SOFTCOM

CLUSIS

Nouvelle Loi sur la **protection des données**

Livre Blanc

Table des matières

NB : l'usage du livre blanc et de ses annexes est exclusivement réservé à l'acquéreur et à sa société. Pour rappel, les bénéfices de la vente de ce livre blanc sont exclusivement destinés au Clusis.

Introduction

A l'échelle mondiale et en particulier au sein de l'UE, la protection des données a été considérablement renforcée et les organisations internationales ont durci leurs normes minimales en la matière. Pour la Suisse, il était donc nécessaire d'adapter sa loi de 1993 aux nouveaux modes de consommations (achats en ligne, réseaux sociaux, etc.), aux développements technologiques (numérisation, intelligence artificielle, etc.) et aux normes internationales. C'est pourquoi, après de nombreux débats, le parlement fédéral a adopté le 25 septembre 2020 la nouvelle loi sur la protection des données. Conformément à la décision du Conseil fédéral en date du 31 août 2022, la nLPD n'entrera en vigueur qu'à partir du 1er septembre 2023. En fixant ce délai, le Conseil Fédéral répond aux préoccupations du monde économique. Ce délai d'un an accordera suffisamment de temps aux responsables en matière de protection des données pour prendre les dispositions nécessaires à la mise en œuvre du nouveau droit

En vue de l'entrée en force de la nouvelle Loi sur la protection des données en 2023, le Clusis - l'association suisse de la sécurité de l'information – a organisé ou coorganisé depuis 2021 plusieurs événements à destination des PMEs/PMIs afin de les sensibiliser à cette nouvelle réglementation. Ces différentes conférences ont montré que ladite Loi est complexe à comprendre et que les organisations rencontrent des difficultés pour percevoir ce qu'elles vont concrètement devoir mettre en œuvre.

Softcom Technologies SA étant membre de l'association et devant se mettre en conformité, se propose de mettre à disposition son expérience et ses différents documents en vue de faciliter la compréhension de la Loi et de simplifier le projet pour les PMEs.

Le présent document ne se veut pas exhaustif mais peut servir de base à toute petite ou moyenne entreprise. Il s'avèrera nécessaire, pour chaque organisation, d'identifier clairement tous ses traitements et d'adapter son projet en conséquence.

Le Clusis reste volontiers à disposition des PME pour toute question ou pour une mise en relation avec des spécialistes/consultants(es) de la protection des données.

En complément de ce dossier, nous vous invitons à consulter les informations officielles de la Confédération Suisse et vous suggérons ces quelques liens :

https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-90134.html

https://www.kmu.admin.ch/kmu/fr/home/faits-et-tendances/digitalisation/protection-des-donnees/check-list-pour-les-pme-comment-se-conformer-a-la-loi-sur-la-protection-des-donnees.html

https://www.edoeb.admin.ch/edoeb/fr/home.html

Comprendre la Loi

La nouvelle Loi sur la protection des données nLPD entrera en force le 1er septembre 2023. A cette date, toutes les entreprises devront être conformes et doivent donc démarrer leur projet au plus tôt afin de respecter ce délai.

L'objectif de Loi, comme son nom l'indique, est de protéger les données des personnes compte tenu des avancées technologiques et des nouveaux modes de consommation ; notamment tout ce qui se passe désormais au travers d'Internet.

La Loi s'applique à toutes les sociétés et prévoit des sanctions – amendes - pouvant aller jusqu'à CHF 250'000.--. A noter et c'est important, au-delà d'un montant de 50'000.- ce n'est pas la société qui serait condamnée, mais la personne dans l'entreprise, responsable du traitement de ces données ! Et c'est pénal.

Qu'entendons-nous lorsque l'on parle de données ?

La Loi s'applique à toutes les données des personnes physiques et elles sont catégorisées en deux groupes :

a) Les données personnelles → ce sont toutes les données qui permettent d'identifier une personne. Par exemple : le nom, les prénoms, l'adresse de domicile, la date de naissance, une pièce d'identité, un compte bancaire, une photo, une adresse électronique, etc.

b) Les données sensibles → ce sont des données dites sensibles dès lors qu'elles donnent des informations très privées sur la personne ou qu'elles permettent de faire un profilage. Par exemple : les données judiciaires, biométriques, génétiques, les opinions politiques, les croyances religieuses, les affiliations syndicales, les origines ethniques, l'orientation sexuelle, les données de santé, etc.

Dans tous les cas, la Loi s'applique, mais elle prévoit que les données, personnelles et/ou sensibles, fassent l'objet d'une protection plus ou moins renforcée selon la sensibilité des données traitée. Par exemple : si ces données sont stockées de manière informatique, leur accès doit être strictement limité aux personnes habilitées (prenons le cas d'une entreprise qui demande des extraits de casiers judiciaires pour ses salariés **:** ceux-ci ne pourraient pas être consultés par un(e) réceptionniste). Au-delà d'une gestion des droits d'accès, ces données doivent être sécurisées, potentiellement chiffrées si c'est possible. Le responsable des traitements doit faire tout son possible pour les protéger.

Qu'est-ce qu'un traitement de données ?

Toute opération effectuée sur des données personnelles ou sensibles peut être considérée comme un traitement de données ; soit :

A) La collecte ou l'enregistrement
B) Le stockage – des dossiers papiers, des fichiers informatiques, des archives, etc.
C) La récupération – consultation, utilisation, modification, etc.
D) Le transfert – l'envoi à un tiers ou le partage d'information
E) La conservation ou la suppression comme la destruction ou l'effacement.

Prenons l'exemple du recrutement : lorsque l'entreprise publie une offre d'emploi sur son site internet, elle doit désormais informer préalablement le(la) candidat(e) de la manière dont sont collectées et traitées les informations liées à sa candidature. L'entreprise ne pourra récolter que les données nécessaires au recrutement et ne pourra vraisemblablement exiger d'avoir accès à la religion de la personne. Le dossier devra ensuite être traité de manière confidentielle et ne pourra pas être consulté par une personne externe au processus de sélection. Si le dossier n'est finalement pas retenu, il ne pourra pas être conservé sans l'accord du (de la) candidat(e).

Quels sont les traitements de données d'une PME ?

La liste ci-dessous ne se veut pas exhaustive mais elle donne une vue générale et transverse que peut rencontrer une PME :

a) Les ressources humaines avec les traitements suivants :
    a. Le recrutement
    b. La gestion des dossiers des collaborateurs(trices)
    c. La gestion des heures, des vacances, des notes de frais, du salaire
    d. La gestion des assurances sociales
    e. La formation
b) Les clients avec les traitements suivants :
    a. Le CRM
    b. La gestion des dossiers clients
    c. La facturation / débiteurs / contentieux
c) Les fournisseurs
    a. La gestion des achats
    b. La gestion des dossiers
d) Le marketing
    a. Cookies sur le site internet
    b. Chatbot
    c. Les listes d'adresses, newsletter, etc.
e) Support ou service après-vente
    a. Gestion des tickets et dossiers de support

Quels sont les principes généraux de la Loi ?

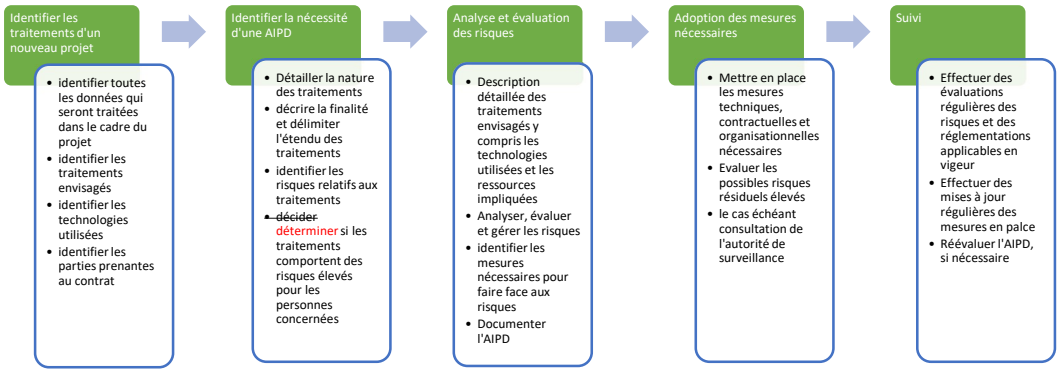
Transparence : informer les personnes concernées du traitement de leurs données personnelles. On doit donc informer implicitement ou explicitement selon la criticité des données, les personnes et conserver la trace de leur accord. On doit également leur donner la possibilité d'y avoir accès, de les vérifier, de les corriger si elles sont fausses ou de les supprimer (droit à l'oubli).

Finalité déterminée : ne traiter les données qu'à des fins communiquées de manière transparente. On ne peut donc pas collecter des données pour recruter une personne, puis utiliser ces données dans ses actions commerciales, ou les vendre.

Minimisation des données : ne collecter et ne traiter que les données nécessaires à la finalité poursuivie

Confidentialité : prévoir des paramètres favorables à la protection des données et prendre en compte la protection des données à un stade précoce (Privacy by design sous-entend que si l'on démarre une nouvelle activité ou un nouveau projet, l'entreprise est tenue de prendre en compte la protection des données en début de projet pour respecter la Loi. – voir la figure ci-dessous qui détaille les étapes à prévoir dans un contexte de privacy by design).

Fig. Etapes du Privacy by design



Principe de sécurité : les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées (destruction accidentelle ou non autorisée, perte accidentelle, erreurs techniques, falsifications, vol ou utilisation illicite, ainsi que la modification, la copie, l'accès ou tout autre traitement non autorisé)

Limitation de la conservation : supprimer ou rendre anonymes les données qui ne sont plus nécessaires à la finalité poursuivie

Exactitude : prendre des mesures appropriées pour garantir l'exactitude des données

Faire un plan de mise en œuvre

Comme pour tout projet, il convient d'organiser les choses et nous ne pouvons que suggérer de désigner un(e) chef(fe) de projet. Si l'entreprise n'a pas les compétences ou le temps pour le faire, elle peut mandater un(e) consultant(e) externe. On parle généralement d'une compétence de DPO (Data Protection Officer).

Le Clusis fournira volontiers une liste de consultants susceptibles d'intervenir pour vous.

Chez Softcom, nous avons le cas échéant défini les étapes suivantes :

a) Pour la direction, comprendre ce que devons faire, appréhender la Loi et obtenir les réponses à nos questions.

b) Nommer un(e) cheffe de projet.

c) Identifier les différents responsables de traitement dans toute l'entreprise.

d) Former toutes les personnes concernées, management, responsables de traitements, etc. Vous trouverez en annexe la présentation qui nous a servi pour la formation du personnel chez Softcom.

e) S'assurer de la bonne disposition d'une politique de sécurité.

f) Inventorier les traitements avec chacun des responsables de traitement :
    a. Documenter les traitements (modèles en annexe)
    b. Identifier les éventuels sous-traitants / transferts (y.c. à l'étranger)
    c. Classifier les données, identifier les écarts par rapport à la Loi et identifier les risques
    d. Etablir une liste des choses à réaliser sur la base des inventaires et risques.

g) Contrôler la réalisation de cette liste des choses à faire.

h) Définition du processus en cas d'incident.

i) Revue finale.

j) Intégration de la formation sur la protection des données dans l'onboarding des nouveaux collaborateurs.

k) Intégration d'une revue régulière dans le cadre de notre manuel qualité (ISO9001). Dans le cas contraire, il faudrait prévoir une revue par année pour s'assurer que les traitements sont toujours corrects et exhaustifs et que les responsables sont définis et formés.

Commencer par la politique de sécurité

Une politique de sécurité regroupe une série d'activités qu'il convient d'adresser pour protéger globalement l'entreprise contre des attaques cyber. La solution idéale serait de réaliser une certification ISO27001 mais ce type de démarche peut s'avérer lourde pour une PME. Dans tous les cas, et face à la croissance exponentielle des attaques, toute PME se doit absolument de disposer d'une hygiène de sécurité. Le Clusis se tient volontiers à disposition pour effectuer un Bilan Cyber ou pour vous orienter vers des entreprises susceptibles de vous conseiller dans cette démarche. Voici toutefois les sujets que vous devriez adresser dans votre politique de sécurité (les plus importants pour une PME en gras).

A. **Sensibiliser les utilisateurs aux risques de cybersécurité**
B. **Authentifier les utilisateurs avec une politique de mot de passe efficiente**
C. **Gérer les habilitations (les droits d'accès selon le rôle)**
D. Sécuriser les échanges avec d'autres organismes
E. **Sécuriser les postes de travail (antivirus et antispam)**
F. Sécuriser l'informatique mobile
G. **Protéger le réseau informatique interne**
H. **Sauvegarder et prévoir la continuité des activités**
I. **Gérer la sous-traitance**
J. **Protéger les locaux**
K. **Sécuriser les serveurs**
L. **Sécuriser les sites web**
M. **Archiver de manière sécurisée**
N. Encadrer la maintenance et la destruction des données
O. **Surveiller les accès et gérer les incidents**
P. Encadrer les développements informatiques
Q. Chiffrer, garantir l'intégrité ou signer

Inventorier les traitements

Cette étape du projet consiste à auditionner tous les responsables de traitement pour les inventorier. Les personnes concernées n'étant pas forcément encore familières avec cette approche de traitements, nous vous conseillons de les interroger sur :

a) Quels sont les traitements que vous appliquez aux données ?
b) Quels sont les logiciels que vous utilisez (autre moyen d'identifier un traitement)
c) Qui sont vos sous-traitants / fournisseurs (autre moyen d'identifier un traitement)
d) ..

