Accord de sous-traitance

LES PARTIES :

1. Vous, en tant que client, dénommé ci-après **« Responsable du traitement »** ;
   et

2. la société privée à responsabilité limitée **Fairtual Technologies BV** ayant son siège statutaire en Belgique, 8000 Bruges, Koningin Elisabethlaan 18 et dont les bureaux sont sis en Belgique, 8000 Bruges, Koningin Elisabethlaan 18, représentée par son dirigeant, monsieur Diego Dupont, dénommé ci-après le **« Sous-traitant »**.

CONSIDÉRATIONS :

I. Le Responsable du traitement passe ou passera un ou plusieurs accords avec le Sous-traitant, en vue de la livraison de divers services par le Sous-traitant au Responsable du traitement. Cet accord ou ces accords sont communs ou seront désignés comme **« l'Accord principal ».**

II. Le sous-traitant, à l'exécution de l'Accord principal traitera les données pour lesquelles le Responsable du traitement est et demeure responsable. Ces données font partie des données personnelles dans le sens du Règlement général européen sur la protection des données (UE 2016/679), autrement nommé le **« RGPD »**.

III. Les parties décident, étant données les dispositions de **l'article 28 paragraphe 3 du RGPD** d'enregistrer les conditions de traitement de ces données personnelles dans cet accord.

ACCORD :

1 Domaine d'application

1.1 Cet accord s'applique, dans la mesure où la prestation des services se conforme à l'Accord principal, et où un ou plusieurs traitements se produisent tels que présentés à **l'Annexe 1**

1.2 Les traitements de **l'Annexe 1** qui se déroulent lors de la prestation des services seront ci-après nommés **« les Traitements »**. Les données personnelles qui sont traitées par la présente : **« les Données personnelles »**.

1.3 Concernant le Traitement, le Responsable du traitement est le responsable du traitement et le Sous-traitant est le sous-traitant. Les personnes physiques qui, conformément à l'Accord principal, utilisent de fait les services du Sous-traitant et, éventuellement, de leurs représentants, sont ci-après dénommées les **« Utilisateurs finaux »**.

1.4 Toutes les notions clés de cet accord revêtent le sens qui leur sont donnés dans le RGPD.

1.5 Les annexes font partie du présent accord. Cela concerne :

Annexe 1 les Traitements, les Données personnelles et les délais de conservation ;

Annexe 2 les Sous-traitants ultérieurs et les catégories de Sous-traitants ultérieurs que ce Responsable du traitement approuve ;

Annexe 3 les mesures techniques et organisationnelles du Sous-traitant ;

Annexe 4 informations concernant une Fuite de données.

2 Objet

2.1 Le Sous-traitant s'engage à traiter les Données personnelles exclusivement dans la portée des activités désignées par cet accord de sous-traitance et/ou cet Accord principal. Le Sous-traitant garantit qu'il (ou elle) n'utilisera en aucun cas les Données personnelles Traitées conformément à cet Accord de sous-traitance, sans l'autorisation expresse écrite du Responsable du traitement, à ses propres fins ou aux fins de tiers, à moins qu'une disposition légale applicable au Sous-traitant l'y oblige. Dans ce cas, le Sous-traitant notifiera immédiatement le Responsable du traitement, préalablement au Traitement, de cette prescription légale, à moins que cette législation n'interdise cette notification pour des motifs justes d'intérêt public.

2.2 Le Sous-traitant tiendra séparées les Données personnelles du Responsable du traitement, des Données (personnelles) Traitées individuellement ou pour des tiers.

2.3 Le Sous-traitant réalise les Traitements de manière juste et attentive.

3 Mesures de sécurité

3.1 Le sous-traitant prend toutes les mesures de sécurité techniques et organisationnelles qui sont exigées de ce dernier sur la base du RGPD et en particulier de **l'article 32 du RGPD**.

3.2 Le Sous-traitant délivrera un document où figurent les mesures adaptées techniques et organisationnelles. Ce document sera joint en tant **qu'Annexe 3** à cet Accord de sous-traitance.

4 Fuites de données

4.1 Le Sous-traitant informera le Responsable du traitement sans délai irraisonné, mais en tous les cas sous 24 heures, de toute « violation de données à caractère personnel » comme repris à **l'article 4 paragraphe 12 du RGPD**. Une telle infraction sera par la suite : nommée **« Fuite de données »**.

