Contrat sur le traitement des données conformément à l'art. 28 du EU-GDPR.

entre

_____

_____

- ci-après dénommée mandant-

et

Design4you sàrl, 46 rue du Commerce, L-3450 Dudelange

- ci-après dénommé mandataire -

Le présent contrat doit être envoyé au mandataire par le mandant après complétion et signature juridiquement valable. Ce n'est qu'après réception et traitement du contrat par le mandataire qu'il devient juridiquement valable. La transmission peut s'effectuer via :

- Lettre à Design4you sàrl, 46 rue du Commerce, L-3450 Dudelange, Luxemburg
- Fax au (+352) 26 35 20 22
- Courriel avec signature électronique qualifiée à l'adresse webhosting@letzebuerg.net
- Remise personnelle à 46 rue du Commerce, Dudelange, Luxemburg.
- Transfert en pièce jointe à un ticket de support à https://www.letzebuerg.net/

1. Objet et durée du mandat

L'objet et la durée du mandat sont déterminés dans leur intégralité conformément aux dispositions en vigueur dans les relations contractuelles respectives.

Sur la base de cette commande, le contractant traite les données personnelles du client au sens de l'art.4 n°2 et de l'art.28 EU-GDPR.

2. Portée, type et objet de la collecte, du traitement ou de l'utilisation des données

La portée, la nature et l'objet de toute collecte, traitement ou utilisation de données à caractère personnel, la nature des données et le groupe de personnes concernées sont décrits au mandant par le mandataire conformément à **l'annexe A** complétée par le mandataire, à moins que cela ne résulte du contenu contractuel des relations contractuelles décrites au point 1.

Le traitement des données convenu contractuellement 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. Tout transfert vers un pays tiers nécessite l'accord préalable du donneur d'ordre et ne peut avoir lieu que si les conditions particulières des articles 44 et suivants de EU-GDPR sont remplies.

Pour l'exécution des services "domaine" commandés par le mandataire, il peut être nécessaire, en fonction de l'affiliation géographique, du bureau d'administration du domaine exigé ainsi que

du partenaire du domaine applicable, que, conformément à EU-GDPR, les données personnelles fournies par le client à cette fin spécifique soient transmises en tant que transfert fonctionnel nécessaire pour l'exécution de la commande à un sous-traitant dans ou en dehors de l'Union européenne ou de l'Espace économique européen. Dans ce cas, le mandant assure que le sous-traitant remplit également les mesures organisationnelles et techniques spécifiées par l'EU-GDPR.

3. Mesures techniques d'organisation selon l'art. 32 du GDPR-EU et l'art. 28 para.3 du GDPR-EU.

(1) Le mandataire doit documenter la mise en œuvre des mesures techniques et organisationnelles définies et requises avant le commancement du traitement de données et les remettre au mandant pour contrôle. Cela s'applique en particulier à l'exécution concrète de la commande (**voir annexe B**). En cas d'acceptation par le mandant, les mesures documentées constituent la base du contrat.

(2) Le mandataire doit établir la protection conformément à l'art. 28 al. 3 phrase 2 lit. c, 32 EU-GDPR, en particulier en relation avec l'art. 5 al. 1, al. 2 EU-GDPR. Dans l'ensemble, les mesures à prendre sont des mesures de sécurité des données ainsi qu'une assurance de niveau de protection approprié au risque en ce qui concerne la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes. Il faut tenir compte de l'état de la technique, des coûts de mise en œuvre ainsi que du type, de l'étendue et des objectifs du traitement. Il faut aussi tenir compte de la probabilité de survenance et de la gravité du risques pour les droits et libertés des personnes physiques au sens de l'article 32, paragraphe 1, du EU-GDPR.

(3) Les mesures techniques et organisationnelles sont soumises au progrès technique et au développement ultérieur. A cet égard, le contractant est autorisé à mettre en œuvre d'autres mesures adéquates. Le niveau de sécurité des mesures définies ne doit pas être inférieur. Tout changement important doit être documenté.

4. Correction, blocage et suppression de données

(1) Le mandataire ne peut pas supprimer ou limiter le traitement des données traitées dans la commande de son propre autorité . Si une personne concernée contacte directement le mandataire à cet égard, le mandataire doit immédiatement transmettre cette demande au mandant.