Le cas échéant, nous vous recommandons de répertorier chaque traitement dans un fichier Excel que nous vous suggérons en annexe - Document 07-Registre des traitements

- Pensez à mentionner une date car vous aurez à réviser ce registre chaque année.
- Nous suggérons, après avoir fait l'analyse de chaque traitement, de compléter les colonnes données sensibles, sous-traitance et risques afin d'avoir une visibilité globale sur les éléments essentiels de votre gouvernance de protection des données.

Loi sur la protection des données : Registre des traitements

CLUSIS

Date de la dernière revue 02.03.2023

No activité	Groupe	Finalité de Traitement	Responsable	Catégories de personnes	Catégories de données	Catégories de d
1	RH	Salaires, Impôts sources et certificats de salaire	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sou
2	RH	Dossiers collaborateurs.trices	Prénon nom	Personnel sous contrat	Données sensibles	Internes et sou
3	RH	Gestion des compétences /CV	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sou
4	RH	Entretien annuels et/ou spécifiques	Prénon nom	Personnel sous contrat	Données sensibles	Internes et sou
5	RH	Archivage des collaborateurs.trices partis.es	Prénon nom	Personnel parti	Données sensibles	Internes et sou
6	RH	Assurances sociales et courtier	Prénon nom	Personnel sous contrat	Données sensibles	Internes et sou
7	RH	Gestion des absences	Prénon nom	Personnel sous contrat	Données sensibles	Internes et sou
8	RH	Gestion de l'image pour notre marketing	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sou
9	RH	Formation	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sou
10	RH	Vidéosruveillance	Prénon nom	Toutes les personnes accédant nos locaux	Donnnées personnelles	Internes et sou
11	RH	Egalité des salaires	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sou
12	Recrutement	Gestion des candidatures	Prénon nom	Candidats	Donnnées personnelles	Internes et sou
13	Commercial	Gestion de la relation client (CRM)	Prénon nom	Personnes de contact clients	Donnnées personnelles	Internes et sou
14	Admin	Contrôle des heures et facturation	Prénon nom	Personnel sous contrat - soustraitants	Donnnées personnelles	Internes et sou
15	Admin	Signature électronique	Prénon nom	Candidats, personnel sous contrat et clients	Donnnées personnelles	Internes et sou
16	Admin	Gestion des fournisseurs / Achats	Prénon nom	Perssonnes de contact fournisseurs	Donnnées personnelles	Internes et sou
17	Marketing	Cookies sur le site internet	Prénon nom		données de navigation	Internes et sou
18	Marketing	Newsletter et inscriptions aux event	Prénon nom	Tiers externes	Donnnées personnelles	Internes et sou
19	IT	Support	Prénon nom	Personnes de contact clients	Donnnées personnelles	Internes et sou
20	IT	Gestion des identifications	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sou
21	IT	Logs	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sou
22	IT	Téléphonie mobile	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sou
23	Compta	notes de frais	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sou
24	Compta	Budget	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sou
25	Compta	ebanking	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sou

Documenter chaque traitement

Dès lors que vous disposez de l'inventaire des traitements, il convient d'analyser, avec chaque responsable, quelles sont les données traitées, à quelle fin, quels sont les risques, les sous-traitants, etc.

Nous vous mettons en annexe également un document intitulé 10-Fiche de registre (Fig. 1) qui vous permettra de documenter le traitement, le cas échéant de déterminer les choses à faire au vu de la situation. Cette liste des choses à faire est à répertorier dans un fichier Excel, Todo List (Fig. 2) que nous mettons également à votre disposition en annexe. – Document 08_Todo_list

Fig. 1 Fiche de registre

Fiche de registre N°
Activité : X

Coordonnées du responsable de traitement	• PME SA, rue d'adresse 1, à 1000 Lausanne. • Tél : 021/ 999 99 99 • E-mail : info@pme.ch
Nom et coordonnées de la personne responsable	• (?)
Date de la dernière revue	•

1.1 Objectifs poursuivis (Finalités)

Décrire clairement l'objet du traitement de données personnelles et dans quel but les données sont récoltées.

"xzy"

1.2 Catégories de personnes concernées

Lister les différents types de personnes dont l'organisme collecte ou utilise les données.

Fig. 2 Todo List

Loi sur la protection des données : Todo List

Date de la dernière revue: 06.03.2023

Date	Activité	Responsable	Délai	Statut	Commentaire
	Vérifier avec notre fournisseur informatique que tous les PC disposent d'un anti-virus et que les mises à jour de sécurité sont effectuées				
	Vérifier avec notre fournisseur informatique que la gestion des droits et mots de passe est efficiante et que ces droits soient limités aux seules personnes habilitées. Ceci particulièrement sur les données RH ou vos données sensibles				
	Vérifier avec notre fournisseur informatique que nos serveurs bénéficient en permanence des mises à jour de sécurité				
	Vérifier avec notre fournisseur informatique que nous disposons bien de protections cyber sur notre réseau informatique (notamment un firewall et un antispam)				
	Vérifier avec nos fournisseurs informatiques que des sauvegardes sont réalisées pour toutes nos données. S'assurer que les restaurations sont testées et qu'un plan de secours est prévu en cas de cyber attaque				
	Contrôler que les locaux sont sécurisés, l'accès aux dossiers papiers limités aux personnes habilitées				
	Adresser un courriers à chaque sous-traitants pour s'assurer qu'il respecte bien la nouvelle Loi				
	Intégrer la politique de confidentialité dans les contrats RH ou la faire signer par chaque salarié				
	Indiquer les clauses de sauvegarde des données dans les lettres de confirmation de résiliation de contrat de travail				
	Anonymiser les informations des collaborateurs partis dans l'AD (système d'accès au réseau informatique)				
	Publier une politque de confidentialité pour notre site internet / candidatures				
	Ecrire une clause de conservation des données dans les réponses négatives recrutement				
	Penser à traduire les politiques de sécurité dans les langues utilisées				
	Banière des coockies à installer sur nos sites web avec lien sur la politque				
	Transférer nos sites web en Suisse				
	Disposer d'une clause contractuelle à intégrer dans tous nos nouveaux contrats sous-traitants				
	Ajouter une clause d'information dans notre newsletter avec possibilité de se désincrire				
	Faire une formation interne de sensibilisation du personnel aux risques cyber et protection des données				
	Organiser une sensibilisation cyber et protection des données pour chaque nouvel(le) employé				
	S'assurer qu'aucune donnée sensible n'est stockée/traitée dans des environnements (applications informatiques, hébergement, cloud) hors de Suisse				
	Vérifier d'avoir des sauvegardes cryptées si elles sont externalisées				
	Revue complète des documents avant mise en application				
	Intégration de la revue annuelle nLPD dans le manuel qualité ISO				

Nous vous aidons sur quelques actions et documentations

La sécurité informatique :

Contactez votre prestataire informatique et si vous n'en avez pas, mandatez un professionnel pour s'assurer de votre niveau de protection Cybersécurité. Il s'agit de vous assurer avec lui que votre réseau, vos serveurs et vos postes de travail sont protégés. Il faut également s'assurer que toutes vos données sont sauvegardées. (Une sauvegarde ne suffit pas, il doit vous proposer une stratégie de sauvegarde quotidienne, hebdomadaire et mensuelle, ainsi que des essais de restauration de données au moins une fois par an).

Si vous utilisez des services dans le Cloud ou hébergés chez des tiers, assurez-vous d'abord de ne pas utiliser des infrastructures hors d'Europe, même hors de Suisse si vous traitez des données sensibles (typiquement travailler dans le secteur de la santé et utiliser GMAIL comme messagerie n'est pas acceptable (compte tenu du fait que c'est un outil américain et que le droit US, dans certaines conditions, permet aux autorités d'accéder aux données).

Pour chacune de vos applications critiques (votre facturation, vos outils de production, dossiers clients, stock, vente en ligne, etc.), vous devez impérativement disposer d'un plan B au cas où l'infrastructure que vous utilisez n'est plus accessible suite à une attaque. La sauvegarde ne suffit pas, vous devez pouvoir redémarrer sur une autre infrastructure dans le cas où vos serveurs ou votre hébergeur sont inaccessibles : on parle dès lors de continuité des activités.

Sensibilisez vos collaborateurs(trices) aux risques Cyber :

Prenez le temps, régulièrement (au moins 4 fois par an) de sensibiliser votre personnel aux risques cyber :

a. Choisir un mot de passe compliqué et le changer régulièrement.
b. Ne pas installer d'application privée sur le matériel informatique de l'entreprise.
c. Ne pas visiter de sites internet douteux, ne pas télécharger des fichiers autres que du PDF.
d. Lorsqu'on reçoit un courriel et qu'il contient un lien ou un fichier Word, Excel, .EXE, on redouble de prudence avant de cliquer. En cas de doute, on contacte par téléphone l'émetteur du courriel et demande au prestataire informatique de vérifier.
e. Pour le personnel, la meilleure règle reste : en cas de doute, pas d'ouverture ! Vérifiez très sérieusement avant de cliquer.
f. Pensez également à sensibiliser tout(e) nouveau(elle) collaborateur(trice).

Votre site internet :

Contactez l'agence web qui s'occupe de votre site internet et assurez-vous des points suivants :

1. votre site est bien sécurisé par un certificat (vous devriez voir un cadenas sur le côté de votre nom de domaine) ;
2. si vous utilisez des cookies, que ceux-ci soient correctement paramétrés et que les visiteurs soient notifiés des possibilités d'acceptation ;
3. si vous disposez d'une boutique en ligne ou d'un espace clients, votre fournisseur vous assure qu'il met à jour l'environnement régulièrement avec les derniers correctifs de sécurité et qu'il confirme la bonne sécurité des données. Vous trouvez en annexe un modèle de lettre pour ce point spécifique des fournisseurs -Document 03 – Lettre sous-traitant ;
4. vous trouvez en annexe un document intitulé «04 -Politique de confidentialité ». Ce document doit regrouper toutes les informations liées à la protection des données et destinées aux visiteurs de votre site web, à vos clients et à vos candidats. Nous vous encourageons vivement à procéder à la revue de ce document, à supprimer ce qui ne vous concerne pas, à ajouter ce qui manquerait et, le cas échéant, à le publier sur votre site internet. Dans la pratique, il conviendra ensuite d'appliquer les règles décrites dans ce document.

Les ressources humaines :

Au même titre que pour la politique de confidentialité destinée aux clients, il est également nécessaire de clarifier la question pour les collaborateurs(trices). Vous trouverez en annexe un document « 05- Clauses de confidentialité » que nous vous invitons à revoir, amender ou compléter. Le cas échéant, il peut être ajouté à votre règlement du personnel ou faire l'objet d'une annexe au contrat.

Il va de soi que comme pour la politique de confidentialité, les règles définies dans les ressources humaines ne doivent pas seulement être décrites mais appliquées.

Sous-traitants :

Écrire à chaque sous-traitant en lui demandant de confirmer son respect de la Loi sur la protection des données. Vous trouverez en annexe un modèle de lettre intitulé 03 - Lettre sous-traitant.

Prévoir dans tout nouveau contrat sous-traitant, des clauses de protection des données. Vous trouverez en annexe un modèle de clauses à intégrer intitulé « 11 - Modèle de clause contractuelle pour sous-traitant ».

Nous vous encourageons à tenir à jour une liste des sous-traitants et fournisseurs. Cette liste vous facilitera chaque année le passage en revue pour vous assurer que les contrats sont à jour et/ou que vous disposez de garanties écrites qu'ils respectent bien la protection des données.

Contrats ou offres clients/conditions générales :

Dans le cadre de vos offres, contrats ou conditions générales, vous devez introduire des clauses qui indiquent clairement vos engagements et limites sur la question de la protection des données. Vous pouvez reprendre les termes prévus dans le document 04-Politique de confidentialité en choisissant les paragraphes concernant vos clients.

Mailings / marketing :

Dans chaque mailing, vous devez offrir la possibilité aux destinataires de se désinscrire pour ne plus recevoir vos communications. Prévoyez soit avec votre agence marketing, soit au bas de votre courriel, une information au client avec la procédure pour se désinscrire. Le cas échéant, vous devrez supprimer ses coordonnées de vos fichiers.

Selon vos traitements et l'analyse que vous aurez réalisée, vous devez pour le surplus mettre en place :

a. S'il y a des données sensibles, les protéger au maximum, limiter les droits d'accès aux seules personnes habilitées à les traiter
b. Informer les propriétaires de ces traitements de ce qui est collecté et à quelle fin
c. Leur permettre de vous contacter pour les corriger
d. Déterminer la rétention de ces données et regarder ce qui peut être supprimé ponctuellement.

