

ANNEXE AUX CONTRATS ET CONDITIONS GENERALES OCTIME SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

La société OCTIME et le Client s'engagent à respecter les dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et de la loi n°2016-1321 du 7 octobre 2016 pour une République Numérique, leur incombant.

1 - PROTECTION DES DONNEES A CARACTERE PERSONNEL DU CLIENT

1.1 Finalités du traitement des données à caractère personnel du Client par la société OCTIME

Le Client accepte que la société OCTIME puisse stocker, traiter et utiliser les données à caractère personnel collectées à l'occasion de la mise en œuvre des relations contractuelles entre le Client et la société OCTIME pour les finalités listées ci-après, dans l'intérêt légitime de la société OCTIME.

En complément des finalités précisées dans le paragraphe 2.2, les données à caractère personnel du Client ne pourront être utilisées que pour les finalités suivantes :

- les contrats et conditions générales ;
- les commandes ;
- les livraisons ;
- les factures ;
- la comptabilité, et en particulier la gestion des comptes clients ;
- le suivi de la relation client tel que la réalisation d'enquêtes de satisfaction, la gestion des réclamations et du service après-vente ;
- la gestion des demandes de droit d'accès, de rectification, d'effacement, d'opposition, de limitation et de portabilité ;
- la gestion des impayés et du contentieux ;
- la gestion des avis des personnes sur des produits, services ou contenus.

A ce titre, les données à caractère personnel du Client pourront être transmises à un organisme de recouvrement ou d'affacturage.

1.2 Durée de conservation des données à caractère personnel du Client

Les données à caractère personnel du Client sont conservées tout le long de la durée des relations contractuelles liant Client et la société OCTIME.

1.3 Les droits du Client sur ses données à caractère personnel

Le Client dispose d'un droit d'accès, de rectification, d'effacement, d'opposition, de limitation et de portabilité de ses données à caractère personnel.

1.4 L'obligation de confidentialité de la société OCTIME

La société OCTIME s'engage à garder ces données confidentielles, à n'effectuer, en dehors des nécessités techniques, aucune copie des données et à n'en faire aucune utilisation autre que celles prévues pour l'exécution des relations contractuelles liant le Client et la société OCTIME.

2 - PROTECTION DES DONNEES A CARACTERE PERSONNEL TRANSMISES AUX FINS D'UTILISATION DES SERVICES APPLICATIFS

2.1 Qualité de sous-traitant du Prestataire

Au sens du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et de la loi n°2016-1321 du 7 octobre 2016 pour une République numérique, la société OCTIME est sous-traitant car il traite les données à caractère personnel que sur instruction du Client, responsable du traitement, et pour son compte. La société OCTIME ne dispose d'aucune initiative.

Le seul traitement de données à caractère personnel effectué par la société OCTIME pour son propre compte l'est à des fins statistiques : dans ce cadre, les données sont rendues anonymes de telle manière que la personne concernée ne soit plus identifiable.

Conformément à l'article 28 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), les clauses ci-après ont pour objet de définir les conditions dans lesquelles la société OCTIME, sous-traitant, s'engage à effectuer pour le compte du Client, responsable de traitement, les opérations de traitement de données à caractère personnel transmises aux fins d'utilisation des services applicatifs.

2.2 Description du traitement

La société OCTIME est autorisée à traiter pour le compte du Client les données à caractère personnel nécessaires pour fournir le service demandé par le Client à travers l'application logicielle Octime et ses dérivés (webservices, API, ...).

La nature des opérations réalisées sur les données concerne le stockage, le traitement algorithmique, et l'affichage de celles-ci suivant les besoins du Client.

2.2.1 Finalités du traitement

Les finalités du traitement sont le comptage des temps de présence et d'absence des salariés du Client, l'envoi de ces mêmes

données vers des logiciels tiers du Client, la planification des temps de travail des salariés du Client.

De plus, dans le cadre d'une prestation de support, d'installation, de configuration, de maintenance ou d'assistance, à la demande du Client, la société Octime peut :

- accéder aux données du Client ;
- analyser les données du Client, le cas échéant effectuant des correctifs sur les données ;
- transférer les données lors d'une migration d'environnement technique ;

Pour l'exécution du service objet du contrat liant le Client et la société OCTIME et de la présente Annexe, les Parties mettront à leurs dispositions respectives les informations nécessaires à la bonne utilisation de l'application logicielle Octime.

Dans le cadre du service SAAS :

- les données appartenant au Client et hébergées par la société OCTIME sont et demeurent exclusivement la propriété du Client.
- il est entendu entre les parties que la société OCTIME ne pourra pas transférer l'hébergement des données dans un autre lieu et/ou hors de L'Union Européenne sans l'accord écrit et préalable du Client.

