RGPD

ChallengeMe fournit une charte à tous ses clients. Nous nous engageons à respecter la confidentialité des données ainsi que leur protection.

Usage dans le cadre GAR / MEN

Tous les utilisateurs s'inscrivant dans un usage GAR de ChallengeMe s'inscrivent dans le Traitement GAR. Les mentions RGPD applicables se trouvent à cette adresse : https://gar.education.fr/mentions-informatives-rgpd/vv

CONTRAT RGPD

I. Préambule

Dans le cadre de l'application le 25 mai 2018, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après, « RGPD »), la présente annexe a pour objet de définir les conditions dans lesquelles ServicesYou, qui a la qualité de Sous-traitant au terme du RGPD, s'engage à effectuer les opérations de traitement des données à caractère personnel définies à l'Article VII de la présente annexe, pour le compte et sur instruction d'Organisation et Développement, responsable de traitement, en conformité avec la règlementation en vigueur, et notamment le RGPD et toute loi ou réglementation nationale applicable au Responsable de traitement et au Sous-traitant (ci-après la « Réglementation applicable »).

II. Obligations du Sous-traitant vis-à-vis du Responsable de traitement

Le Sous-traitant s'engage à :

1. traiter les données uniquement pour la ou les seule(s) finalité(s)qui fait/font l'objet de la sous-traitance telle(s) que décrite(s) dans l'Article VII.

2. traiter les données conformément aux dispositions de la présente annexe et de toute instruction documentée postérieuredu Responsable de traitement. Si le Sous-traitant considère qu'une instruction constitue une violation de la Réglementation applicable, il en informe immédiatementle Responsable de traitement.

3. garantir la confidentialitédes données à caractère personnel traitées dans le cadre du Contrat ou de la Convention.

4. veiller à ce que les personnes autorisées à traiter les données à caractère personnel:

- s'engagent à respecter la confidentialité desdites donnéesou soient soumises à une obligation légale ou contractuelle appropriée de confidentialité
- reçoivent la formationnécessaire en matière de protection des données à caractère personnel

5. prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut.

6. Sous-traitance ultérieure

Dans l'hypothèse où le Sous-traitant recourait à son propre sous-traitant (ci-après le « Sous-traitant ultérieur ») pour le traitement des données qui lui sont confiées, il en informe préalablement et par écrit le Responsable de traitement et lui indique notamment les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et la durée de la sous-traitance ultérieure. Le Responsable de traitement disposera alors d'un délai de 30 jours à compter de la date de réception de cette information pour présenter toute objection motivée à la sous-traitance ultérieure.

Le Sous-traitant s'engage à s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées conformes à la Règlementation applicable et à reporter les stipulations du présent avenant, y incluant le droit de vérification et d'audit, dans le contrat le liant à tout sous-traitant ultérieur. Le Sous-traitant demeure seul et pleinement responsable envers le Responsable de traitement, dans les conditions de la présente annexe, de tout manquement du sous-traitant ultérieur aux obligations lui incombant.

Le Sous-traitant tient une liste des accords de sous-traitance ultérieure conclus en vertu de la présente clause qui sera mise à jour régulièrement et au moins une fois par an. Cette liste est mise à la disposition du Responsable de traitement et, si demandée, de la CNIL.

Dans le cas où le Sous-traitant, ayant obtenu l'accord préalable et écrit du Responsable de traitement, choisit un sous-traitant ultérieur situé en dehors de l'Union européenne, tous travaux de mise en conformité nécessaire seront pris en charge financièrement par le Sous-traitant. Dans une telle hypothèse, le Sous-traitant doit, à minima, justifier au Responsable de traitement :

a) Avoir signé avec le sous-traitant ultérieur les Clauses Contractuelles Type de la Commission Européenne, ou à défaut

b) l'application au sous-traitant ultérieur de « Binding Corporate Rules » approuvées par l'autorité de contrôle compétente, lorsque le sous-traitant ultérieur est une des filiales du Sous-traitant.

7. Obligation d'information

Le Sous-traitant tiendra le Responsable de traitement informé, sans délai et au maximum dans un délai de 5 jours ouvrés :

- de toute demande de communication de données à caractère personnel issue d'une autorité compétente ou qui s'impose au Sous-traitant en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, sauf si une exception légale dûment justifiable interdit une telle information pour des motifs d'intérêts publics ;
- de toute demande de la Personne Concernée d'exercice de ses droits au regard des traitements confiés au Sous-traitant. Dans cette hypothèse, le Sous-traitant ne répondra pas directement à la Personne Concernée à moins qu'il n'y ait été autorisé préalablement par écrit par le Responsable de traitement.