4.2 Le Sous-traitant fournit au Responsable du traitement sans délai irraisonné toutes les informations en sa possession et nécessaires pour satisfaire aux obligations de **l'article 33 du RGPD** et s'engagera à toute collaboration attendue du responsable. Le Sous-traitant fournit par ailleurs les informations concernées aussi rapidement que possible, sous format accessible à déterminer par le Sous-traitant. De plus, le Sous-traitant informera le Responsable du traitement de nouveaux développements éventuels relatifs à la Fuite de données, et prendra toute mesure raisonnable à la résolution de la Fuite de données, tout comme la limitation des conséquences (possibles) aussi rapidement que possible. Le Sous-traitant prendra en outre les mesures nécessaires à la prévention d'une éventuelle Fuite de données future.

4.3 Le Sous-traitant n'informera pas le Responsable du traitement d'une Fuite de données s'il est véritablement clair que la Fuite de données ne pose aucun risque pour les droits et libertés des personnes physiques. En cas de moindre doute, le Sous-traitant communique la Fuite de données au Responsable du traitement pour le mettre en mesure de décider d'une communication éventuelle de la Fuite de données. Le Sous-traitant documentera toute les infractions, même celles qui ne doivent pas être communiquées au Responsable du traitement, et procurera cette documentation une fois par trimestre au Responsable du traitement ou plus tôt si le Responsable du traitement en fait la demande. La documentation comprend au minimum des informations comme signifiées en **Annexe 4**.

4.4 Il est du ressort exclusif du Responsable du traitement de déterminer si une Fuite de données telle que constatée par le Sous-traitant doit être communiquée à l'autorité compétente et/ou à des personnes concernées déterminées.

5 Recours à des Sous-traitants ultérieurs

5.1 Le sous-traitant est autorisé lors du Traitement, à engager des Sous-traitant ultérieurs tiers sans autorisation écrite préalable du Responsable du traitement.

5.2 Le Sous-traitant veille à ce que le(s) tiers concerné(s) passe(nt) un accord selon lequel il(s) respecte(nt) au moins les mêmes obligations légales que celle du Sous-traitant.

5.3 Le Sous-traitant informe le Responsable du traitement de l'engagement des Sous-traitants ultérieurs auquel il a procédé. Le Responsable du traitement peut ainsi s'opposer à l'ajout ou au remplacement de Sous-traitants ultérieurs par le Sous-traitant.

5.4 Le Responsable du traitement donne ainsi, à chaque fois, son autorisation avant l'engagement de Sous-traitants ultérieurs et/ou de catégories de Sous-traitants ultérieurs, tel que stipulé à **l'Annexe 2**.

6 Obligation de confidentialité

6.1 Le Sous-traitant préserve la confidentialité des données personnelles. Le Sous-traitant s'assure que les Données personnelles ne soient pas mises à la disposition directe ou indirecte de tiers. Par tiers, on entend également le personnel du Sous-traitant, dans la mesure où il n'est pas nécessaire que ce personnel prenne connaissance des Données personnelles. Cette interdiction ne vaut pas si cet accord détermine une indication contraire et/ou dans la mesure ou une prescription légale ou un jugement oblige à toute mention.

6.2 Le Sous-traitant s'assure que les personnes, sans se limiter aux employés, qui conjointement au Sous-traitant participent aux Traitements, sont liées à l'obligation de secret professionnel en matière de Données personnelles.

6.3 Le Sous-traitant informera le Responsable du traitement de toute demande d'accès à des données à caractère personnel, tout comme leur fourniture ou toute autre forme de demande et de communication des Données personnelles, en infraction à l'obligation de secret professionnel déterminée par cet article.

7 Délais de conservation et effacement

7.1 Le Responsable du traitement se charge de déterminer les délais de conservation relatifs aux Données personnelles. Dans la mesure où les Données personnelles se trouvent sous le contrôle du Responsable du traitement, ce dernier en a lui-même été informé de manière opportune.

