présent DPA sont indiqués à l'Annexe A. Le Sous-traitant doit dresser la liste de tous les Tiers approuvés à l'Annexe A et inclure le nom de tout Tiers, son emplacement et les coordonnées de la personne responsable de la conformité en matière de protection des données.

## Sans préjudice de la clause 13.1, le sous-traitant reste entièrement responsable vis-à-vis du contrôleur de tout manquement d'un tiers à ses obligations en matière de traitement des données à caractère personnel.

# Plaintes, demandes des personnes concernées et droits des tiers

## Le sous-traitant doit prendre les mesures techniques et organisationnelles convenues par écrit entre les parties et fournir rapidement au responsable du traitement les informations que ce dernier peut raisonnablement exiger, afin de permettre au responsable du traitement de se conformer avec:

### les droits des personnes concernées en vertu de la législation sur la protection des données, y compris les droits d'accès des personnes concernées, les droits de rectification et d'effacement des données personnelles, les droits d'opposition au traitement et au traitement automatisé des données personnelles, et les droits de restriction du traitement des données personnelles ; et

### les avis d'information ou d'évaluation signifiés au responsable du traitement par toute autorité de contrôle en vertu de la législation sur la protection des données.

## Le sous-traitant doit informer le contrôleur immédiatement s'il reçoit une plainte, un avis ou une communication qui se rapporte directement ou indirectement au traitement des données personnelles ou au respect de la législation sur la protection des données par l'une ou l'autre des parties.

## Le Processeur doit notifier le Contrôleur dans les 5 jours ouvrables s'il reçoit une demande d'une Personne concernée pour accéder à ses Données personnelles ou pour exercer l'un de ses droits connexes en vertu de la Législation sur la protection des données.

## Le sous-traitant coopérera raisonnablement avec le contrôleur et l'aidera à répondre à toute plainte, avis, communication ou demande de la personne concernée.

## Le sous-traitant ne doit pas divulguer les données personnelles à une personne concernée ou à un tiers, sauf à la demande ou selon les instructions du contrôleur, comme le prévoit le présent DPA ou comme l'exige la loi.

# Durée et résiliation

## Le présent DPA restera pleinement en vigueur tant que :

### l'accord-cadre reste en vigueur ; ou

### le sous-traitant conserve en sa possession ou sous son contrôle des données à caractère personnel liées à l'accord-cadre (durée).

## Toute disposition du présent DPA qui, expressément ou implicitement, devrait entrer ou rester en vigueur à la fin ou après la fin de l'accord-cadre (y compris, mais sans s'y limiter, la clause 13.1) restera pleinement en vigueur.

# Retour et destruction des données

## En cas de résiliation de l'accord-cadre pour quelque raison que ce soit ou d'expiration de sa durée, le sous-traitant supprimera ou détruira en toute sécurité ou, si le contrôleur le lui demande par écrit, retournera et ne conservera pas toutes les données personnelles liées à ce DPA en sa possession ou sous son contrôle.

## Si une loi, un règlement ou un organisme gouvernemental ou réglementaire exige que le sous-traitant conserve des documents ou du matériel qu'il serait autrement tenu de renvoyer ou de détruire, il notifiera par écrit au contrôleur cette exigence de conservation, en donnant des détails sur les documents ou le matériel qu'il doit conserver, la base juridique de la conservation, et en établissant un calendrier spécifique pour la destruction une fois que l'exigence de conservation prend fin.

## Le sous-traitant certifiera par écrit qu'il a détruit les données personnelles dans les 14 jours suivant l'achèvement de la destruction.

# Audit

## Le sous-traitant met à la disposition du contrôleur toutes les informations nécessaires pour démontrer le respect des obligations en vertu du présent DPA et de la législation sur la protection des données et permet au contrôleur et à ses auditeurs autorisés d'effectuer des audits concernant le respect par le sous-traitant de ses obligations en vertu du présent DPA et de la législation sur la protection des données.