Vous vous assurez que dans le processus de traitement des demandes qui pourraient vous être formulées (des clients, partenaires, collaborateurs qui vous demandent des informations sur leurs données), vous apportez une réponse dans des délais raisonnables.

En cas d'incident

Dans le cas où vous constateriez une attaque de votre système d'information, contactez immédiatement votre société de service informatique ou un prestataire spécialisé. Le Clusis vous mettra volontiers en relation avec ses membres en cas de besoin.

En cas de fuite (vol) de données, vous êtes tenus d'informer le préposé fédéral à la protection des données et vos clients. Ceux-ci doivent en effet pouvoir potentiellement réagir au cas où le vol aurait pour conséquence, des tentatives d'escroquerie à leur encontre.

Vous trouverez en annexe un modèle de courrier intitulé 06 - Lettre au PFDT.

Planifier une revue annuelle

Si pour la première fois, le travail à réaliser dans la mise en conformité pour cette Loi est relativement important, une revue annuelle sera, dans tous les cas, simplifiée. Nous vous invitons à planifier une revue annuelle et à reprendre tous les documents évoqués dans ce livre blanc pour vous assurer que votre entreprise reste conforme aux exigences de la Loi.

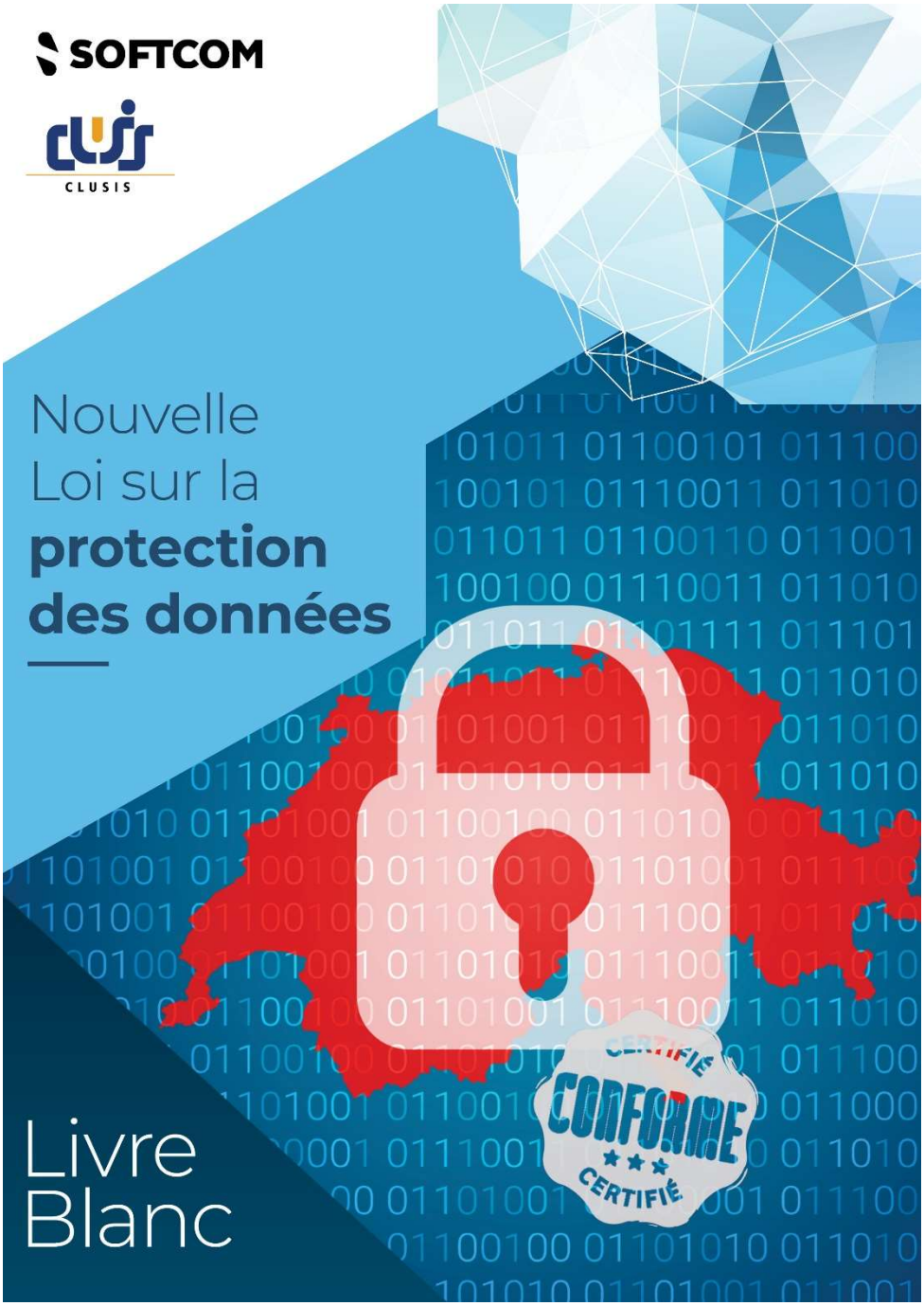
Conclusion

La mise en conformité de votre organisation est non seulement une exigence légale mais elle a également pour but d'augmenter la confiance avec vos clients et vos collaborateurs(trices). C'est également l'opportunité de faire un bilan sur votre cybersécurité car au-delà des risques de fuites de données, c'est surtout votre outil de gestion qui est vulnérable.

Dans tous les cas, formez et informez vos collaborateurs(trices), c'est la meilleur des hygiènes.

Annexe 1 & 2 :

- Modèle « Politique de confidentialité »
- Modèle « Clause de confidentialité RH »



Annexe 1 : modèle « Politique de confidentialité »

Politique de confidentialité

PME SA, rue de l'adresse 1, 1000 Lausanne, Suisse, inscrite au registre du commerce du canton de Vaud sous le numéro CH-999.999.999, est responsable de la collecte, du traitement et de l'utilisation de vos données personnelles.

Votre confiance est importante pour nous, c'est pourquoi nous prenons la protection des données au sérieux et assurons une sécurité appropriée dans l'application du droit suisse.

Si vous avez des questions ou des commentaires concernant notre traitement de données personnelles et la base juridique sur laquelle nous les traitons, vous pouvez nous contacter en utilisant les coordonnées suivantes :

Par courrier : PME SA, rue de l'adresse 1, 1000 Lausanne.
Par courriel : info@PME-SA.ch

1. Traitement des données

Appel de nos sites web

PME SA est l'opérateur du site web www.PME-SA.ch et d'autres sites et sous-sites (ensemble de **nos sites web**). Lorsque vous visitez nos sites web, nos serveurs enregistrent temporairement chaque accès dans un fichier journal. Les données techniques suivantes sont enregistrées et stockées jusqu'à leur suppression automatique au plus tard après 180 jours, comme c'est le cas pour chaque connexion à un serveur web :

- l'adresse IP de l'ordinateur demandeur ;
- le nom de votre fournisseur d'accès à Internet (généralement votre fournisseur d'accès Internet) ;
- la date et l'heure de l'accès ;
- le site web à partir duquel l'accès a été effectué (URL de référence), le cas échéant avec le terme de recherche utilisé ;
- le nom et l'URL des données requises ;
- le code de statut (par exemple, message d'erreur) ;
- le système d'exploitation de votre ordinateur ;
- le navigateur que vous utilisez (type, version et langue) ;
- le protocole de transmission utilisé (par exemple, HTTP/1.1) ;
- le cas échéant, votre nom d'utilisateur provenant d'un enregistrement ou d'une authentification.

Ces données sont collectées et traitées dans le but de permettre l'utilisation de nos sites web et de nos applications (l'établissement de la connexion et l'échange de données), d'assurer en permanence la sécurité et la stabilité du système et de permettre l'optimisation de notre offre Internet. Les données sont également collectées à des fins statistiques internes.

En outre, l'adresse IP est évaluée avec les autres données en cas d'attaques contre l'infrastructure du réseau ou d'autres utilisations non autorisées ou abusives du site web à des fins de clarification et de défense et, si nécessaire, utilisée dans le cadre de procédures pénales pour l'identification et pour les procédures civiles et pénales contre les utilisateurs concernés.

La base légale pour un tel traitement de données est dans notre intérêt légitime au traitement au sens de l'art. 13 al. 1 LPD/31 al. 1 nLPD et l'art. 6 al. 1 lit. f RGPD.

Contact via le service d'assistance téléphonique 24h ou le numéro de téléphone habituel

Vous avez la possibilité de nous contacter par téléphone. Vous êtes vous-même responsable des messages ou du contenu que vous nous envoyez par téléphone (par ex. : les commandes, les demandes d'achat, les demandes générales, etc.).

Afin de pouvoir répondre à vos questions, nous pouvons vous demander de nous fournir des informations supplémentaires, par exemple votre nom complet, votre adresse, votre adresse e-mail, etc. Nous ne recueillerons de vous que les données personnelles qui sont nécessaires pour vous identifier (y compris votre numéro de téléphone) et pour répondre à vos questions de la meilleure manière possible ou pour fournir les services que vous avez demandés.

Le traitement de ces données est donc nécessaire à la mise en œuvre de mesures précontractuelles ou contractuelles conformément à l'art. 13 al. 2 lit. a LPD/31 al. 2 let. a nLPD ou à l'art. 6 al. 1 lit. b RGPD ou est dans notre intérêt légitime conformément à l'art. 13 al. 1 LPD/31 al.1 nLPD ou à l'art. 6 al. 1 lit. f RGPD.

Contact par email, fax ou courrier

Vous avez la possibilité de nous contacter par e-mail ou par courrier. Vous êtes seul responsable des messages ou du contenu que vous nous envoyez de cette manière. Nous vous recommandons de ne pas transmettre d'informations sensibles. Seules les données personnelles que vous nous communiquez volontairement seront collectées. Vous décidez donc des informations que vous nous envoyez.

Afin de répondre à votre demande par e-mail, nous pouvons vous demander de nous fournir des informations supplémentaires, telles que votre nom complet, votre adresse, votre numéro de téléphone, etc. Nous ne recueillerons que les données personnelles qui sont nécessaires pour vous identifier (y compris votre adresse e-mail) et pour répondre à votre demande de la meilleure façon possible.

Le traitement de ces données est donc nécessaire à la mise en œuvre de mesures précontractuelles ou contractuelles conformément à l'art. 13 al. 2 lit. a LPD/31 al. 2 let. a nLPD ou à l'art. 6 al. 1 lit. b RGPD ou est dans notre intérêt légitime conformément à l'art. 13 al. 1 LPD/31 al. 1 nLDP ou à l'art. 6 al. 1 lit. f RGPD.

Utilisation d'un formulaire de contact

Vous avez la possibilité d'utiliser un formulaire de contact pour prendre contact avec nous. Pour cela, nous avons besoin des informations suivantes :

- Titre*
- Nom et prénom*
- Intitulé du poste (pour les clients professionnels)
- Entreprise (pour les clients professionnels)
- Fonction (pour les clients professionnels)
- Adresse*
- Téléphone
- e-mail*
- Remarques*

Les informations marquées d'un (*) sont obligatoires.

Nous utilisons ces données uniquement pour répondre à votre demande de contact de la meilleure façon possible et personnalisée. Le traitement de ces données est donc nécessaire à la mise en œuvre de mesures précontractuelles ou contractuelles conformément à l'art. 13 al. 2 lit. a LPD/31 al. 2 let. a nLPD ou à l'art. 6 al. 1 lit. b RGPD ou est dans notre intérêt légitime conformément à l'art. 13 al. 1 LPD/31 al. 1 nLPD ou à l'art. 6 al. 1 lit. f RGPD.

Achat dans la boutique en ligne (catalogue de produits)

Si vous disposez d'un compte utilisateur, vous pouvez passer des commandes à partir de notre catalogue de produits sur notre site web. Les données suivantes doivent être fournies lors de la commande de produits :

- Numéro de client
- Adresse*
- Téléphone
- E-mail*
- Notification et type d'expédition
- Personnel de terrain
- Centre régional

Les informations marquées d'un (*) sont obligatoires.

Nous utilisons ces données pour répondre aux demandes et aux commandes de la meilleure façon possible et de manière personnalisée. Le traitement de ces données est donc nécessaire à la mise en œuvre de mesures précontractuelles ou contractuelles conformément à l'art. 13 al. 2 lit. a LPD/31 al. 2 let. a nLPD ou à l'art. 6 al. 1 lit. b RGPD ou est dans notre intérêt légitime conformément à l'art. 13 al. 1 LPD/31 al.1 nLPD ou à l'art. 6 al. 1 lit. f RGPD.