7.2 Le Sous-traitant effacera les Données personnelles sous trente jours après la fin de l'Accord principal ou, au choix du Responsable du traitement les transmettra à celui-ci, à moins que les Données personnelles doivent être conservées plus longtemps, tel que dans le cadre des obligations (légales) du Sous-traitant, ou encore si le Responsable du traitement demande la conservation des Données personnelles pour une durée plus longue, ou si le Sous-traitant et le Responsable du traitement parviennent à un accord de couts et autres conditions pour cette durée plus longue, cette dernière hypothèse sans préjudice du respect des délais de conservation légaux par le Responsable du traitement. Un transfert éventuel au Responsable du traitement s'effectue aux frais du Responsable du traitement.

7.3 Le Sous-traitant déclarera, à la demande du Responsable du traitement que la suppression mentionnée au paragraphe précédent a eu lieu. Le Responsable du traitement peut faire exécuter un contrôle à ses propres frais si cela s'est réellement présenté. **L'Article 10** de cet accord s'applique à ce contrôle. Le

Sous-traitant informera dans la mesure nécessaire tous les Sous-traitants ultérieurs concernés par le traitement des Données personnelles, d'une résiliation de l'Accord principal et les instruira de les traiter comme déterminé par la présente.

7.4 À moins que les parties en conviennent autrement, le Responsable du traitement s'assure personnellement d'une sauvegarde des Données personnelles.

8 Droits des personnes concernées

8.1 Si le Responsable du traitement a personnellement accès aux Données personnelles, il satisfait lui-même à toutes les demandes des personnes concernées relatives aux Données personnelles. Le Sous-traitant transmettra éventuellement et sans délai des demandes reçues par lui-même au Responsable du traitement, ce dernier prenant en charge le traitement de la demande.

8.2 Uniquement dans la mesure où ce qui est entendu à l'article précédent n'est pas possible, le Sous-traitant proposera sa collaboration complète et opportune au Responsable du traitement pour :

(i) après approbation de, et à la demande du Responsable du traitement, l'accès des personnes concernées aux Données personnelles les concernant,

(ii) l'élimination ou la correction des Données personnelles,

(iii) attester que les Données personnelles ont été éliminées ou corrigées, si elles sont incorrectes (ou, dans le cas où le Responsable du traitement n'accepte pas que les Données personnelles soient incorrectes, confirmer le fait que la personne concernée considère ses Données personnelles comme incorrectes)

(iv) fournir les Données personnelles concernées au Responsable du traitement ainsi qu'à un tiers désigné par le Responsable du traitement, sous une forme structurée, accessible et lisible par une machine et

(v) autrement donner l'occasion au Responsable du traitement de satisfaire à ses obligations en vertu du RGPD ou une autre législation applicable dans le domaine du traitement des Données personnelles.

8.3 Les couts, et les exigences de la collaboration évoquée au **paragraphe précédent** sont fixés de commun accord par les parties. Sans accord, les couts à cet égard sont imputables au Responsable du traitement.

9 Responsabilité

9.1 Le Sous-traitant est responsable envers le Responsable du traitement de tous dommages et couts supportés par le Responsable du traitement en conséquence d'une faute imputable au Sous-traitant, pour satisfaire à ses obligations en vertu de cet accord, y compris mais sans limitations, les dommages causés par le Sous-traitant lorsque le traitement ne satisfait pas aux obligations spécifiques du Sous-traitant relativement au RGPD ou s'il est en violation aux instructions légales du Responsable du traitement.

9.2 Le Sous-traitant préserve le Responsable du traitement de toute réclamation de tiers en conséquence d'une faute imputable au Sous-traitant pour respecter ses obligations envers le Responsable du traitement en vertu de cet accord.

9.3 Sans préjudice de la disposition de cet article 9, le règlement visé par l'Accord principal vaut sans restriction en ce qui concerne la responsabilité.

10 Contrôle

10.1 Le Responsable du traitement dispose du droit de contrôler ou de faire contrôler à ses propres frais le respect des dispositions de cet accord, lorsqu'il existe un motif raisonnable de le faire, mais en tous les cas, une fois par an, par un expert-comptable ou un comptable Informaticien indépendant.