(2) Dans la mesure où l'étendue des prestations comprend le concept, la suppression, le droit à l'oubli, la correction des données, la transférabilité des données et le doit l'information doivent être assurés directement par le mandataire conformément aux instructions documentées du mandant.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Outre les dispositions du présent contrat, le mandataire a des obligations légales conformément aux articles 28 à 33 du EU-GDPR ; à cet égard, il garantit en particulier le respect des exigences suivantes:

- Le respect de la confidentialité conformément à l'Art. 28 para. 3 p. 2, 29, 32 para. 4 EU-GDPR. Dans l'exécution des tâches, le mandataire n'emploie que des collaborateurs qui sont tenus à la confidentialité et qui ont été préalablement familiarisés avec les dispositions relatives à la protection des données qui les concernent. Le mandataire et toute personne soumise au mandataire qui a accès aux données à caractère personnel peuvent traiter ces données que exclusivement conformément aux instructions du mandant, y compris les pouvoirs conférés dans le présent contrat à l'exception qu'ils ne soient légalement obligés de les traiter.

- La mise en œuvre et le respect de toutes les mesures techniques et organisationnelles nécessaires à cet ordre correspondent à l'article 28, paragraphe 3, phrase 2, alinéa c, 32 EU-GDPR et à l'annexe B.
- Le mandataire et le mandant coopèrent, sur demande, avec l'autorité de surveillance dans le cadre de l'exécution de leurs tâches.
- L'Information immédiate du mandant sur toute action de contrôle et des mesures prises par l'autorité de surveillance se rapportent à ce mandat. Cette disposition s'applique également dans la mesure où une autorité compétente enquête concernant le traitement de données à caractère personnel chez le mandataire dans le cadre d'une procédure pénale.
- Si le mandant est soumis pour sa part à une inspection par l'autorité de surveillance, à une procédure administrative ou pénale, à la responsabilité d'une personne concernée ou d'un tiers ou à toute autre exigence dans le cadre du traitement de données chez le mandataire, ce dernier doit l'assister au mieux de ses capacités.
- Le mandataire surveille régulièrement les processus internes ainsi que les mesures techniques et organisationnelles afin de s'assurer que le traitement de donnnées dans son domaine de responsabilité est effectué conformément aux exigences de la législation applicable en matière de protection des données et que les droits de la personne concernée sont protégés.
- La documentation des mesures techniques et organisationnelles prises à l'égard du client, qui peut être consultée sur le site https://letzebuerg.net/gdpr/ conformément au chapitre 3.

6. Contrats de sous-traitance

Les relations de sous-traitance au sens de la présente disposition s'entendent des services directement liés à la fourniture du service principal. Cela ne comprend pas les services auxiliaires que le mandataire utilise, par exemple des services de télécommunication, services postaux/de transport, services de maintenance et services aux utilisateurs, ainsi que d'autres mesures visant à assurer la confidentialité, la disponibilité, l'intégrité et la résilience du matériel et des logiciels des systèmes de traitement des données. Toutefois, afin de garantir la protection des données et la sécurité des données du client, le mandataire est tenu de réaliser des accords contractuels et des mesures de contrôle appropriés et conformes à la loi, même dans le cas de services auxiliaires externalisés.

7. Les droits de contrôle du mandant
(1) Le mandant a le droit d'effectuer des inspections de la conduite avec le mandataire ou de les faire effectuer par des inspecteurs qui seront désignés au cas par cas. Il a le droit de s'assurer du respect de cet accord par le mandataire dans le cadre de ses activités commerciales au moyen de contrôles par sondage qui, en règle générale, doivent être notifiés en temps utile.

(2Le mandataire veille à ce que le donneur d'ordre puisse s'assurer du respect par le mandataire de ses obligations au titre de l'art. 28 du EU-GDPR. Le contractant s'engage à fournir au client les informations nécessaires sur demande et en particulier à apporter la preuve de la mise en œuvre des mesures techniques et organisationnelles.