Candidature à un poste ouvert

Sur notre site web, vous avez la possibilité de postuler à des postes ouverts en utilisant notre formulaire en ligne. À l'occasion de la demande en ligne, les données suivantes seront traitées :

Données personnelles :

- Poste ouvert*
- Nom et prénom*
- Lieu de résidence et pays*
- Code postal*
- Lieu*
- E-mail*
- Téléphone*
- Date de naissance*
- Fonction professionnelle et employeur actuels*
- Type de source de la candidature*

Documents :

- Curriculum vitae*
- Lettre de motivation*
- Certificats et diplômes*

Les informations marquées d'un (*) sont obligatoires.

Nous avons besoin de ces informations pour examiner votre candidature et pour la mise en œuvre éventuelle de la procédure de candidature. La base juridique du traitement de vos données personnelles est constituée par les mesures précontractuelles ou contractuelles conformément à l'art. 13 al. 2 lit. a LPD/31 al.2 let. a nLPD ou à l'art. 6 al. 1 lit. b RGPD ou est dans notre intérêt légitime conformément à l'art. 13 al. 1 LPD/31 al. 1 nLPD ou à l'art. 6 al. 1 lit. f RGPD.

Abonnement à notre newsletter et marketing par e-mail

Sur notre site web, vous avez la possibilité de vous abonner à notre lettre d'information. Un enregistrement est nécessaire à cet effet. Les données suivantes doivent être soumises lors de l'enregistrement :

- Titre
- Nom et prénom
- Adresse électronique*

Les informations marquées d'un (*) sont obligatoires.

Après avoir saisi les informations ci-dessus, vous pouvez déclencher l'inscription à notre newsletter. Nous utilisons le mécanisme dit "Double-Opt-In". Après avoir envoyé l'inscription, vous recevrez un email de notre part contenant un lien de confirmation. Pour vous inscrire définitivement à la newsletter, vous devez cliquer sur ce lien. Si vous ne cliquez pas sur le lien de confirmation, l'adresse électronique figurant dans notre liste temporaire d'abonnés à la newsletter sera définitivement supprimée au bout de 24 heures et aucun abonnement ne sera effectué.

Nous utiliserons vos données pour l'envoi de la newsletter jusqu'à ce que vous révoquiez votre consentement. Vous pouvez révoquer votre consentement à tout moment avec effet pour l'avenir ou cliquer sur le lien de désabonnement dans les e-mails de la newsletter.

Notre newsletter d'information contient les web-beacons (balises web) ou un moyen technique similaire (pixels espion). Les web-beacons sont des graphiques invisibles de 1x1 pixel qui sont associés à l'ID utilisateur de l'abonné à la newsletter correspondant. Les web-beacons nous donnent les informations suivantes sur l'envoi de la newsletter :

- Fichier d'adresses utilisé ;
- Objet et nombre des newsletters envoyées ;
- Informations sur les adresses qui ont reçu ou non la newsletter et sur les adresses où l'envoi a échoué ;
- Informations sur les adresses à partir desquelles la newsletter a été ouverte ;
- Informations sur les adresses qui ont été supprimées
- Informations techniques (par exemple, l'heure de la recherche, l'adresse IP, le type de navigateur et le système d'exploitation).

Ces informations sont utilisées pour l'analyse statistique de l'envoi de notre newsletter. Les résultats de ces analyses peuvent être utilisés pour mieux adapter les futures newsletters aux intérêts des destinataires. Les web-beacons sont supprimée lorsque vous supprimez la newsletter.

Pour empêcher l'utilisation des web-beacons, vous pouvez paramétrer votre programme de messagerie de manière à ce qu'aucun HTML ne soit affiché dans les messages, si ce n'est déjà le cas par défaut. Dans les pages suivantes, vous trouverez des explications sur la manière de procéder à ce réglage dans les programmes d'email les plus courants.

- Microsoft Outlook
- Mail für Mac ("Charger le contenu supprimé dans les messages")

En vous inscrivant à la newsletter, vous nous donnez votre accord pour le traitement des données fournies pour l'envoi régulier de la newsletter à l'adresse que vous nous avez indiquée ainsi que pour l'évaluation statistique du comportement d'utilisation et l'optimisation de la newsletter. Ce consentement constitue notre base légale pour le traitement des données conformément à l'art. 13 al. 1 LPD/31 al.1 nLPD et à l'art. 6 al. 1 lit. a RGPD. Vous pouvez révoquer votre consentement à tout moment avec effet pour l'avenir.

Cookies

Les cookies contribuent de nombreuses façons à rendre votre visite sur notre site web plus facile, plus agréable et plus significative. Les cookies sont des fichiers d'information que votre navigateur Internet enregistre automatiquement sur le disque dur de votre ordinateur lorsque vous visitez notre site web.

Nous utilisons des cookies, par exemple, pour enregistrer temporairement les services et les entrées que vous avez sélectionnés lorsque vous remplissez un formulaire sur nos pages web, afin que vous n'ayez pas à répéter l'entrée lorsque vous appelez une autre sous-page.

La plupart des navigateurs Internet acceptent automatiquement les cookies. Cependant, vous pouvez configurer votre navigateur de manière à ce qu'aucun cookie ne soit stocké sur votre ordinateur ou qu'un message apparaisse à chaque fois que vous recevez un nouveau cookie. Vous trouverez dans les pages suivantes des explications sur la manière de configurer le traitement des cookies avec les navigateurs les plus courants :

- Microsoft Windows Internet Explorer
- Microsoft Windows Internet Explorer pour les mobiles
- Mozilla Firefox
- Google Chrome de bureau
- Google Chrome pour les mobiles
- Apple Safari de bureau
- Apple Safari pour les mobiles

La désactivation des cookies peut signifier que vous ne pourrez pas utiliser toutes les fonctionnalités de nos sites web.

La base juridique du traitement des données personnelles aux fins susmentionnées est dans notre intérêt légitime, conformément à l'art. 13 al. 1 LPD/31 al. 1 nLPD et à l'art. 6 al. 1 lit. f RGPD, de garantir la fonctionnalité et l'optimisation de nos pages Web. Dans le cas des cookies purement analytiques, nous basons le traitement de vos données personnelles sur votre consentement, que vous donnez via la bannière de cookie.

Tracking-tools / Outils de suivi

A. Google Analytics

Les sites web utilisent Google Analytics, un service d'analyse web de Google Inc., 1600 Amphitheatre Pkwy, Mountain View, CA 94043-1351, USA. Google Analytics utilise des méthodes qui permettent d'analyser l'utilisation de nos sites web, telles que les cookies (voir rubrique "Cookies"). Les informations suivantes sont générées par le cookie concernant votre utilisation de nos sites.

Chemin de navigation du visiteur sur nos sites :

- Durée de séjour sur la page ou sous-page,
- Sous-page à partir de laquelle le site Internet est quitté,
- Pays, région, ou ville d'où le site est accédé,
- Dispositif (type, version, résolution, largeur et hauteur de la fenêtre du navigateur),
- Visiteur récurrent ou nouveau visiteur,
- Type et version du navigateur,
- Système d'exploitation utilisé,
- URL de référence (la page visitée précédemment),
- Nom d'hôte de l'ordinateur accédant (adresse IP)
- Heure de l'interrogation du serveur.

Ces informations sont transmises à un serveur de Google, une société de la société holding Alphabet Inc., aux États-Unis et elles y sont stockées. Du fait de l'activation de l'anonymisation des IP sur ce site web, l'adresse IP est raccourcie avant la transmission aux États-Unis (**anonymizeIP**). L'adresse IP anonymisée transmise par votre navigateur dans le cadre de Google Analytics n'est pas combinée avec d'autres données de Google. Ce n'est que dans des cas exceptionnels que l'adresse IP complète sera transférée à un serveur de Google aux États-Unis et y sera raccourcie. Dans ces cas, nous nous assurons, par un contrat de garantie, que Google respecte un niveau adéquat de protection des données.

Les informations sont utilisées pour évaluer l'utilisation de nos pages web, pour composer des rapports sur les activités menées sur nos pages web et pour fournir d'autres services liés à l'utilisation de nos pages web et à l'utilisation d'Internet à des fins d'études de marché et d'organisation de notre site Internet conformément aux besoins. Ces informations peuvent également être transférées à des tiers lorsque la loi l'exige ou lorsque des tiers traitent ces données pour le compte de Google. Selon Google, en aucun cas l'adresse IP n'est mise en relation avec d'autres informations concernant l'utilisateur.

Les utilisateurs peuvent empêcher la collecte des données générées par le cookie et liées à l'utilisation du site web par l'utilisateur concerné (y compris l'adresse IP) à Google et le traitement de ces données par Google en téléchargeant et en installant le plugin du navigateur disponible sous ce lien. Vous trouverez de plus amples informations sur le service d'analyse web utilisé sur le site web de Google Analytics.

Ce traitement est fondé sur notre intérêt légitime au sens de l'article 6 al. 1 lit. f RGPD.

B. Google Maps

Nous utilisons Google Maps API (Application Programming Interface, **Google Maps**) de Google Inc, 1600 Amphitheatre Pkwy, Mountain View, CA 94043-1351, USA, sur nos sites web pour la présentation visuelle des informations géographiques. En utilisant Google Maps, les informations relatives à l'utilisation de notre site web, y compris votre adresse IP, sont transmises à un serveur de Google aux États-Unis et y sont stockées.

La base juridique pour le traitement des données à cette fin réside dans notre intérêt légitime conformément à l'article 6 al. 1 lit. f RGPD.

Il est possible de désactiver Google Maps et d'empêcher le transfert de données vers Google en désactivant JavaScript dans votre navigateur. Toutefois, nous tenons à souligner que dans ce cas, vous ne pourrez pas utiliser l'affichage de la carte. Vous trouverez de plus amples informations sur la collecte, le traitement et l'utilisation de vos données par Google ainsi que sur vos droits à cet égard ici dans la Politique de Protection des Données Personnelles de Google et ici dans les conditions d'utilisation supplémentaires de Google Maps ou Google Earth. Le fait de ne pas désactiver les services concernés sera considéré comme un consentement au traitement des données à cette fin et un consentement au transfert de données vers les États-Unis (voir section 17, deuxième et troisième paragraphes).

Réseaux sociaux

Nos sites web peuvent contenir des liens vers des réseaux sociaux. Les liens ne conduisent pas à la transmission de données au fournisseur sans que l'utilisateur n'ait d'influence lors du chargement de nos pages web (pas de "plugins"). Derrière les boutons des réseaux sociaux, il n'y a qu'un lien vers notre présence sur le réseau concerné. Aucune donnée d'utilisateur n'est transmise de nos sites web au réseau social.

Nos sites web peuvent comporter les liens suivants :

- Facebook de Facebook Ireland Ltd, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland, respectivement Facebook Inc, 1601 S. California Ave, Palo Alto, CA 94304, USA
- Instagram de Instagram Inc, 1601 Willow Road, Menlo Park, CA 94025, États-Unis
- YouTube géré par Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, respectivement Google Inc, 1600 Amphitheatre Pkwy, Mountain View, CA 94043-1351, USA
- LinkedIn de LinkedIn Corporation, 2029 Stierlin Court, Mountain View, CA 94043, États-Unis

Lorsque vous appelez un lien vers l'un de nos profils de réseau, une connexion directe est établie entre votre navigateur et le serveur du réseau social concerné. Le réseau est ainsi informé que vous avez utilisé votre adresse IP pour visiter nos sites web et appeler le lien. Si vous vous connectez à un réseau alors que vous êtes connecté à votre compte sur ce réseau, le contenu de nos sites peut être lié à votre profil sur le réseau, ce qui signifie que le réseau peut associer votre visite sur nos sites web directement à votre compte. Si vous souhaitez éviter cela, vous devez vous déconnecter avant de cliquer sur un lien. Dans tous les cas, une mission a lieu lorsque vous vous connectez au réseau en question après avoir cliqué sur le lien.

La base légale pour le traitement des données à cette fin est dans notre intérêt légitime selon l'art. 13 al. 1 LPD/31 al. 1 nLPD et l'art. 6 al. 1 lit. f RGPD.

Période de rétention

Nous conservons les données personnelles aussi longtemps que nécessaire pour la fourniture des services susmentionnés ainsi que pour le traitement ultérieur dans le cadre de notre intérêt légitime conformément à l'art. 13 al. 1 et al. 2 lit. a LPD/31 al. A et al. 2 let. a nLPD et à l'art. 6 al. 1, lit. b et f RGPD.

Les données contractuelles seront conservées par nous pendant une période plus longue si cela est prescrit par les obligations légales de conservation ou si nous avons un autre intérêt légitime à le faire. Les obligations de stockage qui nous obligent à conserver des données résultent notamment des réglementations en matière de droit comptable et fiscal. Selon cette réglementation, les communications commerciales, les contrats conclus et les pièces comptables doivent être conservés pendant dix ans après la fin de l'année au cours de laquelle ils ont été traités pour la dernière fois. Si nous n'avons plus besoin de ces données pour la prestation de services pour vous ou dans le cadre d'autres intérêts légitimes, les données seront bloquées. Cela signifie que les données ne peuvent alors être utilisées qu'à des fins comptables et fiscales.