10.2 En cas d'un tel contrôle, s'il apparait que le Sous-traitant n'a pas respecté ou pas respecté de manière juste cet accord et/ou les dispositions légales applicables lors du Traitement des Données personnelles, le Sous-traitant doit supporter les couts de l'enquête. Le Sous-traitant devra immédiatement après prise de connaissance de la défaillance attestée, remédier à ces défaillances. Ceci, sans préjudice des autres droits du Responsable du traitement.

10.3 Le Sous-traitant met à disposition du Responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations stipulées à **l'article 28 du RGPD**. Si la personne tierce engagée par le Responsable donne une instruction qui selon le Sous-traitant, enfreint le RGPD, le Sous-traitant en informera immédiatement le Responsable du traitement.

10.4 L'enquête du Responsable du traitement se limitera toujours aux systèmes du Sous-traitant qui ont été utilisés pour les Traitements. Le Responsable du traitement préservera le secret des informations révélées lors du contrôle et ne les utilisera que pour contrôler le respect des obligations par le Sous-traitant de cet accord et effacer aussi rapidement que possible les informations ou ses parties. Le Responsable du traitement s'assure que les tiers éventuellement engagés respectent ces obligations.
Le Sous-traitant fera exécuter ou exécutera lui-même des contrôles de sécurité périodiques et fournira une synthèse annuelle du résultat de ce contrôle qui comportera au minimum un aperçu des risques ainsi que des mesures pour limiter et résoudre ces derniers.

11 Traitement des données personnelles en dehors de l'Espace économique européen

11.1 Le transfert des Données personnelles par le Sous-traitant en dehors de l'Espace économique européen est uniquement autorisé dans le respect des obligations légales en vigueur à cet effet.

12 Autres dispositions

12.1 Le modifications de cet accord sont exclusivement valables si elles sont convenues par écrit par les deux parties.

12.2 Les parties adapteront cet accord en fonction de règlementations modifiées ou complémentaires, d'instructions complémentaires émanant des autorités compétentes et de l'évolution d'une réflexion en application du RGPD (par exemple par le biais, mais sans s'y limiter, d'une jurisprudence ou de rapports) de l'introduction de clauses types et/ou d'autres évènements ou réflexions nécessitant une telle adaptation.

12.3 Cet accord dure aussi longtemps que l'Accord principal dure. Les dispositions de cet accord demeurent valables dans la mesure du nécessaire pour les déviations à cet accord et dans la mesure où elles sont destinées à survivre la fin de cet accord. Les dispositions relatives au secret professionnel et aux litiges appartiennent entre autres à cette dernière catégorie de dispositions, sans s'y limiter.

12.4 Cet accord prévaut sur tous les autres accords entre le Responsable du traitement et le Sous-traitant.

12.5 Le présent accord est uniquement régi par le droit belge.

12.6 Les Parties soumettront leurs litiges associés à cet accord exclusivement au Tribunal de Bruges.

_____	_____
Par :	Par :
Au nom de : **Fairtual Technologies BV**	Au nom de :
Le :	Le :
À :	À :

Annexe 1

Traitement des données personnelles et délais de conservation

Les Annexes 1 et 2 doivent être renseignées de manière aussi complète que possible par le Responsable du traitement

Cette annexe fait partie de l'Accord de sous-traitance et doit être parafée par les parties.

I. Les Données personnelles devant être traitées par les parties :

[Description des données personnelles qui doivent être traitées sur la base de cet accord, telles que les données personnelles décrites ci-dessous. Prière de remplir.]

- ……
- ……
- ……
- ……
- ……
- ……
- ……
- ……
- ……
- ……
- ……

II. La nature, l'utilisation et l'objectif du traitement des Données personnelles :

[Description du devenir des Données personnelles (par exemple, leur enregistrement dans un fichier, leur insertion dans un envoi d'e-mail, etc.), l'objectif du traitement en question (par exemple, à fins de marketing, prospection commerciale, exécution d'un accord) et le type de moyen utilisé (par exemple le logiciel CRM).]

……
……
……
……
……
……
……
……
……

III. Les catégories des Personnes concernées en relation aux Données personnelles

[Description des catégories de Personnes concernées, par exemple les visiteurs de site Web, les abonnés, les fournisseurs, les enfants, les employés].