## Un tel audit ne peut avoir lieu plus d'une fois par année contractuelle, est aux frais exclusifs du contrôleur et est soumis à la condition que le contrôleur fournisse au sous-traitant un préavis écrit d'au moins trente (30) jours de son intention d'effectuer un audit. L'audit a lieu pendant les heures normales d'ouverture et n'interfère pas de manière déraisonnable avec les activités commerciales du sous-traitant. Le sous-traitant a le droit d'exiger du contrôleur et de tout auditeur tiers qu'ils concluent un accord de non-divulgation avant de procéder à l'audit.

# Divers

## Dans la mesure où le droit applicable le permet, toutes les limitations et/ou exclusions de responsabilité prévues dans l'accord-cadre s'appliquent au présent DPA.

## Si, à tout moment pendant la durée du contrat, l'une des dispositions du présent DPA est jugée invalide, illégale ou inapplicable, la validité, la légalité et l'applicabilité des autres dispositions du DPA ne sont en aucun cas affectées ou compromises. Les parties négocient de bonne foi le remplacement de la disposition invalide, illégale ou inapplicable par une disposition valide, légale et applicable dont l'effet se rapproche le plus possible de celui de la disposition invalide, illégale ou inapplicable.

## Le présent DPA est régi et interprété conformément aux lois applicables à l'accord-cadre. Le même tribunal que celui indiqué dans l'accord-cadre aura une compétence exclusive pour tout litige découlant du présent DPA ou en rapport avec celui-ci.

**Annexes:**

- ANNEXE A Description du traitement et coordonnées

- ANNEXE B Mesures techniques et organisationnelles

**ANNEXE A Description du traitement et coordonnées**

**Autres Finalités commerciales et instructions spécifiques concernant le traitement**

**Nature du traitement**

|  |  |
| --- | --- |
| collecte  enregistrement  organisation  structuration  conservation  adaptation ou modification  extraction  consultation | utilisation  communication par transmission, diffusion ou toute autre forme de mise à disposition  rapprochement ou interconnexion  limitation, effacement ou destruction de données (à l’aide de procédés automatisés ou non)  autre (veuillez préciser) : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Catégories de Personnes concernées**

|  |  |
| --- | --- |
| Employés et/ou consultants du Sous-traitant  Clients du Responsable du traitement des données  Utilisateurs du service/du site web/de l’application suivant(e) :  \_\_\_Data Hub Opinum\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Autre (veuillez préciser) : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Catégories de Données à caractère personnel**

|  |  |
| --- | --- |
| Données d’identification personnelle (*nom, adresse, numéro de téléphone, etc*.)  Données d’identification électronique (*adresse* *IP, adresse MAC, cookies, etc*.)  Données financières (*numéros de compte bancaire, assurance, salaire, etc.*)  Caractéristiques personnelles (*âge, sexe, date de naissance, lieu de naissance, citoyenneté, visas, etc*.)  Données psychologiques (*opinions sur la personnalité, etc*.)  Famille (*situation matrimoniale, cohabitation, nom du conjoint/partenaire, des enfants, parents, etc*.)  Affiliations (*affiliations à des organisations professionnelles et non professionnelles, clubs, groupes, associations, etc*.)  Données judiciaires (*données concernant des condamnations et des infractions, des suspicions, des mises en accusation et des sanctions administratives*) | Caractéristiques du logement (*adresse, type d’habitation, durée de séjour, etc*.)  Données concernant la santé (*santé physique, santé mentale, données génétiques, traitements, prescriptions, etc.*)  Éducation (*curriculum, financement des études, qualifications, expérience professionnelle, publications, etc*.)  Profession et emploi (*emploi actuel, description du travail, données de candidature, carrière, salaire, données concernant l’équipement informatique, mots de passe et codes, etc*.)  Photos ou vidéos  Autre (veuillez préciser) : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**Durée de conservation**

Pendant la Durée d’application

Durées de conservation spécifiques (veuillez préciser) : \_\_\_\_\_\_\_.