Transfert de données à des tiers

Nous ne transmettons vos données personnelles que si vous y avez expressément consenti, s'il existe une obligation légale de le faire ou si cela est nécessaire pour remplir nos obligations contractuelles ou pour faire valoir nos droits, en particulier pour faire valoir des créances découlant de la relation contractuelle. En outre, nous transmettons vos données à des tiers dans la mesure où cela est nécessaire dans le cadre de l'utilisation de nos sites web ou de l'application et de l'exécution du contrat (également en dehors de nos sites web).

Certains tiers ont déjà été mentionnés (Google Inc.). Nos sites web sont hébergés sur des serveurs en Suisse. Les données sont transmises dans le but de remplir nos obligations précontractuelles et contractuelles et de fournir et maintenir les fonctionnalités de notre site web et de nos applications. C'est notre intérêt légitime selon l'art. 13 al. 1 et al. 2 lit. a LPD/31 al. 1 et al.2 let. a nLPD et l'art. 6 al. 1 lit. b et f RGPD.

Transfert de données à caractère personnel à l'étranger

Nous pouvons également transférer vos données personnelles à des sociétés tierces (prestataires de services mandatés) à l'étranger aux fins du traitement des données décrit dans la présente politique de protection des données personnelles. Ces entreprises sont tenues, dans la même mesure que nous, de protéger vos données. Si le niveau de protection des données dans un pays ne correspond pas à celui de la Suisse ou de l'UE, nous veillerons par contrat préalablement communiqué au PFPDT à ce que la protection de vos données personnelles corresponde à tout moment à celle de la Suisse ou de l'UE.

Par souci d'exhaustivité, nous notons que dans le cadre de la législation américaine, les autorités américaines peuvent prendre des mesures de surveillance et accéder aux données, qui peuvent également inclure des données transférées de la Suisse ou de l'Union européenne vers les États-Unis. Cela se fait sans distinction, restriction ou exception fondée sur l'objectif poursuivi et sans critères objectifs qui permettraient de limiter l'accès des autorités américaines aux données à caractère personnel et leur utilisation ultérieure à certaines fins strictement limitées qui justifieraient l'accès à ces données.

En outre, aux États-Unis il n'existe aucun recours juridique pour les personnes concernées des États membres de l'UE ou de la Suisse qui leur permettrait d'accéder, de rectifier ou de supprimer des données les concernant qui font l'objet d'une action gouvernementale, et il n'existe aucune protection juridique efficace contre les droits d'accès généraux des autorités américaines.

Nous tenons à signaler aux utilisateurs résidant en Suisse ou dans un État membre de l'UE que de l'avis des autorités compétentes en Suisse et dans l'Union européenne - en partie à cause des problèmes

mentionnés dans cette section - les États-Unis ne disposent pas d'un niveau de protection des données adéquat. Si les destinataires des données (par exemple, Google) sont basés aux États-Unis ou sont censés effectuer le traitement des données pertinentes aux États-Unis, nous prendrons toutes les mesures raisonnables pour garantir que vos données sont protégées à un niveau approprié avec nos partenaires par des accords contractuels avec ces sociétés et, si nécessaire, par des garanties supplémentaires pour protéger les droits des personnes dont les données personnelles sont transférées vers un pays tiers.

Nous attirons expressément votre attention sur cette situation juridique et factuelle afin que vous puissiez prendre une décision éclairée quant à votre consentement à la divulgation de vos données à des personnes qui sont domiciliées aux États-Unis ou qui sont susceptibles d'effectuer le traitement des données concernées aux États-Unis.

2. Informations complémentaires

Droit d'information, de rectification, d'annulation et de limitation du traitement ; droit de transfert des données

Vous pouvez vous opposer à tout moment au traitement des données, notamment au traitement des données en rapport avec la publicité directe (par exemple contre les courriers électroniques publicitaires). Vous avez également les droits suivants :

Droit à l'information : Vous avez le droit d'exiger à tout moment un accès gratuit aux données personnelles vous concernant qui sont stockées chez nous si nous les traitons. Cela vous donne la possibilité de vérifier quelles données personnelles nous traitons à votre sujet et que nous les utilisons conformément aux réglementations applicables en matière de protection des données.

Droit de rectification : Vous avez le droit de faire rectifier des données à caractère personnel incorrectes ou incomplètes et d'être informé de la rectification. Dans ce cas, nous informerons les destinataires des données concernées des ajustements effectués, à moins que cela ne soit impossible ou n'implique un effort disproportionné.

Droit d'annulation : Vous avez le droit de demander la suppression de vos données personnelles dans certaines circonstances. Dans des cas individuels, le droit de suppression peut être exclu.

Droit à la restriction du traitement : Sous certaines conditions, vous avez le droit de demander que le traitement de vos données à caractère personnel soit limité.

Droit de recours : Vous avez le droit de faire appel auprès d'une autorité de contrôle compétente contre la manière dont vos données à caractère personnel sont traitées.
Droit à la portabilité des données: Si vous êtes domicilié hors de Suisse et que vous résidez dans un État membre de l'UE/EEE, vous avez dans certaines circonstances le droit de recevoir de notre part les données personnelles que vous nous avez fournies gratuitement et sous une forme lisible.

Droit de déposer une plainte auprès d'une autorité de contrôle: Vous avez le droit de déposer une plainte auprès d'une autorité de contrôle compétente si vous estimez que le traitement de données à caractère personnel vous concernant enfreint la réglementation applicable en matière de protection des données.

Droit de révocation : En principe vous avez le droit de révoquer à tout moment un consentement donné. Les activités de traitement fondées sur votre consentement passé ne deviennent pas illégales de par votre révocation.

Sécurité des données

Nous utilisons des mesures de sécurité techniques et organisationnelles appropriées pour protéger vos données personnelles stockées chez nous contre la manipulation, la perte partielle ou totale et contre l'accès non autorisé de tiers. Nos mesures de sécurité sont constamment améliorées en fonction des évolutions technologiques.

Nous prenons également très au sérieux la protection interne des données. Nos employés et les entreprises de services que nous mandatons ont été obligés par nous de maintenir la confidentialité et de respecter les réglementations relatives à la protection des données.

Dernière mise à jour : mars 2023

Annexe 2 : modèle « Clause de confidentialité RH »

Clause de confidentialité

PME est responsable de la collecte, du traitement et de l'utilisation de vos données personnelles dans le cadre de la gestion des ressources humaines.

Dans ce contexte, nous sommes susceptibles de collecter les informations suivantes vous concernant :

- Noms
- Prénoms
- Date de naissance
- Adresse privée
- Numéros de téléphones
- Numéro AVS
- Nationalité et/ou origine
- Piece d'identité
- Permis de travail ou d'établissement pour les étrangers
- Genre
- Etat civil
- Noms, prénoms, date de naissance et genre du (de la) conjoint(e)
- Noms, prénoms, date de naissance et genre des enfants
- Certificat de famille
- Photos
- Curriculum vitae
- Lettre de motivation
- Copie des certificats et diplômes

Votre confiance est importante pour nous, c'est pourquoi nous prenons la protection des données au sérieux et assurons une sécurité appropriée dans l'application du droit suisse.

Si vous avez des questions ou des commentaires concernant notre traitement de données personnelles et la base juridique sur laquelle nous les traitons, vous pouvez nous contacter.

Vous avez les droits suivants :

Droit à l'information : Vous avez le droit d'exiger à tout moment un accès gratuit aux données personnelles vous concernant qui sont stockées chez nous si nous les traitons. Cela vous donne la possibilité de vérifier quelles données personnelles nous traitons à votre sujet et que nous les utilisons conformément aux réglementations applicables en matière de protection des données.

Droit de rectification : Vous avez le droit de faire rectifier des données à caractère personnel incorrectes ou incomplètes et d'être informé de la rectification. Dans ce cas, nous informerons les destinataires des données concernées des ajustements effectués, à moins que cela ne soit impossible ou n'implique un effort disproportionné.

Droit d'annulation : Vous avez le droit de demander la suppression de vos données personnelles dans certaines circonstances. Dans des cas individuels, le droit de suppression peut être exclu.

Droit à la restriction du traitement : Sous certaines conditions, vous avez le droit de demander que le traitement de vos données à caractère personnel soit limité.

Droit de recours : Vous avez le droit de faire appel auprès d'une autorité de contrôle compétente contre la manière dont vos données à caractère personnel sont traitées.

Droit à la portabilité des données : Si vous êtes domicilié hors de Suisse et que vous résidez dans un État membre de l'UE/EEE, vous avez dans certaines circonstances le droit de recevoir de notre part les données personnelles que vous nous avez fournies gratuitement et sous une forme lisible.

Droit de déposer une plainte auprès d'une autorité de contrôle : Vous avez le droit de déposer une plainte auprès d'une autorité de contrôle compétente si vous estimez que le traitement de données à caractère personnel vous concernant enfreint la réglementation applicable en matière de protection des données.

Droit de révocation : En principe vous avez le droit de révoquer à tout moment un consentement donné. Les activités de traitement fondées sur votre consentement passé ne sont pas illégales de par votre révocation.

Sécurité

Nous utilisons des mesures de sécurité techniques et organisationnelles appropriées pour protéger vos données personnelles stockées chez nous contre la manipulation, la perte partielle ou totale et contre l'accès non autorisé de tiers. Nos mesures de sécurité sont constamment améliorées en fonction des évolutions technologiques.

Nous prenons également très au sérieux la protection interne des données. Nos employés et les entreprises de services que nous mandatons ont été obligés par nous de maintenir la confidentialité et de respecter les réglementations relatives à la protection des données.

Période de rétention

Nous conservons les données personnelles aussi longtemps que nécessaire pour la fourniture des services susmentionnés ainsi que pour le traitement ultérieur dans le cadre de notre intérêt légitime.

Les données contractuelles seront conservées par nous pendant une période plus longue si cela est prescrit par les obligations légales de conservation ou si nous avons un autre intérêt légitime à le faire. Les obligations de stockage qui nous obligent à conserver des données résultent notamment des réglementations en matière de droit comptable, fiscal ou légales.

Traitements :
Ces données sont collectées et traitées et transmises dans les buts suivants :

Gestion des salaires :
Nous déléguons le calcul du salaire ainsi que l'établissement de tous les décomptes et certificats à la société OUTSOURCEUR DE SALAIRE sise à rue de l'adresse 1, 1000 Lausanne. Vos données personnelles ainsi que vos données de rémunération sont transmises via l'application en ligne site.ch

Assurances du 1er pilier :
Nous sommes affiliés pour les assurances AVS, AI, APG, AC auprès de la Caisse XXX. Vos données personnelles ainsi que vos données de rémunérations brutes et cotisations sont transmises via l'application en ligne site.ch et via l'interface https://www.swissdec.ch/fr/

Allocations familiales :
Nous sommes affiliés pour les AF auprès de la Caisse XXX. Vos données personnelles ainsi que vos données de rémunérations brutes et cotisations sont transmises via l'application en ligne site.ch et via l'interface https://www.swissdec.ch/fr/

Assurance perte de gain maladie :
Nous sommes assurés pour la perte de gain auprès de la compagnie xxx. Vos données personnelles, de rémunération ainsi que les données relatives aux événements de santé sont transmises via xxx.

Assurance accident :
Nous sommes assurés pour la LAA auprès de la compagnie xxx. Vos données personnelles, de rémunération ainsi que les données relatives aux événements de santé sont transmises via xxx.

Assurance prévoyance :
Nous sommes assurés pour la LPP auprès de la compagnie xxx. Vos données personnelles, de rémunération ainsi que les données relatives aux événements de vie (changement d'état civil, invalidité, retraite, etc.) sont transmises via xxx.

Courtier en assurances :
Nous utilisons les services de la société de courtage xxx. Vos données personnelles, de rémunération ainsi que les cas de maladie, accident sont transmises par courriel.

Gestion des compétences :
Nous utilisons les services en ligne de xxx. Vos données personnelles ainsi que l'ensemble de vos compétences et expériences sont référencées dans cet outil en vue de pouvoir valoriser votre profil dans nos appels d'offres.

Gestion des absences :
Nous utilisons le produit Cloud xyx pour la gestion des absences. Vos données personnelles ainsi que vos données d'absences (y.c. les périodes de maladie, accident, maternité, etc.) y sont référencées à des fins de gestion de soldes, de statistiques d'absentéisme et d'administration RH.

Gestions des notes de frais :
Nous utilisons le produit Cloud xyz pour la gestion des notes de frais. Vos données personnelles ainsi que vos données de frais y sont référencées dans le but de simplifier le processus administratif. Il est possible que nous fassions des statistiques sur ces données.

Dossier RH :
Votre dossier complet contenant vos données personnelles, contrats, avenants, dossier de candidature ainsi que tous les actes administratifs liés à la gestion RH de votre activité dans l'entreprise est stocké dans Microsoft Sharepoint. Sauf exigence d'une institution sociale, publique ou légale s'appuyant sur une demande légitime conforme à la Loi, le contenu de votre dossier n'est transmis à quiconque et reste à usage interne.

Egalité salariale :
Vos données personnelles, notamment votre numéro AVS ainsi que vos données de rémunération sont utilisés dans l'application LOGIB et transmises à la confédération dans le cas de l'analyse périodique de l'égalité salariale.