……
……
……
……
……
……
……

……
……

IV. Les délais d'utilisation et de conservation des (différentes sortes de) Données personnelles :

[Description des délais d'utilisation et de conservation que le sous-traitant doit respecter]

……
……
……
……
……
……
……
……
……

Annexe 2

Sous-traitants ultérieurs/catégories de Sous-traitants ultérieurs

Cette annexe fait partie de l'Accord de sous-traitance et doit être paraphée par les parties.

Cette annexe vous propose un aperçu des Sous-traitants ultérieurs tels que mentionnés à l'article 5.4 de cet accord.

Sous-traitants ultérieurs :

Nom du sous-traitant ultérieur	**Adresse**	**Coordonnées**	**Objectif du sous-traitant ultérieur**
C Bloom Comm. V.	Blauwvoetstraat 49 - 8310 Assebroek	info@cbloom.be GSM : +32478211899 BE0518.858.245	3D design
Sliced Comm. V.	Watermolenstraat 23 9230 Wetteren	info@sliced.be GSM : +32496660979 BE0739734272	Développement - TI
Combell NV	Skaldenstraat 121, 9042 Gand	administratie@combell.com TVA : BE 0541.977.701	hébergement
Whereby AS	Gate 1, N° 107 6700 Maloy, Norvège	pro@whereby.com	Visioconférences
tawk.to inc.	187 East Warm Springs Rd, SB298 Las Vegas, NV, 89119	support@tawk.to	Written chat booths
Chatwee Sp.	Piotrkowska 4, 62-610 Sompolno, Pologne	TVA : PL6652990463 https://chatwee.com/	Written Chat (Network Café)

Annexe 3

Mesures de sécurité du Sous-traitant

FAIRTUAL
TECHNOLOGIES BV

L'organisation surveille régulièrement la législation et la jurisprudence relatives au RGPD.

Chapitre	Objet	Statut
La politique de sécurité et l'organisation de la sécurité des informations	Protection des données : Un DPO a été nommé pour prendre en charge la coordination, la prestation de conseils, le contrôle et la sensibilisation aux procédures et directives relatives à la protection des données. Ce responsable suivra régulièrement des formations, de sorte à ce que ses connaissances soient toujours actuelles et expertes.	Le DPO désigné disposera des compétences nécessaires pour l'exécution de sa mission. Le DPO respecte un descriptif précis des fonctions et il ne peut pas y avoir de conflit d'intérêt avec d'autres tâches exécutées par le DPO à l'intérieur de l'organisation. Des moyens suffisants existent et suffisamment de temps est consacré à l'organisation de la sécurité des informations relatives au traitement des données personnelles. Une plateforme de décision active (DPO + équipe de projet) est en place et se réunit régulièrement pour prendre des décisions. La direction prodigue un soutien clair au début de la mise en œuvre de la protection des données dans l'organisation, ainsi que dans la gestion, le maintenance et si nécessaire l'ajustement.
	Responsabilités relatives à la protection : Des textes de politiques formels relatifs à la protection des données sont approuvés et connus des employés. Les responsabilités relatives à la protection des données sont transmises en interne.	Une politique de protection des informations générale relative au traitement des données personnelles est appliquée et communiquée aussi bien en interne qu'en externe, et évaluée régulièrement. Un soutien actif de la part de la direction est prodigué aux travailleurs autonomes en ce qui concerne le respect de la politique de protection des informations générale relative au traitement des données personnelles.
	Gestion des risques : Une analyse des risques formelle a été réalisée donnant lieu à des mesures de protection des données. Ce processus sera répété périodiquement.	Une analyse des risques régulière a été mise en place pour évaluer la nature des risques en cas de perte, transfert illégal, modification, ... des données personnelles. Une évaluation est menée régulièrement entre le prix d'achat pour la prise de mesures techniques et organisationnelles du point de vue des risques d'infractions éventuelles, et ses conséquences pour les droits et libertés des personnes concernées. Des mesures techniques et organisationnelles ont été et continuent d'être prises régulièrement pour éliminer les risques ayant une influence sur les droits et libertés des personnes concernées.
Politique sur la sécurité du personnel	Obligations de confidentialité : Les employés sont soumis à une obligation de confidentialité dans le cadre du traitement des données personnelles. Cette obligation est incluse dans le contrat de travail ou dans le code du travail.	Le Sous-traitant ne dispose d'aucune personne à son service. Un accord de confidentialité a été conclu avec tous les travailleurs autonomes. Des mesures disciplinaires internes prennent effet en cas d'infractions au traitement des données personnelles. La manière dont les employés traitent les données personnelles fait l'objet de contrôles réguliers.
	Sensibilisation : Les employés doivent être conscients de l'importance de la protection des données et devront suivre les procédures nécessaires dans le traitement des données personnelles. Cette sensibilisation sera répétée périodiquement	Tout travailleur autonome qui travaille avec le Sous-traitant a suivi diverses formations de sensibilisation dans le domaine du RGPD, tout comme dans le domaine de la cybersécurité.
	Entrée en service et cessation des fonctions : Les droits d'accès des différents employés prennent fin lors de la cessation de la collaboration de sorte que les personnes non autorisées n'aient plus accès aux données personnelles.	Il est tenu compte du déplacement interne des employés qui traitent ou traiteront les données personnelles. Les droits d'accès et autres droits sont évalués et modifiés si nécessaire.
Inventaire des immobilisations	Inventaire des immobilisations : Un inventaire de tous les systèmes de traitement des informations utilisés par les employés est tenu.	Au niveau de l'organisation, une claire distinction est établie entre les données personnelles, les données anonymes, les données codées et les données sensibles.