8. Exercice des demandes des Personnes concernées

Dans la mesure du possible, le Sous-traitant s'engage à assister le Responsable de traitement dans l'exécution de ses obligations légales en lien avec le respect des droits des Personnes concernées, à savoir les droits :

- à l'information : le Sous-traitant en charge de la collecte des données à caractère personnel des Personnes concernées s'engage à transmettre à ces dernières, lors de la collecte, la mention d'information fournie au Sous-traitant par le Responsable de traitement ;

- d’accès : extraction et transmission au Responsable de traitement par le Sous-traitant, dans un format lisible, des données qui lui sont confiées sur la Personne concernée ;
- de rectification, d’effacement et d’opposition : transmission au Responsable de traitement par le Sous-traitant d’une attestation d’exécution ;
- à la limitation du traitement : transmission au Responsable de traitement par le Sous-traitant d’une attestation d’exécution ;
- à la portabilité des données : extraction et transmission au Responsable de traitement par le Sous-traitant, dans un format structuré, couramment utilisé et lisible par machine, dans un format lisible, des données qui lui sont confiées sur la Personne concernée ;
- de ne pas faire l’objet d’une décision individuelle automatisée (y compris le profilage) : transmission au Responsable de traitement par le Sous-traitant d’une attestation d’exécution.

Le Sous-traitant s’engage par ailleurs à transmettre au Responsable de traitement toute information nécessaire au respect, par ce dernier, des droits des Personnes concernées, dans les meilleurs délais, et au maximum dans un délai de 10 jours ouvrés à compter de la demande du Responsable de traitement.

9. Notification des Violations de données à caractère personnel

Le Sous-traitant notifie à l’interlocuteur privilégié du Responsable de traitement identifié à l’article 7 toute Violation de données à caractère personnel sans délai, et au maximum dans un délai de 48 heures, après en avoir pris connaissance.

Cette notification est accompagnée de toute documentation utile afin de permettre au Responsable de traitement, si nécessaire, de notifier cette Violation à l’Autorité de contrôle compétente et a minima les informations suivantes :

- la description de la nature de la Violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la Violation et les catégories et le nombre approximatif d’enregistrements de données à caractère personnel concernés ;
- la description des conséquences probables de la Violation de données à caractère personnel ;
- la description des mesures prises ou que le Sous-traitant propose de prendre pour remédier à la Violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Le Sous-traitant coordonnera ses actions de communication externe avec le Responsable de traitement et s’interdit toute communication unilatérale et/ou spontanée, publique ou privée, notamment auprès de l’autorité de contrôle compétente et des personnes concernées, sans l’accord préalable du Responsable de traitement.

A l’issue de la clôture de l’incident ayant entraîné la Violation de données, le Sous-traitant présentera un bilan détaillé au Responsable de traitement faisant figurer notamment :

- les causes de la Violation de données,
- les atteintes portées aux données à caractère personnel, et notamment à la confidentialité et à l’intégrité des données,
- le délai de réaction et d’intervention du Sous-traitant
- les mesures prises afin de faire cesser la Violation et celles visant à ce que cette Violation ne se reproduise plus.

En cas de récurrence d’incidents et/ou compte tenu de la gravité d’un seul incident imputable(s) au Sous-traitant entraînant la Violation de données à caractère personnel dans un environnement de production, le Responsable de traitement sera en droit de procéder à la résiliation anticipée du Contrat ou de la Convention par lettre

recommandée avec accusé réception aux torts exclusifs du Sous-traitant sans indemnité et sans préjudice des éventuels dommages et intérêts qui pourraient être demandés par le Responsable de traitement.

10. Analyses d'impact (PIA)

Compte tenu de la nature du traitement concerné et des informations à sa disposition, le Sous-traitant conseillera le Responsable de traitement et l'assistera diligemment en lui fournissant les informations nécessaires à la réalisation de toute Analyse d'impact relative à la protection des données (PIA).

11. Mesures de sécurité

Le Sous-traitant s'engage à mettre en œuvre les mesures de sécurité techniques et organisationnelles nécessaires pour permettre de s'assurer que les données qui lui sont confiées ne soient ni déformées, ni endommagées, ni communiquées à des personnes non autorisées, telles que listées à l'Article VII.

Le Sous-traitant s'engage à mettre en œuvre des mesures de sécurité techniques et organisationnelles a minima équivalentes à celles développées par la CNIL ou l'ANSSI dans les guides énumérés ci-dessous ou la norme ISO 270001.

Les guides publiés par la CNIL et l'ANSSI sont accessibles aux adresses suivantes :

- https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles
- https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

En tout état de cause, le Sous-traitant s'engage, en cas de changement des moyens visant à assurer la sécurité des données et des documents transmis, à les remplacer par des moyens équivalents ou supérieurs et à en informer le Responsable de traitement en temps utile.