Devoir d'information relatif aux données du personnel

Les collaborateurs(trices) sont tenus de communiquer sans délais au service du personnel tout changement les concernant, tels que changement d'adresse, d'état civil, de prétention aux allocations familiales, de naissance ou de formations, en cas de décès d'un membre de famille proche, ou d'un diplôme acquis.

Droit à l'image et vidéosurveillance

Droit à l'image

Conformément aux dispositions relatives au droit à l'image, le collaborateur autorise PME SA à diffuser, sans limite de territoire ou de durée, les photographies et films pris lors de sorties d'entreprises, shooting ou divers événements dans le cadre du travail. Les photographies et films pourront être exploités et utilisés directement par PME SA. Cette autorisation comprend notamment le droit de reproduire et de communiquer ces éléments au public, par la diffusion lors de rendez-vous commerciaux, supports de communication, site internet et réseaux sociaux.

PME SA s'interdisent expressément de procéder à une exploitation des photographies susceptible de porter atteinte à la vie privée ou à la réputation.

Vidéosurveillance

Vu la nature des activités de Morphean SA, des caméras sont placées dans les environnements de l'entreprise, sans filmer spécifiquement le personnel à leur place de travail. Les collaborateurs(trices) ainsi que les visiteurs de nos sociétés sont informés de la présence des caméras de vidéosurveillance par des panneaux clairs et visibles installés à l'intérieur et à l'extérieur des lieux équipés d'une caméra.

Confidentialité

La préservation de la confidentialité, respectivement de la discrétion, est l'élément essentiel de la relation de confiance. Les collaborateurs s'engagent à ne révéler aucun fait destiné à rester confidentiels, tels que les secrets de fabrication, les affaires et toutes les questions dont ils ont eu connaissance pendant leur activité, que ces informations concernent la société, celle de nos clients ou les données personnelles traitées dans le cadre des missions. Cette obligation les lie même après la fin du contrat de travail. L'employé(e) accepte, si le cas se présente, de se soumettre aux règles de confidentialités du client chez lequel il/elle travaille.

Protection des données

Les données personnelles sont protégées conformément aux dispositions des articles 328 et 328b du Code suisse des obligations (protection des droits de la personnalité du travailleur) et de la loi suisse sur la protection des données.

Annexes 3 à 7 :

- Modèle « lettre PFPDT »
- Modèle « tableau registre des traitements »
- Modèle « liste des tâches »
- Modèle « revue annuelle »
- Modèle « fiche de registre »

Annexe 3 : Modèle « lettre PFPDT »

PME SA
Adresse 1
1000 Lausanne

Préposé Fédéral (PFPDT)
Feldeggweg 1
3003 Berne

Lieu, le DATE

Notification de la violation de données à caractère personnel

Monsieur le Préposé,

Par la présente, nous vous informons que notre entreprise a été victime le DATE d'une violation des données que nous collectons. En l'occurrence, …… collectés par nos services on fait l'objet de cette violation.

Celles-ci peuvent être décrites de la façon générale suivante :

…..

Les conséquences potentielles sont les suivantes :

…..

Nous mettons tout en œuvre pour remédier à ce problème de violation des données à caractère personnel et essayons d'atténuer au maximum les conséquences, notamment :

…..

Nous vous prions d'agréer, Monsieur le Préposé, nos salutations les plus sincères.

PME SA

Responsable du traitement des données

Coordonnées TEL + email

Annexe 4 : Modèle « tableau registre des traitements »

Loi sur la protection des données : Registre des traitements

Date de la dernière revue : indiquer la date

No activité	Groupe	Finalité de Traitement	Responsable	Catégories de personnes	Catégories de données	Catégories de destinataires	Délai de conservation	Sécurité	transfert hors UE	Risques oui/non	Commentaires
1	RH	Salaires, Impôts sources et certificats de salaire	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sous-traitants	10 ans après terme du contrat	Double authen. + sauvegarde	Non	non	
2	RH	Dossiers collaborateurs.trices	Prénon nom	Personnel sous contrat	Données sensibles	Internes et sous-traitants	Durée contractuelle		Non		
3	RH	Gestion des compétences /CV	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sous-traitants			Non		
4	RH	Entretien annuels et/ou spécifiques	Prénon nom	Personnel sous contrat	Données sensibles	Internes et sous-traitants			Non		
5	RH	Archivage des collaborateurs.trices partis.es	Prénon nom	Personnel parti	Données sensibles	Internes et sous-traitants			Non		
6	RH	Assurances sociales et courtier	Prénon nom	Personnel sous contrat	Données sensibles	Internes et sous-traitants			Non		
7	RH	Gestion des absences	Prénon nom	Personnel sous contrat	Données sensibles	Internes et sous-traitants			Non		
8	RH	Gestion de l'image pour notre marketing	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sous-traitants			Non		
9	RH	Formation	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sous-traitants			Non		
10	RH	Vidéosruveillance	Prénon nom	Toutes les personnes accédant nos locaux	Donnnées personnelles	Internes et sous-traitants			Non		
11	RH	Egalité des salaires	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sous-traitants			Non		
12	Recrutement	Gestion des candidatures	Prénon nom	Candidats	Donnnées personnelles	Internes et sous-traitants			Non		
13	Commercial	Gestion de la relation client (CRM)	Prénon nom	Personnes de contact clients	Donnnées personnelles	Internes et sous-traitants			Non		
14	Admin	Contrôle des heures et facturation	Prénon nom	Personnel sous contrat - soustraitants	Donnnées personnelles	Internes et sous-traitants			Non		
15	Admin	Signature électronique	Prénon nom	Candidats, personnel sous contrat et clients	Donnnées personnelles	Internes et sous-traitants			Non		
16	Admin	Gestion des fournisseurs / Achats	Prénon nom	Perssonnes de contact fournisseurs	Donnnées personnelles	Internes et sous-traitants			Non		
17	Marketing	Cookies sur le site internet	Prénon nom		données de navigation	Internes et sous-traitants			Non		
18	Marketing	Newsletter et inscriptions aux event	Prénon nom	Tiers externes	Donnnées personnelles	Internes et sous-traitants			Non		
19	IT	Support	Prénon nom	Personnes de contact clients	Donnnées personnelles	Internes et sous-traitants			Non		
20	IT	Gestion des identifications	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sous-traitants			Non		
21	IT	Logs	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sous-traitants			Non		
22	IT	Téléphonie mobile	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sous-traitants			Non		
23	Compta	notes de frais	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sous-traitants			Non		
24	Compta	Budget	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sous-traitants			Non		
25	Compta	ebanking	Prénon nom	Personnel sous contrat	Donnnées personnelles	Internes et sous-traitants			Non		

Annexe 5 : Modèle « liste des tâches »

Loi sur la protection des données : liste des tâches					
Date de la dernière revue : indiquer la date					
Date	**Activité**	**Responsable**	**Délai**	**Statut**	**Commentaire**
	Vérifier avec notre fournisseur informatique que la gestion des droits et mots de passe est efficiante et que ces droits soient limités aux seules personnes habilitées. Ceci particulièrement sur les données RH ou vos données sensibles				
	Vérifier avec notre fournisseur informatique que nos serveurs bénéficient en permanence des mises à jour de sécurité				
	Vérifier avec notre fournisseur informatique que nous disposons bien de protections cyber sur notre réseau informatique (notamment un firewall et un antispam)				
	Vérifier avec nos fournisseurs informatiques que des sauvegardes sont réalisées pour toutes nos données. S'assurer que les restaurations sont testées et qu'un plan de secours est prévu en cas de cyber attaque				
	Contrôler que les locaux sont sécurisés, l'accès aux dossiers papiers limités aux personnes habilitées				
	Adresser un courriers à chaque sous-traitants pour s'assurer qu'il respecte bien la nouvelle Loi				
	Intégrer la politique de confidentialité dans les contrats RH ou la faire signer par chaque salarié				
	Indiquer les clauses de sauvegarde des données dans les lettres de confirmation de résiliation de contrat de travail				
	Anonymiser les informations des collaborateurs partis dans l'AD (système d'accès au réseau informatique)				
	Publier une politque de confidentialité pour notre site internet / candidatures				
	Ecrire une clause de conservation des données dans les réponses négatives recrutement				
	Penser à traduire les politiques de sécurité dans les langues utilisées				
	Banière des coockies à installer sur nos sites web avec lien sur la politque				
	Transférer nos sites web en Suisse				
	Disposer d'une clause contractuelle à intégrer dans tous nos nouveaux contrats sous-traitants				
	Ajouter une clause d'information dans notre newsletter avec possibilité de se désincrire				
	Faire une formation interne de sensibilisation du personnel aux risques cyber et protection des données				
	Organiser une sensibilisation cyber et protection des données pour chaque nouvel(le) employé				
	S'assurer qu'aucune donnée sensible n'est stockée/traitée dans des environnements (applications				
	Vérifier d'avoir des sauvegardes cryptées si elles sont externalisées				
	Revue complète des documents avant mise en application				
	Intégration de la revue annuelle nLPD dans le manuel qualité ISO				

Annexe 6 : Modèle « revue annuelle »

Loi sur la protection des données : Revue Annuelle					
Date de la dernière revue :		indiquer la date			
ID	**Activité**	**Responsable**	**Statut**	**Résultat**	**Commentaire**
1	Revue de la politique de sécurité				
2	Revue du registre des traitements (ajout / suppression / modification)				
3	Revue des responsables de registres par traitement (idem)				
4	Revue de chaque traitement (idem)				
5	Revue des sous-traitants (idem)				
6	Revue de la politique de confidentialité en ligne				
7	Revue de la politique de confidentialité RH				
8	Revue des risques				
9	Elaboration d'un plan d'action si nécessaire				
10	Rapport à la direction				
11	Planifier la revue pour l'année prochaine				

Annexe 7 : Modèle « fiche de registre »

Fiche de registre n°

Activité : x

Coordonnées du responsable de traitement	• PME SA, adresse 1, 1000 Lausanne • Tél : 000/000.00.00 • E-mail : info@pme.com
Nom et coordonnées de la personne responsable	
Date de la dernière revue	

1. Objectifs poursuivis (Finalités)

Décrire clairement l'objet du traitement de données personnelles et dans quel but les données sont récoltées

2. Catégories de personnes concernées

Lister les différents types de personnes dont l'organisme collecte ou utilise les données
(Ex. : salariés, usagers, clients, prospects, bénéficiaires, etc.)

-
-

3. Catégories de données collectées

Lister les différentes données traitées

☐ Etat-civil, identité, données d'identification, images (*nom, prénom, adresse, photographie, date, lieu de naissance, etc.)* Cochez ici

☐ Vie personnelle (*habitudes de vie, situation familiale, etc.)* Cochez ici

☐ Vie professionnelle (*CV, situation professionnelle, scolarité, formation, distinction, diplômes, etc.)* Cochez ici

☐ Informations d'ordre économique et financier (R*evenus, situation financière, données bancaires, etc.*) Cochez ici

☐ Données de connexion (*adresse Ip, logs, identifiants des terminaux, identifiants de connexion, information d'horodatage, etc.*) Cochez ici

☐ Données de localisation (*déplacements, données GPS, GSM, etc.)* Cochez ici

☐ Internet *(cookies, traceurs, données de navigation, mesures d'audience etc.)* Cochez ici

☐ Autres catégories de données *(précisez)* Cochez ici

Lesquelles ? _____

Des données sensibles sont-elles traitées ?

La collecte de certaines données particulièrement sensible, est strictement encadrée par la LPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique.

☐ Oui ☐ Non Cochez ici

Si oui lesquelles ? _____

4. Durée de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

☐ ___ jours ☐ ___ mois ☐ ___ ans

☐ Autre durée : _____

Si vous ne pouvez pas indiquer une durée chiffrée, précisez les critères utilisés pour déterminer le délai d'effacement (ex. : 3 ans à compter de la fin de la relation contractuelle).

5. Catégories de destinataires de données

Destinataires internes
(Ex. : entité ou service, catégories de personnes habilitées, direction informatique, etc.)

Organismes externes
(Ex. : filiales, partenaires, etc.)

Sous-traitants
(Ex. : hébergeurs, prestataires et maintenance informatique, etc.)

6. Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'UE ?

☐ Oui ☐ Non Cochez ici.

Si oui, vers quel(s) pays?

