Politique de Sécurité SI

Workelo

Dernière mise à jour **Janvier 2024**

Evolutions du document		
Qui	**Quand**	**Quoi**
Mathieu Cochet	15/01/2024	Mise à jour des sous-traitants
Mathieu Cochet	03/11/2023	Mise à jour Organisationnelle
Mathieu Cochet	24/07/2023	Mise à jour des sous-traitants
Mathieu Cochet	20/06/2023	Précision sur le chiffrement des données (paragraphe 3.1)
Mathieu Cochet	20/06/2023	Précision sur la notification sur incident d'atteinte aux données
Mathieu Cochet	03/01/2023	Mentions complémentaires sur politique d'accès
Mathieu Cochet	15/03/2022	Ajout précisions sur sécurité sous-traitants
Mathieu Cochet	06/05/2021	Détails sur les missions des sous-traitants
Mathieu Cochet	27/04/2021	Complément prestataire
Mathieu Cochet	26/11/2020	Changement format
Mathieu Cochet	26/11/2020	Ajout de détail sur le stockage et sur la gestion des incidents
Mathieu Cochet	17/06/2020	Ajout de précisions sur le chiffrement du stockage
Mathieu Cochet	15/05/2020	Mise à jour du DRP
Mathieu Cochet	02/01/2020	Mise à jour de la politique d'accès
Mathieu Cochet	04/06/2018	Ajout précisions sur sécurité applicative
Mathieu Cochet	15/05/2018	Ajout précisions sur sécurisation accès Github
Mathieu Cochet	14/12/2017	Ajout précisions postgres, détails sur encryption mots de passe dans db
Alexandre Grenier	01/10/2017	Ajout de la section RGPD
Mathieu Cochet	22/06/2017	v1 Initialisation du document

TABLE DES MATIÈRES

1. Description du système

1.1. Lieux concernés par la prestation

Les données sont stockées dans un datacenter en région parisienne (production et sauvegarde).

Les locaux de Workelo quant à eux sont à Paris, dans le 2nd arrondissement.

1.2. Sous-traitants

Avec accès partiel à des données personnelles en accord avec le RGPD

Raison sociale	Nature de la prestation	Relation contractuelle	Région d'exécution de la prestation
AWS	Stockage de données	Data Processing Agreement	France (backup Allemagne)
OVH	Stockage de données	Data Processing Agreement	France (backup Allemagne)
Heroku	Serveur applicatif (PaaS)	Data Processing Agreement	Europe
Brevo	Serveur d'envoi des communications	Data Processing Agreement	Europe
Zendesk	Suivi des tickets clients	Data Processing Agreement	Europe
Papertrail	Suivi des logs	Data Processing Agreement	Europe

Avec accès limité à des données pseudo-anonymisées en accord avec le RGPD

Raison sociale	Nature de la prestation	Relation contractuelle	Région d'exécution de la prestation
AppSignal	Suivi des erreurs	Data Processing Agreement	Pays-Bas
Amplitude	Suivi de l'usage	Data Processing Agreement	Europe
Hotjar	Suivi de l'usage	Data Processing Agreement	Europe
Segment	Suivi de l'usage	Data Processing Agreement	Europe

Si option activée

Raison sociale	Nature de la prestation	Relation contractuelle	Région d'exécution de la prestation
Yousign	Signature électronique	Data Processing Agreement	Europe
AccessiBe	Accessibilité	Data Processing Agreement	Etats-Unis

1.3. Détail sur l'hébergement des données

Certifications

L'application et les données sont hébergées chez AWS ou OVH.

Les data centers de nos prestataires sont toujours localisés en France, en région parisienne et possèdent les certifications suivantes :

- ISO 50001 (2014)
- Tiers III design by the Uptime Institute (2014)
- pci-DSS
- HDS
- ISO 27001

Sécurité des installations

Les data centers d'hébergement sont conformes aux niveaux de sécurité R82 et R81 APSAD. Plus de détails sur la sécurité du datacenter peuvent être obtenus sur demande.

Garanties de service du datacenter

Définitions

Time Warranty Intervention (TWI): The technical team is working on the incident during this period.