(3) La preuve de ces mesures, qui ne concernent pas seulement ce mandat concret, peut être apportée par le respect des règles de conduite approuvées conformément à l'art. 40 EU-GDPR, la certification après une procédure de certification approuvée conformément à l'art. 42 EU-GDPR, les certificats actuels, les rapports ou extraits de rapports d'autorités indépendantes (par ex. auditeur, audit, responsable de la protection des données, département de la sécurité informatique, auditeurs de la protection des données, auditeurs de la qualité) et/ou une certification appropriée par des audits de la sécurité informatique ou de la protection des données.

(4) Le mandataire peut faire valoir un droit à rémunération afin de permettre au client d'effectuer ces inspections.

8. Notification en cas de manquement de la part du mandataire.
(1) Le mandataire aide le mandant à se conformer aux obligations énoncées aux articles 32 à 36 du EU-GDPR en ce qui concerne la sécurité des données à caractère personnel, les obligations de notification en cas de fuites de données, les évaluations d'impact sur la protection des données et les consultations préalables. Cela comprend, entre autres, les éléments suivants

a. Garantir un niveau de protection adéquat par des mesures techniques et organisationnelles qui tiennent compte des circonstances et des objectifs du traitement ainsi que de la probabilité et de la gravité prévues d'une éventuelle violation des droits causée par des failles de sécurité et de permettre de déterminer immédiatement les cas de violation pertinents.
b. L'obligation de signaler sans délai les violations des données personnelles au mandant.
c. L'obligation de soutenir le mandant dans le cadre de son obligation d'informer la personne concernée et de mettre sans délai à sa disposition toutes les informations pertinentes à cet égard.
d. Soutenir le mandant dans son évaluation d'impact sur la protection des données.
e. Soutenir le mandant lors de ses consultations préalables avec l'autorité de surveillance.

(2) Le mandataire peut demander une indemnisation pour des services de soutien qui ne sont pas inclus dans la description du service ou qui ne sont pas attribuables à une mauvaise conduite de la part du mandataire.

9. Pouvoir de direction du mandant

(1) Le client confirme les instructions verbales sans délai (au moins sous forme de texte).

(2) Le mandataire est tenu d'informer immédiatement le mandant 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 qu'elle soit confirmée ou modifiée par le mandant.

10. Suppression et restitution des données personnelles

(1) Les copies ou duplicatas des données ne seront pas faites à l'insu du mandant. En sont exclues les copies de sauvegarde, dans la mesure où elles sont nécessaires pour garantir un traitement correct des données, ainsi que les données nécessaires au respect des obligations légales de conservation.

(2) Après l'achèvement des prestations convenues dans le contrat ou plus tôt à la demande du client ou -au plus tard à la résiliation du contrat de service le fournisseur doit remettre au client tous les documents, les résultats du traitement et de l'utilisation ainsi que les stocks de données créés dans le cadre de la relation contractuelle ou les détruire conformément aux dispositions relatives à la protection des données après accord préalable. Il en va de même pour les matériaux de test et de rebut. Sur demande, le fournisseur doit informer le client de la nature et de l'heure de l'effacement.

(3) La documentation qui sert de preuve d'un traitement ordonné et approprié des données doit être conservée par le mandataire après la fin du contrat, conformément aux délais de conservation respectifs. Il peut les remettre au mandataire à la fin du contrat pour son allègement.

11. Autres Accords

11.1. Entgelte

Il n'y a pas de frais pour le présent contrat.

Dans la mesure où le mandant a besoin d'une assistance conformément à l'article 4 pour répondre aux questions des personnes concernées, il doit rembourser les frais qui en découlent au mandataire.

Dans la mesure où le mandant exercera des droits de contrôle conformément à l'article 7, le montant de la rémunération est à convenir à l'avance et sera basé sur un taux horaire déterminé en fonction de l'employé chargé par le mandataire de l'assistance.Erteilt der Auftraggeber dem Auftragnehmer Weisungen nach Ziffer 9, so hat er durch diese Weisung entstehende Kosten zu erstatten

11.2. Période de contrat

La présente entente est assujettie à l'existence d'une relation contractuelle principale conformément à l'article 1, et la résiliation ou toute autre résiliation de la relation contractuelle principale conformément à l'article 1 met également fin à la présente entente.

Le droit à une résiliation isolée et extraordinaire de ce contrat ainsi que l'exercice des droits légaux de rétractation de la convention restent inchangés.