Cryptographie	Immobilisations : Tous les systèmes de traitement des informations sur lesquels des informations des responsables du traitement sont traitées sont cryptés de manière adaptée.	Il existe une politique relative à l'utilisation du chiffrage adaptée à l'analyse des risques dans le but de protéger la confidentialité, l'authenticité et/ou l'intégrité des données personnelles. L'organisation a développé une politique pour protéger la durée de vie des clés cryptographiques durant leur cycle de vie complet.
	Transferts d'informations : L'ensemble des données confidentielles des responsables du traitement sont uniquement transférées via une connexion sécurisée.	Il est toujours fait usage d'une connexion sécurisée.
Sécurité physique	Accès physique : Les bâtiments où les données personnelles sont traitées sont accessibles uniquement aux personnes identifiées et autorisées.	Des mesures de sécurité adaptées sont prises en matière de sécurité physique des locaux et bâtiments. Il est tenu compte de toute forme potentielle de dommages (incendie, eau, ...). Il est tenu compte de la sécurité de l'appareillage, du câblage et des infrastructures de soutien pour prévenir la perte, les dommages, le vol et le changement indésirable des données personnelles. Une attention particulière est accordée à l'appareillage qui se trouve et est utilisé en dehors du terrain de l'organisation.
Contrôle d'accès	Politique d'accès : Les droits de tout employé seront limités en fonction de la base d'une nécessité de savoir. Un accès plus important que prévu initialement sera uniquement possible après une approbation formelle et accompagné de motifs valables.	Une politique d'accès documentée est actuellement en place qui indique clairement quelles sont les personnes qui ont accès à des types de données personnelles définis. On tient compte ici de la classification des données. Une personne responsable est désignée pour répondre aux questions relatives aux droits d'accès. Cette personne responsable est différente de la personne qui octroie, modifie ou élimine les droits d'accès techniques dans les systèmes. Il existe des mesures de sécurité adaptées pour l'accès à des données (telles que la sécurité du mot de passe). Une division des fonctions est en place pour empêcher qu'une personne jouisse de tous les droits.
	Autorisation d'accès : Pour obtenir un accès à des informations sensibles, un système d'autorisation adapté est mis en place. Chaque individu recevra un identifiant unique lui permettant de se connecter.	
	Authentification : L'authentification des utilisateurs repose sur l'application d'un système d'authentification solide. Si l'accès à des données personnelles sensibles via internet est possible, une authentification multifacteur devra être utilisée.	
	Accès au réseau : Il existe un système qui offre, dans une mesure raisonnable de certitude, cet accès protégé et adapté au réseau (p. ex. pare-feux, équipements de sécurité, ...)	La sécurité du réseau (parefeux, Wifi ...) fait partie du plan de sécurité des informations.
Sécurité opérationnelle	Sauvegarde : Les données personnelles sont régulièrement sauvegardées. Ces sauvegardes sont cryptées et conservées sur un emplacement externe.	Une politique de sauvegarde adaptée est en place, testée régulièrement et respectée pour garantir une récupération adéquate après des dommages, la perte, ou le vol et des modifications indésirables des données personnelles. Il existe une politique relative à l'utilisation du chiffrage adaptée à l'analyse des risques dans le but de protéger la confidentialité, l'authenticité et/ou l'intégrité des données personnelles. L'organisation a développé une politique pour protéger la durée de vie des clés cryptographiques durant leur cycle de vie complet.
	Actualisations de sécurité : Les actualisations et correctifs de sécurité sont obtenus et installés systématiquement.	Une protection actualisée contre les logiciels de malveillance est employée. Les utilisateurs finaux et du système sont suffisamment sensibilisés à la sécurité. Les actualisations de sécurité sont régulièrement appliquées.
Protection de la communication	Transfert sur les réseaux : Toutes les données personnelles envoyées via des canaux ou réseaux publics ou internes sont adéquatement cryptées.	Une politique sur les e-mails et internet (transport) est mise en place accordant une grande importance à l'utilisation de données à caractère personnel dans les e-mails.