2.2.2 Instructions du Client

Le Client demande par la présente à la Société OCTIME, au travers de son applicatif, de compter les temps de présence et d'absence des salariés du Client, d'envoyer ces mêmes données vers des logiciels tiers du Client, de lui permettre de planifier les temps de travail de ses salariés.

2.2.3 Données traitées

Les catégories de personnes concernées sont l'ensemble des effectifs du Client (salariés, agents, cadres, ...).

Les données à caractère personnel faisant l'objet d'un traitement dans le cadre de la mission effectuée pour le compte du Client sont : nom, prénom, détails des présences et absences des salariés du Client, adresse mail, identifiant, mot de passe, matricule, date d'embauche, type de contrat, planning et éventuellement badgeage (selon équipement du Client). Le Responsable de traitement s'engage à ne pas saisir dans la solution OCTIME de données dites sensibles au sens de l'article 9.1 du RGPD.

Il est précisé que les données à caractère personnel saisies dans la solution ne devront pas permettre de faire apparaître, directement ou indirectement, les origines ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes composant l'effectif du Client (salariés, agents, cadres, ...), ni des données relatives à leur santé ou à leur vie sexuelle, ni toutes autres données dont la collecte serait contraire aux lois et réglementations en vigueur. Le Client qui procédera au traitement de telles données assumera à lui

seul la pleine et entière responsabilité de ses actes, sans que la responsabilité du Sous-traitant ne puisse être engagée.

2.3 Durée du traitement

La durée du traitement des données à caractère personnel effectué par la société OCTIME pour le compte du Client est la même que celle des relations contractuelles liant le Client et la société Octime. Dans le cadre du service SAAS, la Société Octime conservera sur ses serveurs les données du client au maximum 5 ans.

2.4 Obligations de la société OCTIME

2.4.1 La société OCTIME s'engage à :

a. Fournir un progiciel de gestion des temps permettant au client de traiter les données, **conformément aux instructions du Client** décrites au paragraphe 2.2.1.

Si la société OCTIME considère qu'une instruction constitue une violation du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général 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 Client.

En outre, si la société OCTIME est tenue 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 français, il doit informer le Client de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

b. Traiter les données **uniquement pour la ou les seule(s) finalité(s)** listées à l'article 2.1

c. Garantir la **confidentialité** des données à caractère personnel traitées dans le cadre de l'utilisation des services applicatifs.

d. Assister le Client aux fins de réalisation d'une **analyse d'impact relative à la protection des données** (: AIPD), dans le cas où le niveau de risque présenté pour les droits et libertés des personnes physiques par le traitement mis en œuvre l'imposerait ;

e. Veiller à ce que les personnes **autorisées à traiter les données à caractère personnel** en vertu de la présente Annexe s'engagent à respecter la **confidentialité** ou soient soumises à une obligation légale appropriée de confidentialité et que celles-ci aient reçues la formation nécessaire en matière de protection des données à caractère personnel.

2.4.2 Appel à un sous-traitant

La société OCTIME est autorisée à faire appel, dans le cadre de la réalisation du service, à un ou plusieurs des sous-traitants dont la liste est précisée ci-après. Les sous-traitants sont tenus de respecter les obligations de la présente Annexe pour le compte et selon les instructions de la société OCTIME. A ce jour, les sous-traitants autorisés par le responsable du traitement sont :

- OVH
- SPEC
- Pyres.com

2.4.3 Mesures de sécurité

Conformément à l'article 32 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), la société OCTIME et le Client s'engagent à mettre en œuvre les mesures de sécurité suivantes :

- *Une connexion sécurisée à l'application Octime notamment via le protocole HTTPS,*
- *L'activation par défaut du module de gestion des mots de passe qui impose une complexité, une longueur minimum et un renouvellement périodique,*
- *La traçabilité par défaut de toutes les actions et événements effectués dans l'application,*
- *La pseudonymisation et le chiffrement des données à caractère personnel,*
- *La sauvegarde des bases de données,*
- *Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement,*

Cette liste pourra être complétée en fonction des besoins et des évolutions techniques apportés par la Société Octime et/ou le Client.

Le Client doit veiller au respect de ces mesures et sera tenu pour responsable de l'absence de mise en œuvre de ces mesures de sécurité. Octime recommande au Client de disposer de la version 9.2.6-0 ou de la dernière mise à jour supérieure.

2.4.4 Sort des données

Dans le cadre du service SAAS, au terme de la prestation de services relatifs au traitement de ces données, la société OCTIME s'engage à détruire toutes les données à caractère personnel. Le Client pourra solliciter d'OCTIME une justification par écrit de la destruction.

2.4.5 Exercice des droits des personnes concernées

S'agissant des données traitées en application du 1. de la présente Annexe, la société OCTIME s'engage à répondre directement à la personne concernée et dans les délais prévus par le règlement européen sur la protection des données en cas d'exercice de leurs droits.