Time Warranty Repair (TWR): The technical team must repair the incident during this period.

worked Hours: Monday-Friday 9:00 a.m. to 6:00 p.m. CEST+2

Incident standard

TWI 2 hours during business hours , 3 hours apart.

TWR: 6:00

Critical Incident

TWI: 30 minutes during business hours, 2 hours away.

TWR 2 hours during business hours, three hours apart.

SLA de l'hébergement

Le taux de disponibilité garanti est de 99.999% en standard

Politique de sécurité de l'hébergeur

- Chiffrage systématique des connections et des push du code lors de la mise à jour de l'application, le push se fait toujours en ssh
- Les failles O-day sont corrigés en moins de 8H.
- La base de données (postgres) est régulièrement mise à jour avec les patchs de sécurité
- Protection anti-DDos

Chiffrement des données

Les données stockées sont chiffrées au repos : AES 256 avec rotation des clés deux fois par an, utilisant des modules de sécurité matériels (HSM).

Les clés sont gérées par Workelo et ne sont ainsi pas connues de l'hébergeur de données qui n'a aucun moyen d'avoir accès à la donnée en clair.

2. Sécurité Organisationnelle

2.1. Organisation humaine

Organisation

Le Directeur Technique est chargé d'assurer la sécurité IT dans le fonctionnement de l'entreprise. Chaque membre de l'équipe technique suit une formation initiale sur les principes de sécurité.

Un comité "Sécurité et RGPD" constitué du Directeur Technique, des fondateurs et des responsables de pôles se rassemble 2 fois par an afin de s'assurer de la bonne application des mesures de sécurité au sein de toutes les équipes et afin de définir si des ajustements doivent être apportés.

Sensibilisation des acteurs

Tous les trimestres le Directeur Technique anime un atelier de travail afin de revoir les principes de la politique de sécurité et en particulier s'assurer du respect des principes OWASP dans le cycle de développement de l'application.

2.2. Procédures de sécurité

Gestion des incidents de sécurité

Identification des incidents

Les incidents peuvent être remontés de plusieurs manières :

- Notification envoyée lorsqu'une vulnérabilité sur un composant utilisé par Workelo est ajoutée à la **base CVE**
- Alerte venant de notre outil **AppSignal** en charge de remonter les erreurs rencontrées par nos utilisateurs
- Alerte venant de notre outil **UpTimeRobot** en charge de mesurer la disponibilité des services Workelo
- Alerte venant d'un client

Qualification des incidents

Les vulnérabilités sont qualifiées par le directeur Technique dès remontée selon une notation sur 3 dimensions :

- Confidentialité - Des données clients sont-elles exposées ?
- Périmètre - Quel est le périmètre fonctionnel touché ?

- Disponibilité - Quel impact sur la disponibilité de l'application ?

Traitement des incidents

Tout incident et toute demande fait l'objet d'un enregistrement dans notre outil de suivi par le directeur Technique. Un développeur est assigné sur la résolution de l'incident et le délai de prise en charge et celui de résolution varient en fonction de la criticité :

- **standard** : prise en charge en 4h et résolution en 5 jours
- **majeur** : prise en charge en 4h et résolution en 1 jour
- **critique** : prise en charge en 2h et résolution en ½ journée

Communication autour des incidents

Dès la vulnérabilité identifiée, Workelo informe le client :

- Les destinataires sont le responsable du compte Workelo, le RSSI et le DPO
- Le format de cette communication est un email envoyé
- Le délai est inférieur à 48h suivant l'incident
- Cette information détaille notamment
    - L'origine de la vulnérabilité
    - Le périmètre impacté et le nombre d'utilisateur concerné
    - Le cas échéant les données impactées
    - Les mesures prises pour le retour à la normale
    - Les mesures prises pour éviter qu'un tel incident ne se reproduise
- Dans le cas d'incident majeur ou critique
    - tout au long de la résolution de l'incident, une mise à jour des informations est communiquée toutes les heures (par email)
    - une fois résolu le client est informé et un brief post-mortem sera fourni par email

Gestion de l'authentification

L'authentification peut se faire de plusieurs manières, chacune de ces manières pouvant être activée sur l'ensemble du compte ou sur certaine population d'utilisateur.

