



**TP**PLANNING

**AG PROGICIELS**

**POLITIQUE DE TRAITEMENT DES DONNEES**

**Pour AG Progiciels**  
Alexandre Garcia  
24/05/2018

Annexe aux contrats de service conclus entre AG Progiciels et ses clients.

AG Progiciels, 23 rue Chrétien de Troyes, 91090 Lisses, représenté par Alexandre Garcia (ci-après, « *le sous-traitant* ») d'une part, et le client utilisateur des services AG Progiciels (ci-après, « *le responsable de traitement* ») 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 service(s) suivant(s) : mise à disposition des données utiles au fonctionnement de TP Planning, modules et applications associées.

Les opérations réalisées sur les données sont la collecte, l'enregistrement, la transmission, le stockage, la conservation, l'extraction, la consultation, l'utilisation.

Les finalités du traitement sont d'enregistrer et stocker les données afin d'assurer le fonctionnement du progiciel TP Planning.

Les données à caractère personnel traitées sont : nom, prénom, identifiants et mot de passe, téléphone portable, téléphone fixe, adresse, date de naissance, N° de sécurité sociale, date d'embauche, e-mail, photo, permis de conduire, CACES

Les catégories de personnes concernées sont les salariés du client ainsi que les interlocuteurs des clients et fournisseurs du client.

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

## III. Durée du contrat

Le présent contrat entre en vigueur à compter du 25 mai 2018 et est valable jusqu'à résiliation du contrat de services nous liant au client.

## IV. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

1. Traiter les données **uniquement pour les seules finalités** qui 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 Etats 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'Etat 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 :
  - S'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité
  - 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 72 heures 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.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du règlement européen sur la protection des données.

## 7. Droit d'information des personnes concernées

Il appartient au responsable de traitement de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

## 8. Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

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 72 heures après en avoir pris connaissance par e-mail. 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.

## **11. Mesures de sécurité**

Le sous-traitant via les prestations du sous-traitant ultérieur, OVH, s'engage à mettre en œuvre les mesures de sécurité suivantes :

- Des mesures de sécurité physique afin d'empêcher l'accès aux infrastructures sur lesquelles sont stockées les données du client par des personnes non autorisées
- Un personnel de sécurité chargé de veiller à la sécurité physique des locaux d'OVH 24 heures sur 24 et 7 jours sur 7
- Un système de gestion des habilitations permettant de limiter l'accès aux locaux et aux données aux seules personnes ayant besoin d'y accéder dans le cadre de leurs fonctions et de leur périmètre d'activité

- Un système d'isolation physique et/ou logique (en fonction des services) des clients entre eux
- Des processus d'authentification forts des utilisateurs et administrateurs grâce notamment à une politique stricte de gestion des mots de passe et le déploiement de certaines mesures de double authentification
- Des processus et dispositifs permettant de tracer l'ensemble des actions réalisées sur son système d'information et d'effectuer, conformément à la réglementation en vigueur, des rapports en cas d'incident affectant les données du client

Le sous-traitant via les prestations du sous-traitant ultérieur, OVH, s'engage à mettre en œuvre les mesures de sécurité prévues par *certification PCI-DSS, certification ISO/IEC 27001, attestations SOC 1 TYPE II et SOC 2 TYPE II*

## **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