Règlement Général pour la Protection des Données

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).

Open Bee™ - Description de la mise en œuvre du RGPD pour les services Cloud Open Bee™

Open Bee™

Vous trouverez dans le présent document une description des procédures et moyens techniques qui sont mis en œuvre dans les services Cloud d'Open Bee™ pour être en conformité avec le Règlement UE - 2016/679 du Parlement européen et du Conseil du 27 avril 2016 sur la protection des personnes physiques à l'égard du traitement des Données à Caractère Personnel et des règles relatives à la libre circulation de ces données (le "**Règlement Européen**").

Il est de votre responsabilité d'appliquer en interne une politique de protection des Données à Caractère Personnel afin de vous conformer au Règlement Européen. Vous devez notamment créer et maintenir à jour un registre des traitements de Données à Caractère Personnel. Aucune déclaration particulière n'est effectuée par Open Bee™ au titre de ses activités de collecte et de traitement pour votre compte dans la mesure où vous êtes seul juridiquement responsable du traitement des Données à Caractère Personnel collectées pour votre compte, traitement sur lequel Open Bee™ ne peut disposer d'un contrôle effectif.

Si vous souhaitez obtenir plus d'informations sur le Règlement Européen, vous pouvez consulter les contenus suivants :

- Le contenu de ce règlement :
  http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

- Des explications et des conseils :
  https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels

- La mise en conformité :
  https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes

Sommaire

I Introduction

Open Bee™ est amené dans le cadre de l'utilisation des logiciels Open Bee™ et des services y afférents, à collecter des Données à Caractère Personnel au nom et pour votre compte, Open Bee™ agissant alors comme un sous-traitant, c'est-à-dire comme une personne morale extérieure traitant des Données à Caractère Personnel selon les instructions et sous l'autorité du responsable du traitement, à savoir, vous. On entend par **Données à Caractère Personnel** : « toute information se rapportant à une personne physique identifiée ou identifiable, toute donnée permettant d'identifier une personne physique, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

Les Données à Caractère Personnel collectées restent sous votre responsabilité exclusive.

Ce document fournit des éléments concernant la sécurité des systèmes, aussi bien physique que logicielle, qui permettent d'assurer la confidentialité, la disponibilité et l'intégrité des Données à Caractère Personnel.

Open Bee™ a désigné un DPO (Data Protection Officer) afin d'appliquer, en interne, le Règlement Européen pour les Données à Caractère Personnel. Les coordonnées du DPO figurent ci-après en Annexe 1.

La protection des Données Personnelles collectées et le respect de la vie privée des utilisateurs des logiciels et services Open Bee™ sont au cœur des préoccupations d'Open Bee™. Open Bee™ s'engage par conséquent à déployer, tout au long de la chaîne de collecte, d'hébergement, de traitement et de circulation des documents et des données qui lui sont confiés, les moyens techniques et organisationnels nécessaires à cette protection et à ce respect, ainsi qu'à ne travailler qu'avec des acteurs qui déploient des moyens équivalents et qui adhèrent eux-mêmes au Règlement, conformément aux engagements ci-après.

II Contrôles et sûreté des accès aux logiciels et aux services

Les contrôles d'accès aux logiciels et aux services Open Bee™ comportent un ensemble de vérifications possibles que vous pouvez paramétrer :

- Identification unique des utilisateurs ;
- Activation et désactivation des comptes utilisateurs par l'administrateur ;
- Complexité et longueur minimum des mots de passe imposés aux utilisateurs ;
- Blocage des accès après un certain nombre de tentatives infructueuses ;
- Arrêt automatique des sessions après un certain temps d'inactivité de l'utilisateur ;
- Possibilité d'utiliser des certificats de SSL pour l'accès à l'URL des sites ;
- Possibilité d'utiliser un second facteur d'authentification.

De plus, Open Bee™ a mis en place des outils pour limiter le risque de divulgation des mots de passe utilisés pour accéder aux logiciels et aux services Open Bee™ :

- Hachage[1] et salage[2] pour leur stockage ;
- Aucune transmission d'information en clair ;
- Pas de journalisation des éléments d'identification.

Enfin, pour certains services, les utilisateurs des logiciels Open Bee™ peuvent s'authentifier par l'intermédiaire d'une application tierce du type SSO afin d'éviter la ressaisie de leurs identifiants.

III Ségrégation des données et des documents

Les logiciels Open Bee™ sont conçus de telle façon qu'ils isolent les données et les documents de tout utilisateur. L'architecture technique installée et exploitée fournit une séparation fiable entre toutes les informations contenues dans ces systèmes.