Indépendamment du type d'authentification, la session utilisateur est automatiquement clôturée après un délai d'inactivité d'une heure.

L'authentification par email / mots de passe

Les mots de passe doivent faire au moins 12 caractères, dont 1 majuscule, 1 minuscule et 1 chiffre. Ils doivent être changés tous les 3 mois.

L'email utilisé peut être l'email personnel de l'utilisateur (dans le cas d'un onboardee, avant qu'il rejoigne l'entreprise) ou son email professionnel. Il est possible de basculer de l'un vers l'autre au cours du temps.
L'accès est automatiquement bloqué après 5 tentatives de connexion erronées. La réactivation du code se fait en cliquant sur un lien sécurisé envoyé par email.

Dans ce cas d'authentification, l'utilisation d'un gestionnaire de mot de passe est fortement recommandé afin de générer un mot de passe complexe et pouvoir facilement le changer.

L'authentification par SSO
Il est recommandé d'activer le SSO sur votre compte Workelo, cela afin d'en augmenter la sécurité mais également afin de proposer à vos utilisateurs une expérience plus agréable en évitant un "n ième mot de passe".
Workelo peut se connecter avec tout IDP SSO utilisant le protocole SAML v2. Il s'agit d'une connexion SSO "SP initiated" (initiée par le Service Provider).

L'authentification par lien sécurisé
Ce mode de connexion est très simple : l'utilisateur entre son email sur Workelo et reçoit instantanément un lien unique et temporaire de connexion lui permettant de s'authentifier. Cela a l'avantage de renforcer la sécurité en changeant à chaque connexion le lien de connexion.
Ce mode d'authentification est de plus en plus répandu car répond à la double problématique de (1) renforcer la sécurité et (2) améliorer l'expérience de l'utilisateur en simplifiant la connexion. Si cette tendance vous intéresse : étude du Forum Economique Mondial et étude Gartner.

Détail sur la gestion des mots de passe

Les mots de passe sont enregistrés dans la base de données après un chiffrage non récupérable : de manière à prévenir le déchiffrage des mots de passe par tout tiers y compris le personnel Workelo . En cas de perte de mot de passe, l'unique possibilité est la génération par l'application d'un token de connexion envoyé sur l'adresse email de l'utilisateur (lien unique et temporaire pour changer de mot de passe).

A aucun moment, le mot de passe d'un utilisateur n'est visible par un collaborateur Workelo : le mot de passe est directement crypté dans la base de données. Compte tenu de la technique de chiffrage utilisée, un collaborateur Workelo, y compris du service technique, n'a aucune possibilité pour accéder au mot de passe en clair.

Les mots de passe des utilisateurs sont chiffrés dans la base de données en utilisant un algorithme de type 'bf', de type Blowfish based cypher, avec 8 itérations. De plus, une valeur aléatoire ("salt") est utilisée pour chiffrer.

Gestion des habilitations

Le Directeur Technique gère les accès au SI Workelo des membres de l'équipe technique. Les différents niveau d'accès sont

1. l'accès administrateur à Workelo
2. l'accès au code et la possibilité de soumettre des modifications
3. l'accès au code et la possibilité de valider des modifications
4. l'accès aux serveurs applicatifs (production et staging)
5. l'accès aux serveurs de stockage (production et staging)

Seul le Directeur Technique (et le lead dev. en son absence, par délégation) ont accès à l'ensemble de ses droits. Les autres membres de l'équipe technique n'ont accès qu'à (1) et (2). Par délégation temporaire ils peuvent avoir accès à d'autres droits si c'est nécessaire à la réalisation d'une mission.
En cas de départ de l'équipe, les droits sont immédiatement révoqués.

Plan de reprise d'activité

Contexte

Au-delà des dispositions prises pour assurer au quotidien la continuité de service tel que précisé contractuellement, des précautions particulières sont mises en œuvre pour limiter la probabilité d'un sinistre majeur, mais un tel événement demeure possible.