11.3. Loi applicable

Le droit du Grand-Duché de Luxembourg est applicable.

11.4. Tribunal compétent

Les parties conviennent que le tribunal compétent est celui de Luxembourg.

Signatures

Mandant	**Mandataire**
_____,	_____,
le _____	le _____
_____	_____
Signature Mandant	Signature Mandataire

Annexe A : Type de données et groupe de personnes concernées

Pour que le présent contrat soit valable, le mandant doit énumérer tous les traitements ou types de collecte de données concernés par l'EU-GDPR.

Type de données	Objet de la collecte, du traitement ou de l'utilisation des données	Personnes concernées
Données de base personelles	_____ _____ _____ _____	[ ] Clients et parties intéressées du mandant. [ ] Employés et fournisseurs du client [ ] _____
Données de communication p.ex. téléphone, email, fax, ...	_____ _____ _____ _____	[ ] Clients et parties intéressées du mandant. [ ] Employés et fournisseurs du client [ ] _____
Détails de contrats	_____ _____ _____ _____	[ ] Clients et parties intéressées du mandant. [ ] Employés et fournisseurs du client [ ] _____
Journals/Protocoles Fichiers journaux, informations d'audit, journaux d'accès,.....	_____ _____ _____ _____	[ ] Clients et parties intéressées du mandant. [ ] Employés et fournisseurs du client [ ] _____
_____ _____	_____ _____ _____ _____	[ ] Clients et parties intéressées du mandant. [ ] Employés et fournisseurs du client [ ] _____

Annexe B : Actions du mandataire au titre de l'article 32 du EU-GDPR.

I. Confidentialité
- Contrôle d'accès physique
  - Datacentre Accelerated-IT à Frankfort
    - système électronique de contrôle d'accès avec journalisation
    - l'attribution bien documentée des clés aux employés et aux clients autorisés
    - Directives pour l'accompagnement et le marquage des visiteurs dans le bâtiment
    - 24/7 dotation en personnel
    - Vidéosurveillance aux entrées, sorties et salles de serveurs.
    - L'accès aux salles pour les personnes extérieures (par ex. visiteurs) est limité comme suit : uniquement si elles sont accompagnées d'une personne autorisée.
  - Administration
    - surveillance électronique avec des clés individuelles
    - Vidéosurveillance aux entrées et sorties
- Contrôle d’accès au système
  - Pour commandes “Serveur” ou “serveur virtuel”
    - Les mots de passe de serveur, qui sont à modifier par le client lors de la première utilisation et qui ne sont pas connus au mandataire.
    - Le mot de passe de l'interface d'administration principale est attribué par le mandant lui-même - les mots de passe doivent être conformes aux directives prédéfinies. De plus, le mandant peut utiliser l'authentification à deux facteurs pour sécuriser davantage son compte.
  - Pour commandes „Serveur administré“ ou „Hêbergement web“
    - L'accès est protégé par mot de passe, l'accès est réservé aux employés autorisés du mandataire; les mots de passe utilisés doivent avoir une longueur minimale et sont renouvelés à intervalles réguliers.
- Contrôle d’accès de tiers
  - Sur les systèmes internes du mandataire
    - L'entrepreneur s'assure que l'accès non autorisé est empêché par des mises à jour régulières de la sécurité et conforme à l'état actuel de la technique.
    - Procédures d'autorisation pour les employés du mandataire
  - Pour commandes “Serveur” ou “serveur virtuel”
    - La responsabilité du contrôle d'accès revient au mandant.
  - Pour commandes „Serveur administré“ ou „Hêbergement web“
    - L'entrepreneur s'assure que l'accès non autorisé est empêché par des mises à jour régulières de la sécurité conformément à l'état actuel de la technique.
    - Procédures d'autorisation pour les employés du mandataire
    - Le mandant est le seul responsable de la sécurité et mises à jour des données/logiciels transmis.
- Contrôle des supports des données
  - Datacentre Accelerated-IT
    - Les disques durs virtuels et réels sont effacés après la terminaison en utilisant une procédure définie. Après vérification, les disques durs sont à nouveau insérés.
    - Les disques durs défectueux qui ne peuvent pas être effacés en toute sécurité seront détruits.
- Contrôle de séparation
  - Sur les systèmes internes du mandataire