Par ailleurs, Open Bee™ dispose de plusieurs environnements (tests et production), ainsi que des procédures pour la mise en place des nouvelles versions de ses logiciels et la création de nouveaux clients qui assurent l'étanchéité entre les différents clients et qui ne permettent, en aucun cas, la divulgation de documents confidentiels.

---

[1] Hash : Séquence de caractères alphanumériques de longueur fixe, qui représente le contenu d'un message ou d'un fichier, sans le révéler, dont la valeur unique est produite par un algorithme de **hachage**.
[2] Salage : Le salage est une méthode cryptographique permettant de renforcer la sécurité des informations qui sont destinées à être hachées (par exemple des mots de passe) en y ajoutant une donnée supplémentaire afin d'empêcher que deux informations identiques ne conduisent au même Hash.

IV Politique de sécurité et procédures

Une politique de sécurité des systèmes informatiques (PSSI) a été mise en place. Open Bee™ est en phase de mise en conformité par rapport à la norme ISO 27001 (Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences) afin de disposer d'une gouvernance de la sécurité de ses systèmes d'information.

V Journalisation des opérations

Toutes les actions sur les dispositifs d'Open Bee™ sont journalisées. Cette journalisation est réalisée à deux niveaux :

- D'une part, au niveau global pour tous les équipements de connexion et les serveurs ;
- Et, d'autre part, au niveau des documents où toutes les actions sur ceux-ci sont tracées dans un journal sécurisé et dont l'intégrité est assurée par des mécanismes cryptographiques.

Le journal est conçu de telle façon qu'il ne contient aucune Donnée à Caractère Personnel. Cela permet d'assurer aux utilisateurs du logiciel Open Bee™ que, lors de la suppression d'un document, rien ne subsiste dans les serveurs Open Bee™, excepté son hash, qui ne peut en aucun cas être utilisé pour reconstituer le document détruit.

VI Gestion des incidents

Open Bee™ a mis en place des procédures de gestion des incidents de sécurité. Open Bee™ vous informe en cas d'une divulgation non autorisée des Données à Caractère Personnel dans les plus brefs délais. Cela permet aux clients d'Open Bee™ de réaliser leurs déclarations à la CNIL et d'avertir, le plus rapidement possible, toutes les personnes concernées. Cette information vous sera notifiée par courrier électronique confirmé par lettre recommandée avec accusé de réception. Cette notification sera accompagnée de toute documentation utile afin de vous permettre, si nécessaire, de notifier cette violation à l'Autorité de Contrôle compétente.

VII Hébergement des données

Open Bee™ sous-traite ses activités d'hébergement de données à la société Orange. Les coordonnées de ce sous-traitant et la date du contrat qui le lie à Open Bee™ figure en Annexe 2 ci-après. Le centre d'hébergement de la société Orange utilisé par Open Bee™ est équivalent Tier IV[3], situé en France et certifié ISO 27001, ce qui assure un haut niveau de sécurité et donc de confidentialité.

Les centres de traitement de production utilisés par Open Bee™ pour fournir ses services d'hébergement disposent de contrôles d'accès. Ces contrôles ne permettent qu'aux personnels autorisés d'avoir accès aux zones protégées.

Les équipements sont dans des salles sécurisées prévues pour résister à des intrusions malveillantes et à des variations de conditions climatiques. Des générateurs électriques de secours sont disponibles, avec une réserve de carburant permettant de répondre à une perte d'alimentation électrique de longue durée.

Des détecteurs de présence sont également mis en œuvre à l'intérieur des locaux pour prévenir toute intrusion.

Open Bee™ vous informera préalablement et par écrit de tout changement envisagé concernant l'ajout ou le remplacement de sous-traitants auxquels Open Bee™ peut faire appel. Cette information indiquera clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Vous disposerez d'un délai minimum de trente (30) jours à compter de la date de réception de cette information pour présenter vos objections. En cas d'objections, vous devrez adresser à Open Bee™ - avant l'expiration du délai de trente (30) jours et de la prise d'effet de l'ajout ou du remplacement d'un sous-traitant - une lettre recommandée avec accusé de réception, prononçant la résiliation du ou des licences et services Open Bee™ concernés par l'ajout ou le remplacement du sous-traitant. Cette résiliation prendra alors effet à compter de l'expiration du délai de trente (30) jours précité. Vous supporterez alors les conséquences éventuelles de cette résiliation anticipée prévues par le contrat ou la licence que vous avez souscrit. A défaut de notification de résiliation adressée à Open Bee™ avant l'expiration du délai de trente (30) jours précité, vous serez réputé avoir irrévocablement accepté l'ajout ou le remplacement de sous-traitants.