Dans le cas où les systèmes informatiques de Workelo ou de ses sous-traitants subiraient un sinistre majeur, par exemple un incendie, rendant impossible l'exécution, dans les conditions habituelles, des prestations effectuées pour nos Clients, Workelo a mis en place un plan de continuité de service.

Ce plan permet, selon les conditions contractuelles définies entre Workelo et ses Clients, d'assurer un redémarrage rapide de ses systèmes sur un site de secours, ainsi que le rétablissement des connexions avec les Clients et les différents partenaires. Les procédures critiques pour les Clients pourront ainsi être exécutées dans des délais acceptables.

Ces plans sont maintenus en conditions opérationnelles :

- évolutions du plan de secours en fonction des évolutions des environnements, de la production, de l'organisation, des techniques
- tests de validation réguliers couvrant l'ensemble des offres des Clients, impliquant l'ensemble des équipes concernées, y compris les utilisateurs et les Clients
- processus d'amélioration continue à partir des retours d'expérience liés aux tests
- audits externes

Disaster Recovery Plan

La mise en œuvre de ce plan n'intervient qu'en cas de sinistre grave sur le site principal de production de Workelo.

Il vise à garantir, dans ce contexte, une reprise de l'ensemble des activités liées à la maintenance et à l'exploitation des applications des Clients de Workelo en mode outsourcing, par la mise à disposition d'un environnement de production sur un site de backup.

Workelo s'engage, dans un délai maximum de 24 heures nettes, à remettre en état opérationnel l'environnement de production de ses clients.

Cette remise en état se fait en application d'un certain nombre de procédures prévues par Workelo, et notamment :

- une sauvegarde de l'ensemble des données (données individuelles et collectives, programme) est réalisée depuis le site principal
- le support magnétique sur lequel a été faite la sauvegarde est crypté, puis mis en sécurité dans le centre de secours situé en France métropolitaine

Workelo intègre en standard la prestation de plan de reprise d'activité.

La procédure de Disaster Recovery (DR) sera activée dans deux cas :

- quand les services de production du site principal de Workelo ne sont plus accessibles par l'ensemble des Clients,
- ou lorsque se produit un incident technique lourd affectant les Clients (dégradation importante des performances, pertes de fonctionnalités importantes…)

La procédure se déroule comme suit :

- Workelo informe tous les Clients de la mise en place de la procédure de Disaster Recovery
- le trafic est redirigé sur le site de backup (action au niveau DNS) ou tout autre site permettant ladite mise en œuvre de la procédure
- test de la plateforme de DR au niveau système et base de données
- ouverture de l'accès à la plateforme aux équipes internes Workelo
- test de la plateforme de DR au niveau applicatif
- ouverture de l'accès à la plateforme à l'ensemble des Clients
- Workelo informe les Clients que le site de backup est opérationnel.

Pendant que le site de DR prend le relais, les équipes techniques Workelo corrigent les problèmes sur le site principal, puis testent la plateforme principale (système d'exploitation, base de données, applications).

Lorsque la décision est prise de revenir sur le site principal et d'arrêter le site de secours, Workelo :

- informe les Clients de la prochaine remise en service du site principal (cette remise en service se fait en dehors des heures ouvrables)
- procède à la fermeture des accès des Clients à la plateforme de DR
- arrête les applications sur le site de DR
- synchronise les environnements du site de DR avec ceux du site principal
- redémarre les applications sur le site principal
- teste les applications sur la plateforme principale
- ouvre l'accès de la plateforme principale aux Clients.

2.3. Conformité

Cadre réglementaire applicable

Nous garantissons une **conformité RGPD** dans les traitements que l'on applique aux données de nos clients.

En particulier en termes de sécurité, possibilité de modification et suppression. Chaque données que nous traitons est considérée comme personnelle et est traitée selon la RGPD (chiffrage robuste).
Le chapitre **Engagements RGPD** détaille cela.

3. Sécurité de l'Infrastructure

3.1. Cloisonnement des systèmes

Cloisonnement stricte des environnements

Les environnements de Staging et de Production sont sur des serveurs différents, utilisent des bases différentes et des serveurs de stockage différents.

Par ailleurs aucune information de l'environnement de Production ne se retrouve en environnement de Développement, Test ou Staging.