Data Protection Officer OPINUM : dpo**AT**opinum.com

**Liste de Sous-traitants ultérieurs pour l’environnement UAT (environnement Saas Opinum)**

|  |  |  |
| --- | --- | --- |
| **Dénomination sociale** | **Lieu du traitement** | **Nature de la sous-traitance ultérieure** |
| Altova | BE | MapForce transforme les fichiers de données dans le format standard d'Opinum |
| Aspose Pty Ltd | BE | Génére les rapports contenant des données clients, à la demande des clients en Excel ou PS. |
| Exavault | US | FTP dans lequel les clients peuvent déposer leurs fichiers de données pour les injecter dans Data Hub. |
| Microsoft Ireland Operations Limited | UE | Hébergeur de toutes la solution Data Hub en mode Saas + BDD des utilisateurs |
| MongoDB Cloud | UE | Base de donnée dans laquelle sont stockes les metadonnées de sites et sources. |
| Claranet | FR | Maintenance des bases de données Cassandra |
| Plivo Inc. | US | Outils d'envoi de SMS |
| Schneider electric industries sas | FR | Algorythme |
| SendGrid | US | Plateforme d'envoi d'email |
| Splunk | US | Outil de logs centralisés |
| Paddle | UK | Outils analytiques |
| Greymatter | US | Fournit les licences Microsoft Bing qui nous permet de convertir les adresses des sites fournies par les clients en geopoints affichable sur des cartes. |
| HATCH Group | BE | Affichage des données |

**Liste de Sous-traitants ultérieurs pour l’environnement PROD (environnement cloud souverain français)**

|  |  |  |
| --- | --- | --- |
| **Dénomination sociale** | **Lieu du traitement** | **Nature de la sous-traitance ultérieure** |
| Aspose Pty Ltd | BE | Génére les rapports contenant des données clients, à la demande des clients en Excel ou PS. |
| Agora Calysé | FR | Hébergeur de l’environnement cloud souverain français et fournisseur du FTP. |
| Claranet | FR | Gestionnaire des bases de données Cassandra |
| Mailjet | FR | Plateforme d'envoi d'email |
| Graylog | UE | Outil de logs centralisés |
| Paddle | UK | Outils analytiques |
| Greymatter | US | Fournit les licences Microsoft Bing qui nous permet de convertir les adresses des sites fournies par les clients en geopoints affichables sur des cartes. |
| HATCH Group | BE | Affichage des données |

**ANNEXE B Mesures techniques et organisationnelles**

## Mesures Organisationnelles

* ***Sécurisation physique des bâtiments (alarme, badge d’accès, caméras)***
* ***Les ordinateurs des employés sont protégés par un mot de passe et tous les ordinateurs des employés sont équipés d'un logiciel antivirus.***
* ***Désignation d’un DPO (DPD) et d’un CISO (RSSI)***
* ***Politique de sécurité de l’information***
* ***Politique interne de respect du RGPD***
* ***Clauses de confidentialité contractuelles***
* ***Sensibilisation à la protection des données et à la sécurité de l’information***
* ***Contrat de traitement de données avec les sous-traitants***
* ***Journalisation (logs)***

## Mesures techniques

**API (Opinum)**

L’accès à l’API REST est sécurisé par authentification. Pour se connecter à l’API REST, une paire client ID /secret unique doivent être demandée puis générée par Opinum. Ces informations d’autorisation donnent uniquement le droit d’accéder à l’API REST.

Un utilisateur doit encore s’authentifier avant de pouvoir accéder exclusivement au compte auquel il est lié.

**STORAGE (Opinum)**

Les fichiers téléchargés directement dans le Storage de Opinum Data Hub sont sécurisés de fait par la connexion HTTPS. Plus de détails dans le chapitre [Accès aux données](bookmark://_Acc%C3%A8s_aux_donn%C3%A9es/).