Tout sous-traitant d'Open Bee™ est tenu de respecter les obligations du présent règlement. Il appartient à Open Bee™ de s'assurer que le sous-traitant 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. Open Bee™ demeure pleinement responsable devant vous de l'exécution par le sous-traitant de ses obligations.

[3] Définition des niveaux de certification «Tier» : https://uptimeinstitute.com/tier-certification

VIII Composant coffre-fort numérique

Open Bee™ Portal est certifié NF Logiciel 203 Composant Coffre-Fort Numérique. Cela signifie que la solution se conforme aux exigences de la norme AFNOR NF Z42-020 qui définit les spécifications fonctionnelles d'un composant Coffre-Fort Numérique destiné à la conservation d'informations numériques dans des conditions de nature à en garantir leur intégrité dans le temps.

IX Fiabilité et copies des données

Tous les composants du système d'archivage sont redondés. Les données et documents clients sont stockés sur un serveur primaire. Ces données et documents sont copiés sur un site secondaire qui peut prendre le relais du site primaire en cas de défaillance de celui-ci.

X Plan de reprise d'activité

Open Bee™ dispose d'un Plan de Reprise des Activités (PRA) afin de pouvoir redémarrer ses activités d'hébergement le plus efficacement possible. Des procédures de restauration des données et des documents endommagés ou perdus prévoient toutes les étapes nécessaires de la détermination de l'ampleur de l'incident jusqu'au contrôle de l'intégrité des données en passant par la configuration de nouvelles machines si nécessaire.

Des tests de ce PRA sont effectués régulièrement afin de vérifier son efficacité.

XI Virus

Open Bee™ a mis en place des moyens de détection des virus grâce à des logiciels spécialisés. Ces outils sont mis à jour très régulièrement afin d'être toujours les plus performants possibles.

XII Chiffrement des données

Open Bee™ utilise des moyens cryptographiques à la fois lors de la connexion aux serveurs ainsi que lors des transferts des documents, tels que TLS 1.2, certificats SHA256 avec chiffrement RSA 2048. Les documents stockés dans des coffres forts électroniques sont chiffrés en AES 256 bits.

Open Bee™ suit les recommandations de l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information) dans ce domaine. Pour plus de détails, consultez : http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/.

XIII Accès et suppression des Données à Caractère Personnel

Grâce aux technologies d'indexation et de reconnaissances de caractères des solutions Open Bee™ et à son moteur de recherche avancé, il est possible d'opérer à la recherche/suppression de documents, garantissant une mise en conformité efficace pour ces aspects du Règlement. Cela permet, notamment, de supprimer des documents à la demande des possesseurs de données ou de l'Autorité de Contrôle.

XIV Réversibilité

Pendant toute la durée du contrat d'hébergement, vous pouvez exporter des copies de n'importe quelle Donnée à Caractère Personnel (document ou dossier) ainsi que les métadonnées associées. Dans les trente (30) jours après la demande d'arrêt d'une licence de logiciel et/ou d'un contrat de service Open Bee™, vous pouvez demander le retour de la totalité des Données à Caractère Personnel de vos utilisateurs (documents et métadonnées associées). Cette restitution se fait via des canaux sécurisés et dans des formats de fichier qui auront été définis préalablement à cette restitution.

A l'issue de cette restitution et après votre accord, toutes les données et documents sur les serveurs Open Bee™ sont détruits. A défaut d'accord de votre part, toute Donnée à Caractère Personnel sera détruite trois (3) mois après la date de restitution susmentionnée. Open Bee™ s'engage à vous aider, dans la mesure du possible et aux tarifs éventuellement prévus par votre contrat, à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des utilisateurs : 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).

XV Exercice des droits des utilisateurs

Lorsque qu'un utilisateur concerné exerce auprès de vous des demandes d'exercice de ses droits et que cette demande implique une ou plusieurs actions de la part d'Open Bee™, celle-ci mettra en œuvre les moyens pour répondre à ces demandes et vous adressera un compte rendu de ses actions par courrier électronique.

Open Bee™ vous aidera, aux tarifs éventuellement prévus par votre contrat, pour la réalisation d'analyses d'impact relatives à la protection des Données à Caractère Personnel des utilisateurs (PIA). Open Bee™ vous aidera pour la réalisation d'éventuelles consultations préalables de l'Autorité de Contrôle.