Relations avec les fournisseurs	Choix des Sous-traitants ultérieurs : Un processus de sélection adéquat est utilisé lors du choix des Sous-traitants ultérieurs, donnant lieu à l'évaluation de la sécurité des données personnelles. Seules les parties satisfaisant aux normes actuelles en matière de sécurité des informations et	Les efforts de sécurité des systèmes informatiques des sous-traitants ultérieurs sont contrôlés à l'achat. Lors du développement de nouveaux systèmes d'informations, ou lors de l'élargissement des systèmes informatiques actuels (applications, services, outils TI ou autre dispositif traitant des informations, ...) un contrôle des exigences de sécurité sera mis en place.

	de la protection des données sont utilisées pour le traitement des données personnelles.	
	Obligations contractuelles : Un accord de sous-traitance est en place avec tous les fournisseurs potentiels susceptibles de traiter les données personnelles. Cet accord comporte toutes les dispositions obligatoires et a été signé.	Des accords de sous-traitance juridiquement approuvés avec des responsables du traitement externes sont disponibles. Les accords de sous-traitance sont contrôlés en matière de sécurité des données personnelles. Les accords de sous-traitance comportent des garanties suffisantes que le(s) sous-traitant(s) (ultérieur(s)) traitera/-ont les données personnelles conformément au RGPD. Ce(s) sous-traitant(s) (ultérieur(s)) est/sont soumis à un contrôle à fins de conformité au Règlement général sur la protection des données (RGPD).
Gestion des incidents de sécurité de l'information	Gestion des incidents : Une procédure interne est en place pour garantir que les infractions à la sécurité possibles sont communiquées et transmises ensuite aux responsables. Cette procédure a été clairement communiquée en interne. Toutes les atteintes potentielles à la sécurité sont rassemblées en un point central.	Il est assuré que les incidents puissent être détectés, traités et signalés sur la base de procédures documentées. En cas d'incidents, le DPO est immédiatement informé. Le DPO connaît tous les emplacements vulnérables pouvant mener à des incidents, ainsi que les solutions permettant d'éliminer ces risques. En cas d'incident, les responsabilités sont établies.
	Notification des incidents : En cas d'incident de sécurité ayant un impact sur la confidentialité, l'intégrité ou la disponibilité des données personnelles, des mesures nécessaires seront prises pour informer le responsable du traitement en temps utile et de manière satisfaisante.	L'organisation est en mesure de garantir la continuité et la disponibilité des données personnelles sur la base des résultats d'une analyse de risque. Une planification de la continuité des activités est en place. L'organisation prévoit une redondance satisfaisante (= la prévention d'un incident) à l'intérieur des services de traitement des données pour garantir la disponibilité des données personnelles. Les risques de protection des données supplémentaires en conséquence d'une redondance seront ici observés.

