Specimen

Clauses contractuelles de sous-traitance

RGPD

[Nom de l'entreprise]
[Raison sociale] au capital social de **[Somme du capital]** euros, inscrite au RCS [Adresse du registre du commerce] [n°], dont le siège social est sis [Adresse du siège social], représentée par [Nom et prénom], agissant en sa qualité de responsable technique et DPO, dûment habilité à l'effet des présentes.

Ci-après dénommée le **« LE RESPONSABLE DE TRAITEMENT ».**

D'une part,

ET

Wexample Labs
Société **Association de loi de type 1901**, sous le numéro 838 910 859 00019, dont le siège social est sis 17 rue Porte de Crouy 02200 Soissons, représentée par Carole Lavocat agissant en sa qualité de cheffe de projet et DPO dûment habilité à l'effet des présentes.

Ci-après dénommée **« le SOUS-TRAITANT ».**

D'autre part,

I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (ci-après, « le règlement européen sur la protection des données »).

II. Description du traitement faisant l'objet de la sous-traitance

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les services suivants :

- **[développement et maintenance des applicatifs des sites web]...**

La nature des opérations réalisées sur les données est réservée aux environnements de test local et pré-production.

Les finalités du traitement sont recensées dans un registre des données disponible lu et disponible à tout moment par les développeurs et mis à jour par les DPO côté client et prestataire.

Les données à caractère personnel traitées ne servent uniquement au bon fonctionnement du ou des sites web en question.

Les catégories de personnes concernées sont **[description de la population]**.

Pour l'exécution du service objet du présent contrat, le responsable de traitement met à la disposition du sous-traitant les informations nécessaires suivantes :

- le registre des personnes qui travaillent sur le projet,
- le registre du traitement des données,
- les clauses de confidentialité et RGPD.

III. Durée du contrat

Le présent contrat entre en vigueur à compter du **[date]** pour une durée de un an.

IV. 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 ;

2. traiter les données conformément aux instructions documentées du responsable de traitement figurant en annexe du présent contrat. Si le sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des États membres relative à la protection des données, il en informe immédiatement le responsable de traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public ;

3. garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat ;

4. veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :

    a. s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
    b. reçoivent la formation nécessaire 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 :
   Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le responsable de traitement dispose d'un délai minimum de une semaine à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

7. Droit d'information des personnes concernées

Le sous-traitant, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'il réalise. La formulation et le format de l'information doit être convenue avec le responsable de traitement avant la collecte de données.

8. Exercice des droits des personnes
   Le sous-traitant doit répondre, au nom et pour le compte du responsable de traitement et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d'exercice de leurs droits, s'agissant des données faisant l'objet de la sous-traitance prévue par le présent contrat.

9. Notification des violations de données à caractère personnel
   Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 24 heures après en avoir pris connaissance et par le moyen suivant **[email du responsable du traitement]**. 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.

Option possible
Après accord du responsable de traitement, le sous-traitant notifie à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte du responsable de traitement, les violations de données à caractère personnel dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.
La notification contient au moins :

- 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 ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- la description des conséquences probables de la violation de données à caractère personnel ;
- la description des mesures prises ou que le responsable du traitement 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.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu.

Après accord du responsable de traitement, le sous-traitant communique, au nom et pour le compte du responsable de traitement, la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et contient au moins :

- 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 ;

- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

- la description des conséquences probables de la violation de données à caractère personnel ;

- la description des mesures prises ou que le responsable du traitement 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.

10. Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations.

Le sous-traitant aide le responsable de traitement
- pour la réalisation d'analyses d'impact relative à la protection des données.
- pour la réalisation de la consultation préalable de l'autorité de contrôle.

11. Mesures de sécurité
Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité suivantes :

Mesures organisationnelles :
- le développeur a pris connaissance de l'évolution de la réglementation RGPD Européenne et s'engage à la respecter ;
- le développeur se doit d'informer le DPO des évolutions du traitement des données personnelles ;
- penser et développer l'ensemble de l'applicatif selon la nouvelle réglementation RGPD ;
- le développeur s'engage à ne pas divulguer des informations personnelles issues des bases de données des applicatifs de **[nom du client] ;**
- les bases de données installées en local sont systématiquement effacées lorsque le développeur sort du projet.

Mesures techniques de sécurités des données personnelles :
- le mot de passe des bases de données installées en local est protégé,
- SSH mis en place pour les sites en production,
- FTP ouvert que pour les sites qui en ont besoin,
- sauvegardes BDD en local,
- le développeur s'engage à installer les BDD uniquement sur son ordinateur de travail qui sera protégé par un antivirus.

Mesures techniques de sécurités structurelles :

- Le WiFi de notre réseau d'entreprise est protégé par un mot de passe.
- Un logiciel de prévention des fuites est utilisé pour protéger les données personnelles et sensibles.

- Utilisation de mots de passe complexes.

12. Sort des données
Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à détruire toutes les données à caractère personnel.

13. Délégué à la protection des données
Le délégué à la protection des données de Wexample Labs est Carole Lavocat, carole.lavocat@wexample.com.

14. Registre des catégories d'activités de traitement
Le sous-traitant déclare 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 du 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 constante 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
Le sous-traitant met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

V. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s'engage à :

1. fournir au sous-traitant les données visées au II des présentes clauses ;
2. documenter par écrit toute instruction concernant le traitement des données par le sous-traitant ;
3. veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du sous-traitant ;
4. superviser le traitement, y compris réaliser les audits et les inspections auprès du sous-traitant.

(Source du document : la CNIL).

Signature datée et accompagnée de la mention "lu et approuvée" :