Cloisonnement logique des données au sein d'un environnement

Entre comptes, le cloisonnement est logique : une même table comprend les informations liées à différents clients. Cependant il est rigoureusement impossible d'effectuer une requête sans préciser le compte concerné (clé ID spécifique à chaque compte). Chaque accès à la donnée ne peut se faire qu'en utilisant cette clé ID spécifique.

Les données sont séparées logiquement. Si les informations sont stockées sur un disque alors chaque client a son propre dossier, si les données sont stockées sur une base de données alors l'accès à ces données ne peut se faire qu'avec un identifiant afin de garantir l'étanchéité des données entre clients.

Par ailleurs les données sont chiffrées au repos (cf. paragraphe 1.3) : AES 256 avec rotation des clés deux fois par an, utilisant des modules de sécurité matériels (HSM). Chaque client bénéficie d'une clé spécifique. Elles sont gérées par Workelo et ne sont ainsi pas connues de l'hébergeur de données qui n'a aucun moyen d'avoir accès à la donnée en clair.

3.2. Sécurité des échanges

Les communications avec l'application utilisent le protocole TLS (1.2 minimum) avec un certificat SSL (clé 2048) wildcard, signature SHA-256 et encryption RSA.

L'utilisation de la connexion HTTPS est forcée :

- par un redirection côté serveur
- par l'utilisation d'un header http
- par l'utilisation d'une Content Security Policy

3.3. Sauvegardes

La base de données de l'application est sauvegardée quotidiennement la nuit à 2h du matin. La durée de rétention est de 6 mois.

Le dump de la sauvegarde est chiffrée (chiffrement au repos AES-256) vers notre hébergement de backup en France (AWS ou OVH).

Les données sauvegardées sont traitées avec le même niveau de sécurité que les données de production.

Des tests de restauration sont effectués tous les 6 mois en staging.

3.4. Surveillance et traçabilité

Les connexions et réalisations d'actions donnent lieu à des traces pour tous les utilisateurs.

Pour les administrateurs, les modifications de paramétrage du compte donnent aussi lieu à des traces.

Les logs sont centralisés (Papertrail) et sont analysés en temps réel par notre outil Coralogix qui identifie les comportements à risques.

4. Sécurité Applicative

4.1. Règles d'ingénierie

Workelo applique les principes de l'OWASP pour Ruby on Rails.

Avant chaque mise en production le code développé passe par une vérification automatique (CodeFactor notamment) qui analyse le respect de principes de sécurité, puis une relecture manuelle et une procédure de test en staging.

4.2. Audits de sécurité

L'application web est auditée régulièrement par les services suivants :

Service	Note obtenue par Workelo
SSL Labs https://www.ssllabs.com/ssltest/index.html	**A**
Security Headers https://securityheaders.io	**A**

Nous n'effectuons pas d'audit de sécurité nous-même - cependant certains clients font appel à des prestataires externes afin de réaliser des audits / tests d'intrusion. Chaque année 1 à 2 tests sont ainsi réalisés. De manière générale le périmètre analysé est le suivant :

- Contrôler le niveau de confidentialité et d'intégrité des données échangées et stockées
- Contrôler l'identification / authentification des utilisateurs et la traçabilité des actions
- Qualifier le processus de gestion des habilitations
- Évaluer la résistance aux tentatives d'intrusions internes et externes
- Identifier les possibilités d'intrusion au niveau des bases de données, au niveau du réseau, au niveau des systèmes
- Contrôler le cloisonnement applicatif entre les différentes entités et les profils applicatifs: utilisateur, manager, RH, administrateur

Par ailleurs, certains clients ont mis en place des scans quotidien automatisé (par exemple avec Qualys).

4.3. Sécurité des librairies

Concernant le code applicatif, Workelo limite au stricte minimum l'utilisation de librairie extérieure. Quoi qu'il en soit, un audit des vulnérabilités est effectué de manière régulière.

4.4. Détail des mesures de sécurité

Firewall

Firewall applicatif en place (via Cloudflare) assurant le renforcement de la sécurité via un ensemble de règles prédéfinies visant à arrêter une large gamme d'attaques d'applications. Les règles couvrent l'ensemble des principes OWASP notamment.