Continuité des activités	Récupération après un sinistre : Un système adapté est présent en cas de pannes pour garantir la disponibilité et l'intégrité des données.	Une déclaration de confidentialité est en place conformément au RGPD et les données suivantes comportent : • l'identité de la personne responsable du traitement • les objectifs pour lesquels les données sont traitées • les données personnelles qui sont traitées par objectif • la base légale du traitement des données • les délais de conservation • si les données sont échangées en dehors de l'Union européenne • la possibilité pour la personne concernée de procéder à une réclamation auprès du GBA si cette personne pense que ses données personnelles ont été traitées de manières défaillante • les droits des personnes concernées • les mesures techniques et organisationnelles prises par l'organisation pour protéger les données personnelles un registre comportant les activités de traitement et satisfaisant à la règlementation RGPD est utilisé Ce registre comporte : • le nom et les coordonnées du responsable du traitement (commun), du représentant du responsable du traitement et/ou du fonctionnaire chargé de la protection des données • les objectifs de traitement • une description des catégories des personnes concernées • une description des catégories des données personnelles ? • les catégories des destinataires pour qui les données personnelles ont été ou seront utilisées • les destinataires des pays tiers ou des organisations internationales • les délais de conservation • une description générale des mesures de sécurité techniques et organisationnelles ? • transferts de données personnelles à un pays tiers ou une organisation internationale et si nécessaire les documents relatifs aux garanties appliquées ? Il peut être satisfait à la demande de personnes concernées au sujet de leur droits : • les droits des personnes concernées sont présentés de manière sommaire, transparente, compréhensible et sous forme facilement accessible, en langue claire et simple pour les personnes concernées ? • l'organisation accueille favorablement le droit à l'information • l'organisation accueille favorablement le droit d'accès aux dossiers • l'organisation accueille favorablement le droit à la modification • l'organisation accueille favorablement le droit de suppression/d'oubli

		• l'organisation convient que la portée des données personnelles traitées est limitée • l'organisation prend compte du droit de transférabilité des données • l'organisation accueille favorablement le droit d'objection • l'organisation prend compte du droit pour les personnes concernées de ne pas être assujetties à une prise de décision automatisée, y compris le profilage l'organisation dispose de fondements légaux pour tout traitement défini Si nécessaire, une autorisation est demandée aux personnes concernées pour le traitement de leurs données personnelles, grâce à quoi un choix libre est donné aux personnes concernées de pouvoir expressément adhérer (un opt-in). L'autorisation est obtenue grâce à un traitement actif et la personne concernée peut à tout moment suspendre son autorisation de manière simple lorsqu'un opt-in a été prévu. Toutes les autorisations octroyées pour le traitement des données personnelles sont contrôlables (connexion, ...) Des données relatives à des enfants ne sont pas traitées. Préalablement à tout traitement, une Étude d'impact sur la protection des données est exécutée lorsqu'un risque important à la confidentialité est perçu.

		L'organisation surveille la législation et la jurisprudence relatives au RGPD de manière régulière.
Respect	Conformité : La démontrabilité du respect des exigences peut être demandé auprès du responsable du traitement des données	

Annexe 4

Informations relatives à une Fuite de données

Le Sous-traitant fournira tous les renseignements dont le Responsable du traitement aura besoin pour évaluer la Fuite de données ou l'incident. De même, le Sous-traitant fournira dans tous les cas les renseignements suivants au Responsable du traitement :

- quelle est la cause (supposée) de la Fuite de données ou de l'incident ;
- quelle en est la conséquence (jusqu'à présent connue et/ou à prévoir) ;
- quelle est la solution proposée ;
- les coordonnées pour le suivi de la communication ;
- (une évaluation du) nombre de personnes dont les données sont concernées par la Fuite de données ou l'incident ;
- une description de la catégorie des personnes concernées affectées par la Fuite de données ou l'incident ;
- la sorte ou les sortes de Données personnelles affectées par la Fuite de données ou l'incident ;
- la date/période à laquelle la Fuite de données ou l'incident a eu lieu ;
- la date et le moment où la Fuite de données ou l'incident ont été détectés par le ous-traitant ou un tiers ou un sous-traitant ultérieur engagés par ce Sous-traitant ;
- si les données ont été cryptées, hachées ou autrement rendues inaccessibles pour des personnes non autorisées ;
- quelles mesures ont été prises pour mettre un terme à la Fuite de données ou l'incident. et limiter les conséquences de l'infraction.