Les règles de classement et métadonnées qu'il est possible de mettre en œuvre avec la solution Open Bee™ Portal vous permettent de cartographier les Données à Caractère Personnel stockées et ce, afin de pouvoir permettre à vos utilisateurs d'exercer leurs droits (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-).

Open Bee™ s'engage à réaliser les demandes de droit à l'effacement des utilisateurs dans un délai de six (6) mois à compter de la date de réception de ces demandes.

XVI Obligations d'Open Bee™ en tant que sous-traitant

Audit

Open Bee™ s'engage à mettre à votre disposition la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par un auditeur que vous aurez mandaté et contribuer à ces audits.

Vous pourrez donc, à vos frais, vous faire assister par tout Auditeur désigné par vous, sous réserve que celui-ci présente les qualifications nécessaires et n'exerce pas lui-même une activité directement ou indirectement concurrente de l'activité d'Open Bee™, ni ne soit lié à une société exerçant directement ou indirectement l'activité d'Open Bee™, ait, préalablement à l'audit, accepté par écrit d'être soumis à l'obligation de confidentialité visée par le contrat de service Open Bee™ et ait remis une déclaration d'absence de conflit d'intérêts. Open Bee™ pourra récuser l'Auditeur désigné sur motif justifié, sans préjudice alors de votre droit de désigner un autre Auditeur dans les conditions ci-dessus.

Vous êtes limité à un audit par année.

L'audit devra être demandé par écrit avec un préavis de quinze (15) jours.

L'audit devra respecter des dispositions et méthodologies fixées par la délibération n° 2011-316 du 6 octobre 2011 de la CNIL, portant adoption d'un référentiel pour la délivrance de labels en matière de procédure d'audit tendant à la protection des personnes à l'égard du traitement des Données à Caractère Personnel.

Registre des données traitées

Open Bee™ s'engage à tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour votre compte comprenant :

- Le nom et les coordonnées du responsable de traitement pour le compte duquel Open Bee™ agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;
- Les catégories de traitements effectués pour votre compte ;
- 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, 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 : (i) l'anonymisation et/ou le chiffrement des données ou des documents ; (ii) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ; (iii) 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'incidents physiques ou techniques ; (iv) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Obligation de confidentialité du personnel Open Bee™

Les personnes chez Open Bee™ qui traitent les données des clients sont soumises à une obligation de confidentialité.

XVII Vos obligations en tant que responsable du traitement

Vous déclarez :

- Qu'aucune collecte ni aucun traitement de Données à Caractère Personnel ne sera confié à Open Bee™ en l'absence de l'inscription dans votre registre de traitements des Données à Caractère Personnel et dans lequel vous aurez attesté de la licéité du traitement ;
- Que la finalité du traitement des Données à Caractère Personnel confié à Open Bee™ est déterminée, explicite et légitime.
- Que le consentement des utilisateurs de vos services, qu'Open Bee™ héberge, a été recueilli, sur la base d'un document présentant vos services de façon claire et explicite.

Vous vous engagez par ailleurs, à :

- Ne pas revendre ou exploiter les Données à Caractère Personnel en dehors du cadre strict accepté par les utilisateurs.
- Garantir le droit des utilisateurs à modifier leur consentement à tout instant et sur tout support mis à leur disposition et à transmettre à Open Bee™ dans les plus brefs délais toute information, qui dans ce cadre, doit être prise en compte pour les opérations de gestion et de maintenance.
- Ce que tout utilisateur dispose du droit d'accès, de rectification et de suppression de toutes ou partie de ses Données à Caractère Personnel. Ainsi chacun des utilisateurs peut, gratuitement et sur simple demande, avoir accès à l'intégralité des informations le concernant et les rectifier, les compléter ou s'opposer à leur traitement.
- Désigner un responsable de traitement des Données à Caractère Personnel dans le cadre de la licence de logiciel ou du contrat qui vous lie à Open Bee™, à défaut le responsable du traitement sera votre représentant légal.

A1 Annexe 1

Coordonnées du Data Protection Officer d'Open Bee™ :
Jean-Louis PASCON
Adresse email : jl.pascon@mb2i.fr
Numéro de téléphone : +33 (0)6 27 65 05 75

A2 Annexe 2

Coordonnées du sous-traitant d'activité d'hébergement d'Open Bee™ :

Dénomination sociale : Orange Business Services
Adresse : 7 voie de l'Orée, 27100 Val-de-Reuil
Numéro de téléphone : +33 (0)2 32 09 26 00
Site internet : https://www.orange.com/sirius/datacenter/
Date du contrat : 29/01/2016

Open Bee™