Dans le cadre du service SAAS, OCTIME informera le Client de toute demande qu'il recevra de la part d'une personne concernée. OCTIME ne donnera pas suite à cette demande, qui incombera au Client en sa qualité de responsable du traitement.

La société OCTIME, dans la mesure du possible, aidera le Client à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées.

Dans le cadre de la mise à disposition du logiciel Octime installé dans l'environnement

informatique du client « On Premise », les personnes concernées exerceront directement auprès du Client des demandes d'exercice de leurs droits.

2.4.6 Notification des violations de données à caractère personnel

La société OCTIME aide le Client à lui permettre de réaliser une notification de violation de données à caractère personnel auprès de la CNIL et de la personne concernée.

Pour ce faire, conformément à l'article 33 2. du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), la société OCTIME notifie au Client toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

Cette notification, adressée par courriel au DPO du Client ou à la personne identifiée par OCTIME comme étant en charge du sujet RGPD pour le Client, est accompagnée de la documentation utile au Client pour que ce dernier notifie la violation de données à caractère personnel à la CNIL et à la personne concernée, s'il le juge nécessaire.

2.4.7 Localisation

Dans le cadre du service SAAS, la société OCTIME s'engage à informer le Client, sur demande, de la localisation des données et plus généralement à communiquer les informations utiles et nécessaires pour réaliser les déclarations.

Il est précisé en tant que de besoin qu'au jour de la diffusion de la présente Annexe, les données sont hébergées en France ou dans un pays de l'Union Européenne.

2.5 Qualité de responsable de traitement du Client

Au sens du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et de la loi n°2016-1321 du 7 octobre 2016 pour une République numérique, le Client est le responsable du traitement des données à caractère personnel utilisées pour mettre en œuvre les services applicatifs **car le Client décide les finalités et détermine les moyens du traitement des données à caractère personnel.**

Les données transmises aux fins d'utilisation des services applicatifs comportant des données à caractère personnel, le Client garantit au Prestataire qu'il a procédé à l'ensemble des obligations lui incombant aux termes du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des

données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et de la loi n°2016-1321 du 7 octobre 2016 pour une République numérique.

2.6 Obligations du Client

2.6.1 Obligation de fourniture de données, de documentation, de respect du règlement (UE) 2016/679 et de supervision du Client

Le Client s'engage à :

- fournir à la société OCTIME les données visées à l'article 2.2 de la présente Annexe
- documenter par écrit toute instruction concernant le traitement des données par la société OCTIME
- veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) de la part du Prestataire
- superviser le traitement, y compris réaliser les audits et les inspections à sa charge financière auprès de la société OCTIME.
- Ne pas saisir dans l'application OCTIME des données autres que celles nécessaires au bon fonctionnement de l'application.
- Informer les personnes concernées du traitement de leurs données, en application de l'article 13 du RGPD et disposer du consentement explicite des personnes dont les données personnelles ont été recueillies.

2.6.2 Obligations et mesures de sécurité

Le Client est responsable de la sécurité des données à caractère personnel.

Conformément à l'article 32 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), le Client et la société OCTIME s'engagent à mettre en œuvre les mesures de sécurité suivantes :

- Une connexion sécurisée à l'application Octime notamment via le protocole HTTPS,
- L'activation par défaut du module de gestion des mots de passe qui impose une complexité, ne longeur minimum et un renouvellement périodique,
- La traçabilité par défaut de toutes les actions et événements effectués dans l'application,
- La pseudonymisation et le chiffrement des données à caractère personnel,
- La sauvegarde des bases de données,
- Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des

mesures techniques et organisationnelles pour assurer la sécurité du traitement,

☞ Cette liste pourra être complétée en fonction des besoins et des évolutions techniques apportés par la Société Octime et/ou le Client.

☞ Le Client doit veiller au respect de ces mesures et sera tenu pour responsable de l'absence de mise en œuvre de ces mesures de sécurité.

2.6.3 Notification des violations de données à caractère personnel

Le Client notifie à la CNIL 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 Client 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.

Le Client communique 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 Client 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.

2.6.4 Délégué à la protection des données et tenue du Registre des traitements

Le Client communique à OCTIME le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données. Pour Octime, les coordonnées du DPO sont :

par mail : dpo@octime.com

par courrier : DPO Octime, 2 Allée de l'Innovation 64300 BIRON

Les parties déclarent tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées comprenant :

- ☑ le nom et les coordonnées, le cas échéant, du délégué à la protection des données;
- ☑ les catégories de traitements effectués;
- ☑ 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.

2.6.5 Obligation d'information des personnes concernées

Le Client a l'obligation d'informer les personnes concernées des opérations de traitement sur leurs données à caractère personnel au moment de la collecte des données.

2.6.6 Garanties du Client

Le Client garantit la société OCTIME contre tout recours, plainte ou réclamation émanant d'une personne physique dont les données à caractère personnel seraient reproduites et hébergées via le service applicatif.■