**CHIFFREMENT DES DONNEES**

Toutes les données sont chiffrées entre la plateforme et le navigateur.

**STOCKAGE DES DONNEES**

Opinum utilise plusieurs types de base de données, qui ont toutes un haut niveau de sécurité et de disponibilité.

* **Stockage des données** 
  + **Environnement Saas Opinum**

Opinum utilise le centre de données Microsoft appelé Europe de l'Ouest, basé aux Pays-Bas.

Microsoft™ Azure s’exécute dans des centres de données gérés et exploités par Microsoft™. Ces centres de données répartis à divers endroits sont conformes aux principales normes du secteur relatives à la sécurité et à la fiabilité, telles que ISO/IEC 27001:2013 et NIST SP 800-53.

Les bases de données SQL de Microsoft™ Azure créent automatiquement des sauvegardes de base de données qui sont conservées 35 jours et utilisent le stockage géo-redondant à accès en lecture Azure (RA-GRS) pour assurer leur préservation même si le centre de données est indisponible.

* + **Environnement cloud souverain français (PROD)**

Opinum utilise l’hébergeur Agora Calysé qui est certifié selon les référentiels de Sécurité ISO 27001v.2013et HDSv.2018.

La sauvegarde des données est quotidienne avec une rétention de 30 jours et une sauvegarde redondante est effectuée sur un Datacenter distant.

​**GESTION DES UTILISATEURS**

* ***Accès des utilisateurs***

Chaque utilisateur du Opinum Data Hub a un accès strict au compte dont il fait partie. Chaque utilisateur est identifié par un identifiant unique, son adresse email. Chaque adresse email, et donc chaque utilisateur, ne peut avoir accès qu’à un seul compte. Il n’est pas possible pour un utilisateur de se connecter à un autre compte.

Chaque utilisateur a des permissions sur des sites et des sources selon son rôle.

Les utilisateurs de rôle Manager ont accès à tous les sites et à toutes les sources de leur compte.

Les utilisateurs de rôle Utilisateur ont uniquement accès aux sites et aux sources pour lesquels une permission leur a été donnée. Ces permissions sont définies par un utilisateur de ce compte avec le rôle de Manager. En aucun cas un utilisateur ne peut accéder aux données d’un site ou d’une source auxquels il n’a pas de permission.

* ***Authentification des utilisateurs***

Opinum utilise les standards d’authentification Oauth v2, JWS (JSON Web Signature) et Open ID Connect.

Seul un hash des mots de passe est stocké. Opinum n’a aucun moyen d’avoir accès aux mots de passe décryptés.

* ***Gestion des sessions***

Chaque session par utilisateur est limitée à une heure. Au bout d’une heure l’utilisateur est déconnecté et doit se reconnecter.

**AUTRES MESURES**

* ***Anti-virus et malware***
* ***Firewalls***
* ***Ségrégation des réseaux***
* ***Sécurisation des accès distants***
* ***Protocole de tests***

Chaque année Opinum fait réaliser un test de pénétration par un organisme indépendant et certifié.  Les résultats du dernier test de pénétration sont disponibles sur demande par email à [support@opinum.com](mailto:support@opinum.com).

Opinum Data Hub et ses points d’entrée sont éprouvés :

* https://identity.opinum.com
* https://datahub.opinum.com
* https://api.opinum.com
* https://push.opinum.com
* FTP

La méthodologie utilisée couvre les normes de l’industrie :

Le Technical Guide to Information Security Testing and Assessment (SP 800-115) produit par le NIST (National Institute of Standards and Technology)

Le standard PTES (Penetration Testing Execution Standard), créé par des professionnels de la sécurité pour fournir un cadre détaillé à la réalisation des tests de pénétration.

Les éléments clés du guide de tests Open Web Application Security Project (OWASP).