7. Mesures de sécurité

Décrire les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

☐ Contrôle d'accès des utilisateurs
Décrire les mesures :

☐ Mesures de traçabilité
Préciser la nature des traces (*ex. : journalisation des accès des utilisateurs),* les données enregistrées (*ex. : identifiant, date et heure de connexion, etc.) e*t leur durée de conservation :

☐ Mesures de protection des logiciels (*ex. : antivirus, mise à jour et correctifs de sécurité, tests, etc.)*
Décrire les mesures :

☐ Sauvegarde des données
Décrire les modalités :

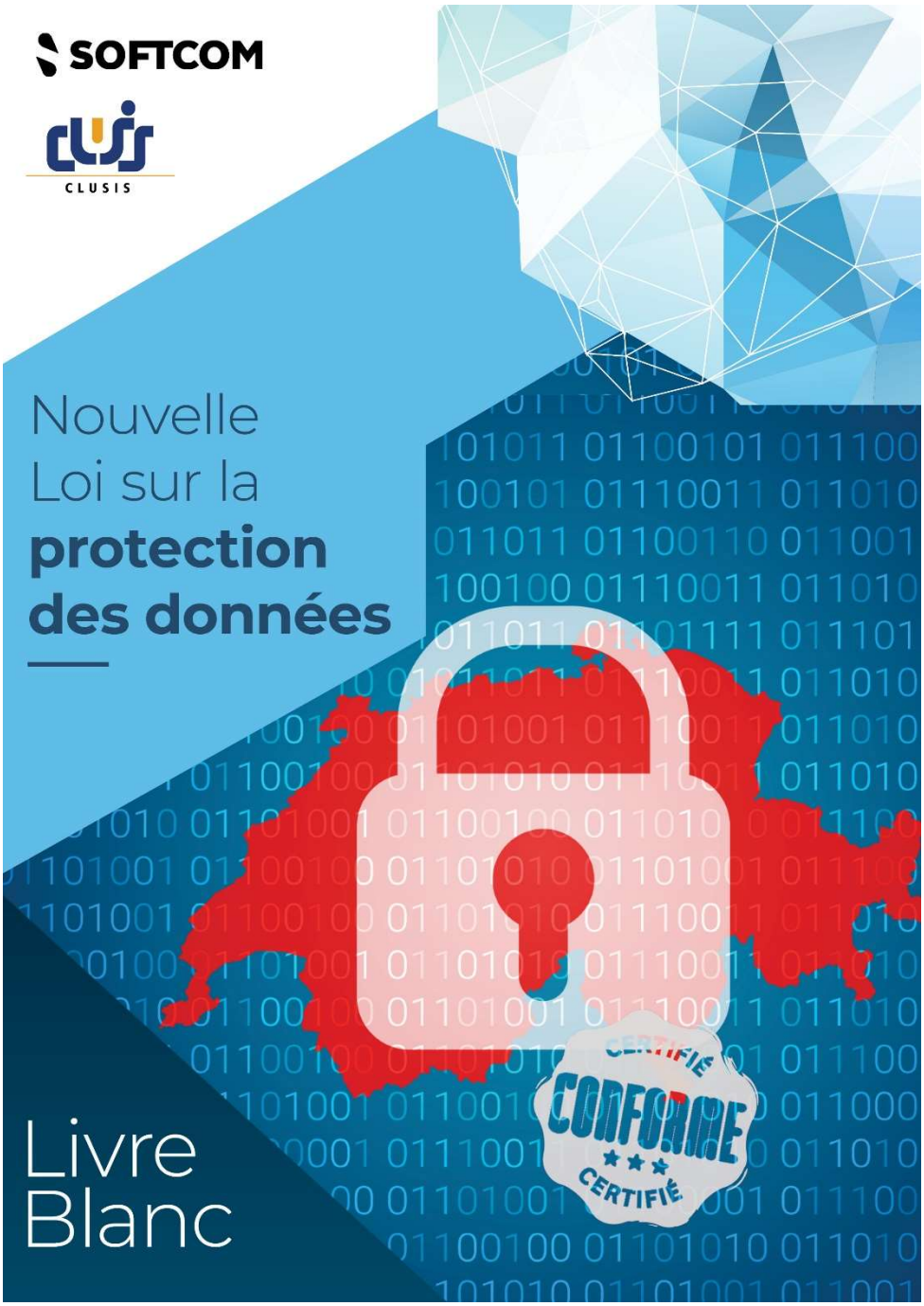
☐ Chiffrement des données
Décrire les mesures (e*x. : site accessible en https ; utilisation de TLS, etc.) :*

☐ Contrôle des sous-traitants
Décrire les modalités :

☐ Autre mesures :

Annexe 8 & 9 :

- Modèle « lettre sous-traitant »
- Modèle « contrat de sous-traitance »



Annexe 8 : modèle « lettre sous-traitant »

PME SA
Adresse 1
1000 Lausanne

Sous-taitant X
Adresse 2
1000 Lausanne

Respect de la nouvelle Loi sur la protection des données

Madame, Monsieur,

Nous nous référons à l'entrée en vigueur de la nouvelle Loi sur la protection des données au 1er septembre 2023.

Dans le cadre de nos activités, nous vous sous-traitons la gestion de …… (éventuellement au travers de l'utilisation du site/logiciel xxxxxx), traitements qui impliquent l'exploitation de données personnelles.

Nous vous prions dès lors de nous confirmer les éléments suivants :

Vous déclarez et garantissez que l'usage qu'il fera des données respectera en tous points les principes énoncés dans notre mandat et que vous vous interdisez tout traitement ou usage des données qui serait contraire au contrat. À cet effet, et sans que cette énumération soit limitative, vous vous engagez en particulier à respecter les obligations suivantes :

- ✓ L'hébergement des données est exclusivement en Suisse.
- ✓ Vous disposez d'une liste désignant par leur fonction les personnes concernées par le traitement.
- ✓ Vous vous assurez que les données sont protégées contre un emploi abusif en prenant des mesures organisationnelles et techniques appropriées ; vous veillez à l'intégrité, à la disponibilité et à la confidentialité des données. Les mesures seront plus élevées s'il s'agit de données sensibles.
- ✓ Vous vous engagez à ne pas sous-traiter à votre tour les données sans notre accord express.
- ✓ Vous faites signer à votre personnel un engagement à respecter la protection des données
- ✓ Vous faites usage des données pour les finalités suivantes, à l'exclusion de toutes autres, à savoir : [*les énumérer*] ;

- ✓ Vous nous Informerez immédiatement si vous n'êtes plus en mesure de respecter ces conditions, si n'importe quel accès accidentel, non autorisé ou non convenu a eu lieu.

- ✓ Vous vous interdisez de traiter des données à caractère personnel révélant l'origine raciale, les opinions politiques ou les convictions religieuses ou autres, ainsi que toutes données à caractère personnel concernant la santé ou la vie sexuelle ou le casier judiciaire, à moins que ce traitement ne soit régi par les garanties qui auraient été appliquées en vertu du droit interne de notre part.

- ✓ Vous Exploitez les données exclusivement pour votre usage personnel et ne communiquerez les données, gratuitement ou contre paiement, à aucune autre personne morale ou physique, sauf en cas d'obligation prévue par votre droit interne et mentionnée expressément.

- ✓ Vous rectifierez, effacerez et mettrez à jour immédiatement les données, dès que vous aurez reçu les instructions à cet effet.

- ✓ Vous garantissez aux personnes concernées le droit d'accès à leurs données ainsi que le droit de rectification et d'effacement de celles-ci dans les mêmes conditions qu'en vertu du droit interne de notre relation.

- ✓ Vous vous soumettez aux mêmes contrôles que ceux auxquels nous sommes soumis, notamment à ceux du PFPDT.

- ✓ Respectez la durée de conservation convenue et effacez les données si nous le demandons.

- ✓ Vous choisissez e personnel chargé du traitement avec soin et assurez sa formation concernant la protection des données.

Dans l'attente de vos confirmations, nous vous prions d'agréer, Madame, Monsieur, nos meilleures salutations.

PME SA

Nom

Annexe 9 : Modèle « contrat de sous-traitance »

Table des matières du contrat de sous-traitance

Modèle de Contrat entre les parties

La société privée à responsabilité limitée <**Société**>, dont le siège social est <adresse>, représentée par son administrateur <nom>, ci-après dénommée « **Responsable du traitement** ».

et

La société privée à responsabilité limitée **PME SA**, dont le siège social est situé en Suisse (Adresse), représentée par son(ses) directeur(s) <nom(s)>, ci-après dénommée « **Sous-traitant** ».

Tandis que :

- Le Responsable du traitement souhaite que le Sous-traitant traite les données à caractère personnel pour la mise en œuvre du Contrat de sous-traitance conclu avec le Sous-traitant le **<date>** (ci-après : le « **Contrat** »).
- Le Sous-traitant, qui traite des données à caractère personnel dans le cadre de la mise en œuvre du contrat conclu avec le responsable du traitement, peut être considéré comme le Sous-traitant au sens du règlement général sur la protection des données (ci-après : « **RGPD / LPD** »), tandis que le Responsable du traitement peut être considéré comme le Responsable du traitement au sens du RGPD / LPD.
- Toute référence aux données personnelles dans le présent Contrat de sous-traitance fait référence aux données à caractère personnel au sens de l'article 4, paragraphe 1, du RGPD.
- Compte tenu également de l'exigence énoncée à l'article 28, paragraphe 9, du RGPD, les parties souhaitent saisir leurs droits et obligations par écrit au moyen du présent Contrat de sous-traitance.

Est convenu ce qui suit :

Finalités du traitement

1.1. Le Sous-traitant s'engage à traiter les données personnelles sous réserve des conditions du présent Contrat de Sous-traitance tel que commandé par le Responsable du traitement. Le traitement n'aura lieu que dans le cadre du Contrat de sous-traitance et concernera exclusivement les catégories de données à caractère personnel spécifiées à **l'annexe A**.

1.2. Le Sous-traitant ne traitera pas les données personnelles à d'autres fins que celles énumérées à **l'Annexe A**.

1.3. Le Sous-traitant n'a aucun contrôle sur la finalité et les ressources utilisées pour traiter les données personnelles. Le Sous-traitant ne prend aucune décision concernant la réception et l'utilisation des données personnelles, la fourniture à des tiers et la durée de stockage des données personnelles.

Responsabilité du responsable du traitement

2.1 Le Responsable du traitement garantit au Sous-traitant qu'il traite les données conformément au RGPD / LPD, et que lorsqu'un Responsable du traitement exige l'approbation de l'autorité de contrôle, il l'ait demandée et obtenue.

Obligations du sous-traitant

3.1. En ce qui concerne les activités de traitement énoncées à l'article 1, le Sous-traitant veillera au respect des conditions imposées au traitement des données à caractère personnel conformément au RGPD / LPD.

3.2. Le Sous-traitant imposera une obligation de confidentialité à ses employés concernant toutes les données personnelles du Responsable du traitement qui leur sont divulguées dans le cadre de la fourniture des services par le Sous-traitant.

3.3. Le Sous-traitant informera le Responsable du traitement, à sa première demande, des mesures qu'il a prises en relation avec ses obligations en vertu du présent Contrat de sous-traitance.

3.4. Le Sous-traitant ne conservera aucune donnée personnelle qui lui est fournie dans le cadre du Contrat de sous-traitance autre que nécessaire (i) à la mise en œuvre du Contrat ; ou (ii) pour se conformer à l'une de ses obligations légales. Tout accord dérogatoire figure à l'annexe **A**.

3.5. Le Sous-traitant respectera strictement la confidentialité des données personnelles.

3.6. Les obligations du Sous-traitant découlant du présent Contrat de Sous-traitance s'appliquent également à toute personne qui traite des données personnelles sous l'autorité du Sous-traitant.

3.7. Le traitement des données personnelles par le Sous-traitant n'enrichira jamais les bases de données du Sous-traitant avec des données provenant des ensembles de données du Responsable du traitement.

3.8. Le Sous-traitant respectera toutes les instructions raisonnables données par le Responsable du traitement concernant le traitement des données à caractère personnel. Le Sous-traitant informera immédiatement le Responsable du traitement s'il estime que les instructions enfreignent la législation applicable.

3.9. Le Sous-traitant est tenu d'informer immédiatement le Responsable du traitement des modifications futures apportées à la mise en œuvre du Contrat de sous-traitance afin de s'assurer que le Responsable du traitement peut vérifier que les accords avec le Sous-traitant sont respectés. Cela inclut l'embauche de (nouveaux) tiers, sans préjudice des dispositions de l'article 5.1embauche de tiers ou de sous-traitants) et de l'article 11.3 (amendements).

3.10. Traitement des demandes d'accès et des violations de données (obligation d'informer et de participer voir ci-dessous)

Transfert de données personnelles

4.1. Le Sous-traitant peut traiter les données personnelles dans des pays de l'Union européenne. Le transfert vers des pays en dehors de l'Union européenne et de la Suisse n'est pas autorisé sans l'autorisation écrite préalable du Responsable du traitement.

4.2. Le Sous-traitant informera le Responsable du traitement du ou des pays impliqués à la première demande de ce dernier.

Embauche de tiers ou de sous-traitants

5.1. Le Sous-traitant ne peut, dans le cadre du Contrat de sous-traitance, engager aucun nouveau tiers lié à une partie du traitement des données sans l'acceptation du Responsable du traitement, les tiers non impliqués dans le traitement seront communiqués au Responsable du traitement.