12. Propriété et sort des données

Les données confiées au Sous-traitant par le Responsable de traitement en vertu du Contrat ou de la Convention restent sa propriété. En aucun cas le Sous-traitant ne peut revendiquer un droit sur ces données, ni, directement ou indirectement, les utiliser, les modifier ou les détruire sans instruction expresse du Responsable de traitement.

Au terme du Contrat ou de la Convention, le Sous-traitant devra, dans les meilleurs délais, spontanément et à charge pour lui d'en justifier à première demande du Responsable de traitement :

- restituer au Responsable de traitement les données n'étant pas en la possession de ce dernier ;
- détruire les autres données.

En tout état de cause, le Sous-traitant procèdera à la destruction de toutes les copies existantes des données qui lui sont confiées dans ses systèmes d'information et ceux de ses sous-traitants ultérieurs et communiquer au Responsable de traitement une attestation d'exécution, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des données à caractère personnel.

13. Localisation

Le Sous-traitant communiquera au Responsable de traitement la localisation physique de ses serveurs via l'Article VII, de même que toute modification de ladite localisation. Cette information s'applique dès que le Sous-traitant prend la décision de modifier le lieu d'hébergement des serveurs, sans attendre leur déménagement effectif.

Toute localisation des serveurs dans un pays n'appartenant pas à l'Union européenne et non reconnu par les autorités nationales comme disposant d'un niveau de protection suffisant devra faire l'objet d'un accord préalable et écrit du Responsable de traitement. En cas de désaccord, le Responsable de traitement sera en droit de procéder à la résiliation du Contrat ou de la Convention dans les conditions prévues au Contrat ou dans la Convention.

Tout transfert autorisé par le Responsable de traitement ne pourra intervenir qu'après signature par les Parties des clauses types de la Commission européenne telles que définies dans la « décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil », ou dans une décision plus récente de la Commission.

Dans un tel cas, le Responsable de traitement sera considéré comme l'Exportateur et le Sous-traitant comme l'Importateur.

14. Registre des catégories d'activités de traitement

Le cas échéant, le Sous-traitant s'engage à tenir par écrit un Registre de toutes les catégories d'activités de traitement effectuées pour le compte du Responsable de traitement comprenant :

- le nom et les coordonnées du responsable de traitement pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données;
- les catégories de traitements effectués pour le compte du Responsable de traitement;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées;
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
- la pseudonymisation et le chiffrement des données à caractère personnel ;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

15. Documentation, vérifications et audits

15.1 Le Sous-traitant met à la disposition du Responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations et s'engage à mener régulièrement sur l'ensemble de ses systèmes d'information, ses procédures internes et ses locaux des audits pour vérifier notamment le respect de l'ensemble des obligations à sa charge au titre de la présente annexe ainsi que de la Règlementation applicable et notamment de s'assurer que les mesures de sécurité prévues par les présentes clauses sont bien mises en place et ne peuvent être contournées sans que cela ne soit détecté et notifié.

A ce titre, le Sous-traitant communiquera sur demande au Responsable de traitement les conclusions du rapport d'audit mené par ses soins ou tout prestataire de son choix soumis à une obligation de confidentialité conforme aux conditions fixées au présent Contrat ou à la présente Convention et non-concurrent du Responsable de traitement et/ou de ses sous-traitant, dont l'identité sera communiquée au Responsable de traitement au minimum dix (10) jours avant la tenue de l'audit.

En cas de constat avéré de non-conformité, le Sous-traitant prendra à sa charge les moyens nécessaires à la mise en conformité dans des délais raisonnables convenus entre les Parties. A l'issue de sa mise en conformité, le Sous-traitant fournira au Responsable de traitement une attestation d'exécution démontrant sa mise en conformité.

A défaut de respect des dispositions du présent article, le Responsable de traitement sera en droit de résilier le Contrat ou la Convention aux torts exclusifs du Sous-traitant sans préavis, ni indemnité et sans préjudice de toute réclamation du Responsable de traitement en cas de préjudice pour lui en résultant.

15.2 Le Sous-traitant reconnait que l'Autorité de contrôle (CNIL) ainsi que les Agents de la DGCCRF ont le droit d'effectuer des vérifications chez le Sous-traitant et chez tout sous-traitant ultérieur dans la même mesure et dans les mêmes conditions qu'en cas de vérifications opérées chez le Responsable de traitement conformément à la Règlementation applicable.

Le Sous-traitant informe le Responsable de traitement, dans les meilleurs délais, de l'existence d'une législation le concernant ou concernant tout sous-traitant ultérieur faisant obstacle à ce que des vérifications soient effectuées chez lui ou chez tout Sous-traitant conformément au paragraphe précédent. Dans ce cas, le Responsable de traitement se réserve le droit de suspendre le traitement de données et/ou de résilier immédiatement sans frais le Contrat ou la Convention.