Protection contre les failles CSRF

L'authentification utilise un mécanisme de session stockée côté serveur (*stateful)*. Un token est généré par le serveur lors de l'authentification réussie. Ce token est ensuite retourné au client qui le stocke en session navigateur. Chaque requête transmise au serveur doit contenir un token valide sous peine d'être rejetée.

Protection contre les attaques DoS

En plus des dispositifs anti-DDos implémentés par l'hébergeur, nous avons implémenté au niveau du serveur web une limitation de nombre de requêtes par seconde, avec un bannissement en cas de dépassement de la limite.

Par ailleurs, nous utilisons le service CloudFlare afin d'ajouter une couche de protection supplémentaire en cas d'attaque DDoS (attaques DDoS HTTP, protection d'origine, attaques DDoS SSL/TLS, attaques DDoS de la couche réseau).

Cross-site scripting

Les vulnérabilités XSS peuvent exister à différents niveaux :

- dans la page HTML qui contient l'application client
- dans le code source de l'application qui traite les réponses serveur,
- dans le rendu HTML des contrôles

L'application Workelo n'utilise pas de contrôles permettant à l'utilisateur de saisir du code HTML à l'exception d'un éditeur de texte WYSIWYG. De manière général, tout contenu est « échappé » (escaped) avant d'être renvoyé au navigateur afin qu'il ne soit pas interprété autrement que comme un simple texte.

Base de données

Le SGBD est postgresql. La version actuellement utilisée par l'application est 10.14. Nous installons systématiquement le dernier patch disponible sur https://www.postgresql.org/. L'authentification à la base de données est cryptée en SSL

SQL Injection

Mesures pour lutter contre l'injection SQL :

5. La connexion utilisée par l'application pour accéder à la base de données à des droits d'accès réduits (uniquement un rôle CRUD, sans droits DDL, ou de droits d'élévation de privilèges, etc). Les droits sur les tables de l'application sont définis expressément. Par défaut, aucun droit CRUD sur aucune table.
6. L'application accède à la base de données via le serveur applicatif (architecture 3-tiers). Par design, l'application cliente n'envoie pas de requête SQL et ne peut décider des sources de données accessibles : c'est le serveur applicatif qui détermine les données accessibles à l'utilisateur d'après la route appelée et l'identité de l'utilisateur.
7. Les requêtes SQL sont effectuées à partir de requêtes paramétrées et non par concaténation de chaînes. Tous les paramètres sont échappés. Le module utilisé pour accéder à la base de données échappe tous les paramètres et protège contre l'injection SQL.

8. Engagements RGPD

La société teamr.io Sas (nom commercial Workelo) à travers ce document s'engage à :

1. **traiter les données uniquement pour finalité qui fait l'objet du contrat.**
2. **traiter les données conformément aux instructions documentées du Client.** Si Workelo 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 Client. En outre, si Workelo 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 Client 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**
   - Workelo 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 Client 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 Client dispose d'un délai maximum de sept (7) jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le Client 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 Client. Il appartient à Workelo 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. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, Workelo demeure pleinement responsable devant le Client de l'exécution par l'autre sous-traitant de ses obligations.
7. **Exercice des droits des personnes**
   - Dans la mesure du possible, Workelo doit aider le Client 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).
   - Lorsque les personnes concernées exercent auprès de Workelo des demandes d'exercice de leurs droits, Workelo doit adresser ces demandes dès réception par courrier électronique à au Client.
8. **Notification des violations de données à caractère personnel**
   - Workelo notifie au Client toute violation de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance, par mail. Cette notification est accompagnée de toute documentation utile afin de permettre au Client, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.
9. **Sort des données**

- Au terme du contrat, Workelo s'engage à détruire toutes les données à caractère personnel ou à renvoyer toutes les données à caractère personnel au Client.
- Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information de Workelo. Une fois détruites, Workelo doit justifier par écrit de la destruction.

10. Délégué à la protection des données

- Workelo communique au Client 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.

11. Registre des catégories d'activités de traitement

- Workelo déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du Client 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 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.

12. Documentation

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