        - Les données sont stockées physiquement ou logiquement séparées des autres données.
        - Les données sont aussi sauvegardées sur des systèmes logiquement et/ou physiquement séparés.
    - Pour commandes “Serveur” ou “serveur virtuel”
        - Le contrôle de la séparation est la responsabilité du client.
    - Pour commandes „Serveur administré“ ou „Hébergement web“
        - Les données sont stockées physiquement ou logiquement séparées des autres données.
        - Les données sont aussi sauvegardées sur des systèmes logiquement et/ou physiquement séparés.
- Pseudonymisation
    - Le mandant est responsable de la pseudonymisation.

II. Integrité (Art. 32 para. 1 lit. b EU-GDPR)

- Contrôle des transferts
    - Tous les employés sont instruits au sens de l'art. 32 al. 4 EU-GDPR et sont tenus de veiller à ce que les données personnelles soient traitées dans le respect de la réglementation sur la protection des données.
    - Suppression des données conformément aux exigences en matière de protection des données après la clôture de la commande.
    - Les possibilités de transmission de données cryptées sont mises à disposition dans le cadre de la description du service de la commande principale.
- Contrôle d'entrée
    - Sur les systèmes internes du mandataire
        - Les données sont saisies ou enregistrées par le mandant lui-même.
        - Les modifications apportées aux données sont enregistrées.
    - Pour commandes “Serveur” ou “serveur virtuel”
        - La responsabilité du contrôle d'entrée revient au mandant.
    - Pour commandes „Serveur administré“ ou „Hébergement web“
        - Les données sont saisies ou enregistrées par le mandant lui-même.
        - Les modifications apportées aux données sont enregistrées.

III. Disponibilité et résilience (art. 32 para. 1 lit. b EU-GDPR)

- Contrôle des disponibilités
    - Sur les systèmes internes du mandataire
        - Concept de sauvegarde et de restauration avec sauvegarde quotidienne de toutes les données pertinentes.
        - Utilisation professionnelle de programmes de protection (antivirus, pare-feu, programmes de cryptage, filtres anti-spam).
        - Miroir des disques durs sur tous les serveurs concernés.
        - Surveillance de tous les serveurs pertinants..
        - Utilisation d'une alimentation sans coupure, d'un système d'alimentation de secours.
        - Protection DDoS au niveau du réseau et du serveur.
    - Pour commandes “Serveur” ou “serveur virtuel”
        - La sauvegarde des données est la responsabilité du mandant.
        - Utilisation d'une alimentation sans coupure, d'un système d'alimentation de secours.
        - Protection DDoS au niveau du réseau et du serveur.
    - Pour commandes „Serveur administré“ ou „Hébergement web“
        - Concept de sauvegarde et de restauration avec sauvegarde quotidienne de toutes les données pertinentes.
        - Miroir des disques durs sur tous les serveurs concernés.
        - Utilisation d'une alimentation sans coupure, d'un système d'alimentation de secours.

        - Utilisation d'un pare-feu logiciel et une réglementation sur les ports.
        - Protection DDoS au niveau du réseau et du serveur.
    - Recouvrabilité rapide (Art. 32 para. 1 lit. c) EU-GDPR)
        - Une chaîne d'escalade est définie pour tous les systèmes internes, qui spécifie qui doit être informé en cas d'erreur afin de restaurer le système le plus rapidement possible.

IV. Procédure d'examen, d'évaluation et d'évaluation réguliers (art. 32 para. 1 lit. d EU-GDPR ; art. 25 para. 1 EU-GDPR)
    - La gestion des interventions en cas d'incident est disponible.
    - Les paramètres favorables à la protection des données sont pris en compte dans les développements de logiciels (Art. 25 para. 2 EU-GDPR).

Contrôle des commandes

- Nos collaborateurs sont régulièrement formés au droit de la protection des données et connaissent les instructions de procédure et les directives d'utilisation pour le traitement des données pour le compte du mandant, y compris en ce qui concerne le droit d'instruction du mandant.
- Les CGV contiennent des informations détaillées sur le type et l'étendue du traitement et de l'utilisation des données personnelles du mandant.
- Les CGV contiennent des informations détaillées sur l'appropriation des données personnelles du client.