III. Obligations du Responsable de traitement vis-à-vis du Sous-traitant

Le Responsable de traitement s'engage à :

1. fournir au Sous-traitant les informations prévues à l'Article VII de la présente annexe.

2. documenter par écrit toute instruction concernant le traitement des données à caractère personnel par le Sous-traitant

3. veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le RGPD de la part du Sous-traitant

4. superviser le traitement, y compris réaliser les vérifications et audits prévues à l'article II de la présente annexe auprès du Sous-traitant.

IV. Responsabilité

Nonobstant toute stipulation contraire prévue au Contrat ou à la Convention, les Parties reconnaissent que tout manquement à la présente annexe constitue des dommages directs et indemnisables, engageant la responsabilité du Sous-traitant en cas de manquement de sa part et/ou de tout sous-traitant ultérieur.

En conséquence, le Sous-traitant garantit le Responsable de traitement et le tiendra indemne de toute conséquence financière (condamnation ou indemnisation versée, frais et dépens) ayant pour cause la violation des règles prévues à la présente annexe par le Sous-traitant ou ses sous-traitants ultérieurs, sans limitation.

V. Dispositions générales

1. La présente annexe fait partie intégrante du Contrat ou de la Convention et s'impose aux Parties.

2. Les termes comportant une majuscule et non définis dans la présente annexe trouvent leur définition dans le RGPD.

3. Le fait par une des Parties de ne pas exiger à un moment quelconque l'exécution stricte par l'autre Partie d'une disposition de la présente annexe n'est en aucun cas réputé constituer une renonciation, quelle qu'elle soit, à l'exécution de celle-ci.

4. Dans le cas d'une évolution de la législation concernant les données à caractère personnel, les Parties négocieront de bonne foi toute modification de la présente annexe nécessaire à la mise en conformité, dans des délais raisonnables définis d'un commun accord.

VI. DESCRIPTION DU(DES) TRAITEMENT(S) DE DONNEES A CARACTERE PERSONNEL OBJET DE LA SOUS-TRAITANCE

1. La nature des opérations réalisées sur les données dans ce cadre est définie ci-après :
   - Hébergement
   - ~~Opérations de gestion de la relation clients et du service après-vente~~
   - ~~Opérations de gestion des opérations promotionnelles et jeux concours~~
   - ~~Opérations marketing~~
   - ~~Opérations de gestion des ressources humaines~~
   - ~~Opérations de gestion de la paie~~
   - ~~Enrichissement des bases de données~~
   - Fourniture d'un service en mode SaaS
   - ~~Développement et test des applications & logiciels~~
   - Archivage des données
   - ~~Destruction de documents~~
   - Réalisation de statistiques
2. La ou les finalité(s) du traitement sont les suivantes :
   - ~~Gestion électronique de documents~~
   - ~~Gestion des clients / prospects~~
   - ~~Gestion des opérations promotionnelles et jeux concours~~
   - ~~Gestion d'un site e-commerce~~
   - ~~Gestion des réclamations et du service après-vente~~
   - ~~Mesure de la satisfaction~~
   - ~~Gestion et traitement du courrier~~
   - ~~Gestion des ressources humaines~~
   - Réalisation de statistiques
   - ~~Archivage à des fins probatoires~~
3. Les données à caractère personnel traitées sont définies ci-après :
   - Données d'identification : état civil, email
   - Vie professionnelle : poste
   - ~~Situation familiale & sociale~~
   - ~~Données bancaires ou relatives aux moyens de paiement~~
   - ~~Vie personnelle, habitudes de vie, préférencesNuméro de sécurité sociale~~
   - ~~Adresse IP~~
   - ~~Géolocalisation~~
   - X Données de connexion
   - ~~Données biométriques~~
   - ~~Données sensibles (de santé, raciale, opinions politiques, religion, condamnation judiciaire)~~
4. Les catégories de personnes concernées sont définies ci-après.
   - Salariés
   - ~~Clients~~
   - ~~Fournisseurs~~
   - ~~Partenaires commerciaux~~
   - ~~Prestataires de service~~
   - Autres : statut d'étudiant

5. Pour l’exécution du service objet du Contrat ou de la Convention, le Sous-traitant met en œuvre les mesures de sécurité techniques et organisationnelles suivantes :
   - ~~la pseudonymisation et le chiffrement des données à caractère personnel~~
   - les moyens permettant de garantir la confidentialité, l’intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
   - les moyens permettant de rétablir la disponibilité des données à caractère personnel et l’accès à celles-ci dans des délais appropriés en cas d’incident physique ou technique;
   - une procédure visant à tester, à analyser et à évaluer régulièrement l’efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement
6. Les données à caractère personnel sont hébergées : OVH Roubaix, OVH Gravelines, OVH Strasbourg