5.1.1. Liste des Tiers sous-traitants existants :

NOM	NUMÉRO D'ENREGISTREMENT DE L'ENTREPRISE	ADRESSE	DESCRIPTION DU TRAITEMENT

5.2. Le Sous-traitant s'assurera inconditionnellement que ces Tiers sous-traitants acceptent les mêmes obligations imposées au Sous-traitant que celles convenues entre le Responsable du traitement et le Sous-traitant. Le Sous-traitant doit s'assurer que ces Tiers sous-traitants respectent correctement ces obligations et sera responsable vis-à-vis du Responsable du traitement de tous les dommages causés par des erreurs de ces tiers comme s'il avait commis ces erreurs lui-même.

Sécurité

6.1. Le Sous-traitant prendra des mesures techniques et organisationnelles, telles que définies en termes généraux à **l'Annexe A**, pour protéger les données personnelles contre la perte et toute autre forme de traitement illégal. Ces mesures garantissent, compte tenu de l'état de la technologie et des coûts de mise en œuvre, un niveau de sécurité adapté en fonction des risques du traitement et de la nature des données. Ces mesures servent également à éviter une collecte et un traitement ultérieurs inutiles. Le Sous-traitant enregistrera les mesures par écrit et s'assurera que la sécurité énoncée dans le présent paragraphe répond aux exigences de sécurité imposées par le RGPD/LPD.

6.2. Les Parties reconnaissent que les exigences en matière de sécurité sont sujettes à des changements continus et qu'un niveau efficace de sécurité exige des examens fréquents et des améliorations régulières des mesures de sécurité désuètes. En conséquence, le Sous-traitant continuera d'examiner, d'améliorer ou de compléter les mesures qui ont été mises en œuvre sur la base du présent article afin de continuer à se conformer à ses obligations imposées par le présent article.

6.3. Le Sous-traitant appliquera son plan de réponse aux incidents de sécurité pour gérer les problèmes de sécurité.

Obligation de notification

7.1. En cas de suspicion ou de violation réelle (i) des données ; (ii) violation des mesures de sécurité ; iii) violation de l'obligation de confidentialité ; ou (iv) la perte de données confidentielles, le Sous-traitant en informera le Responsable du traitement immédiatement, mais au plus tard 24 heures après la découverte de l'incident. Le Sous-traitant prendra toutes les mesures raisonnablement nécessaires pour empêcher ou atténuer toute divulgation, modification et dispositions illégales ou autres formes de traitement illégal. De plus, il prendra les mesures pour mettre fin ou prévenir toute violation (future) des mesures de sécurité, des violations du devoir de confidentialité ou des pertes supplémentaires de données confidentielles, sans préjudice des droits du Responsable du traitement de réclamer une indemnisation ou d'autres mesures. Cette disposition s'applique aux incidents qui surviennent chez le Sous-traitant et l'un de ses Tiers sous-traitants.

7.2. Les informations du Sous-traitant concerneront au moins les données définies à **l'Annexe B**, le cas échéant. Le Sous-traitant garantit que les informations fournies sont complètes, correctes et exactes.

7.3. Le Sous-traitant coopérera, à la demande du Responsable du traitement, à l'information des autorités compétentes et des personnes concernées. Le Responsable du traitement est chargé d'informer les autorités compétentes.

7.4. Le Sous-traitant conclura des accords écrits avec les Tiers sous-traitants sur la manière de signaler les incidents au Sous-traitant afin de permettre au Sous-traitant et au Responsable du traitement de se conformer à leurs obligations telles que définies au paragraphe 1 en cas d'incident. Ces accords doivent au moins inclure l'obligation pour le Tiers sous-traitant d'informer immédiatement, mais au plus tard dans les 18 heures suivant la première découverte, le Sous-traitant d'un incident tel que défini au paragraphe 1 et doit, à la demande du Responsable du traitement, coopérer à l'information des autorités compétentes et de la ou des personnes concernées.

Traitement des demandes des personnes concernées

8.1. Le Sous-traitant accordera toute la coopération nécessaire pour permettre au Responsable du traitement de se conformer à ses obligations découlant du RGPD, telles que la réalisation d'évaluations d'impact sur la vie privée et lorsqu'une personne concernée exerce ses droits en vertu du RGPD ou d'autres réglementations applicables concernant le traitement des données personnelles.

8.2. Si une personne concernée soumet une demande d'accès au sens de l'article 15 du RGPD, ou une demande de rectification, de complément, de modification, de limitation ou de suppression au sens de l'article 16, de l'article 17, paragraphe 1, et de l'article 18 du RGPD au Sous-traitant, le Sous-traitant transmettra cette demande au Responsable du traitement et en informera la personne concernée. Le Responsable du traitement traitera ensuite la demande indépendamment.

Audit

9.1. Le Responsable du traitement a le droit de commander des audits à un tiers indépendant qui est tenu à une obligation de confidentialité pour vérifier le respect de tous les aspects du présent Contrat de Sous-traitance.

9.2. Cet audit n'aura lieu qu'une fois que le Responsable du traitement aura demandé et évalué des rapports d'audit similaires disponibles chez le Sous-traitant, et soulèvera des arguments raisonnables qui justifient un audit initié par le Responsable du traitement. Un tel audit sera justifié si les rapports d'audit similaires présentés au Sous-traitant ne fournissent pas de preuve (suffisante) du respect du présent Contrat de Sous-traitance par le Sous-traitant. L'audit aura lieu après un préavis envoyé par le Responsable du traitement 30 jours à l'avance, et n'aura pas lieu plus d'une fois par an, sauf s'il existe une raison spécifique pour un audit, auquel cas l'audit peut avoir lieu à tout moment.

9.3. Le Sous-traitant coopérera à l'audit et fournira toutes les informations raisonnablement nécessaires à l'audit, y compris les données justificatives telles que les journaux système, et mettra ses employés à disposition dès que possible dans un délai raisonnable. Dans ce contexte, une période de deux semaines au maximum sera raisonnable, à moins qu'un intérêt urgent ne s'y oppose.

9.4. Les constatations de cette vérification seront évaluées par les Parties en consultation et mises en œuvre conjointement par l'une ou les deux Parties en réponse.

Mesures prises par l'organisme de réglementation

10.1 Si, dans le cadre de ses fonctions, le régulateur impose une mesure ou une amende au Responsable du traitement et si cette mesure ou amende est due à un manquement du Sous-traitant à respecter ses accords énoncés dans le présent Contrat de sous-traitance, le Responsable du traitement peut recouvrer tous les coûts de cette mesure ou de l'amende auprès du Sous-traitant.

Durée, résiliation et modifications

11.1 La durée du présent Contrat de Sous-traitance est égale à la durée du Contrat. Le Contrat de sous-traitance ne peut pas être résilié indépendamment du Contrat.

11.2 Le contrat de sous-traitance ne peut pas être résilié prématurément.

11.3 Les parties ne peuvent modifier le présent Contrat de sous-traitance que par consentement mutuel.

11.4 Après la fin du Contrat de sous-traitance ou à la suite d'une demande écrite du Responsable du traitement, le Sous-traitant détruira, sans frais supplémentaires et à la discrétion du Responsable du traitement, les données personnelles ou les retournera au Responsable du traitement. À la demande du Responsable du traitement, le Sous-traitant fournira la preuve du fait que les données ont été détruites ou supprimées (fournir un journal d'audit des opérations de manière sécurisée).

11.5 Le Sous-traitant informera tous les Tiers sous-traitants impliqués dans le traitement des données personnelles de la fin du Contrat de Sous-traitance. Les obligations énoncées à l'article 11.4 s'appliquent mutatis mutandis à ces Tiers sous-traitants. Le Sous-traitant veillera à ce que tous les Tiers sous-traitants concernés respectent leurs obligations.

Droit applicable et règlement des litiges

12.1 Le Contrat de sous-traitance et sa mise en œuvre sont régis par le droit suisse.

12.2 Tous les litiges qui surviennent entre les Parties en relation avec l'accord de traitement seront d'abord soumis à une médiation.

12.3 Tous les litiges qui n'ont pas pu être résolus par la médiation seront soumis au tribunal compétent du district où le Responsable du traitement est établi.

Annexes

13.1 **Les annexes A** et **B** font partie intégrante du présent accord de traitement.

Signatures :

Ainsi convenu en double exemplaire :

<société>	**<société>**
_____/_____/_____	_____/_____/_____
Date	Date
<nom>	<nom>
_____	_____
signature	signature

Annexe A : Spécification du traitement des données à caractère personnel

Le traitement des données personnelles par le Sous-traitant est ventilé comme suit dans la présente annexe :

- Les (catégories de) Données personnelles à traiter ;
- Les finalités du traitement ;
- Périodes de conservation ;
- Coordonnées.

Les (catégories de) données personnelles à traiter

Catégories de données personnelles	Données personnelles	Type d'installation
Employés, visiteurs, clients, public dans les espaces publics	Images de caméra et enregistrements audio et leur stockage respectif	CCTV
Employés du client	Prénom, Nom, E-mail, Adresse, Code Postal, Ville, Pays et Numéro de téléphone, mots de passe	CCTV, contrôle d'accès
Employés, visiteurs, clients, public dans les espaces publics	Plaques d'immatriculation	CCTV, contrôle d'accès
Salariés	Balises de contrôle d'accès	Contrôle d'accès

Tableau 1 : Description des catégories de données à caractère personnel traitées

Les finalités du traitement

Les (catégories de) Données à caractère personnel traitées par le Sous-traitant pour le compte du Responsable du traitement sont énumérées dans le tableau 1. Ces données personnelles sont traitées par le Sous-traitant uniquement pour mettre en œuvre les devoirs et/ou responsabilités énoncés dans l'accord principal. Il s'agit notamment des éléments suivants :

- Fournir un soutien ;
- Gestion technique de l'application et/ou des services ;
- Effectuer des sauvegardes.
- Les données sont collectées à des fins d'optimisation et d'amélioration de la plate-forme lors de la connexion au site Web et/ou aux applications mobiles.
- Les gens sont surveillés dans le magasin de manière anonyme en utilisant la technologie de flou. Les images de la caméra sont immédiatement anonymisées. Les données de localisation sont collectées sur ces personnes anonymes et transmises et traitées en tant que métadonnées.

Durée de conservation

Le Sous-traitant ne conservera pas les données personnelles et/ou les sauvegardes plus longtemps que nécessaire pour mettre en œuvre le Contrat ou pour se conformer à une autre obligation légale à laquelle il est soumis, avec un maximum de 180 jours. En cas de cessation de la fourniture de services de traitement de données à caractère personnel, le sous-traitant est tenu de supprimer toutes les données à caractère personnel traitées pour le compte du responsable du traitement et de certifier au responsable du traitement qu'il l'a fait.

Mesures de sécurité mises en œuvre

Le Sous-traitant a pris plusieurs mesures de sécurité. Il existe des procédures et des instructions pour les employés, et les connaissances et les compétences sont tenues à jour grâce à des cours de formation. En outre, le Sous-traitant a pris des mesures de sécurité techniques, y compris la sécurité numérique des systèmes et des applications, des mesures matérielles et logicielles, des solutions antivirus, des pares-feux, des mesures de journalisation, la gestion des mots de passe, l'autorisation et le cryptage.

Coordonnées

Si vous avez des questions concernant la présente annexe et/ou les services du Sous-traitant, veuillez contacter :

PME SA

Employé : <nom>

Poste : <poste>

Adresse e-mail : <email>

Numéro de téléphone : <téléphone>

Les violations de données au sens de l'article 7 doivent être signalées à :

<Société>

À l'attention du responsable de la protection de la vie privée

Employé : <nom>

Adresse e-mail : <email>

Numéro de téléphone : <téléphone>

Annexe B : Renseignements à fournir en cas d'atteinte à la protection des données

Si le Sous-traitant doit informer le Responsable du traitement conformément à l'article 7, il doit fournir au moins les données suivantes :

Coordonnées de la partie déclarante :

- Nom, fonction, adresse e-mail, numéro de téléphone
- Données concernant la violation de données
- Fournir un résumé de l'incident qui a entraîné la violation de la sécurité des données personnelles.
- Combien de personnes ont été touchées par l'atteinte ? (Entrez un numéro)
  a. Minimum : (entrez)
  b. Maximum : (entrez)

- Décrivez le groupe de personnes touchées par l'atteinte.

- Quand la violation s'est-elle produite ? (Choisissez l'une des options suivantes et complétez si nécessaire)
  a. Le (date)
  b. Entre (date de début de période) et (date de fin de période)
  c. Pas encore connu

- Quelle est la nature de l'atteinte ? (Vous pouvez cocher plusieurs options)
  a. Lire (confidentialité)
  b. Copier
  c. Changement (intégrité)
  d. Supprimer ou détruire (disponibilité)
  e. Vol
  f. Pas encore connu

- Quel type de données personnelles est concerné ? (Vous pouvez cocher plusieurs options)
  a. Nom, adresse et données de résidence
  b. Numéros de téléphone
  c. Adresses électroniques ou autres adresses pour la communication électronique
  d. Informations d'identification ou d'accès (par exemple, nom d'utilisateur/mot de passe ou numéro de client)
  e. Données financières (par exemple, numéro de compte, numéro de carte de crédit)
  f. Numéro de service citoyen (BSN) ou numéro de sécurité sociale
  g. Copies de passeport ou copies d'autres documents de légitimation
  h. Sexe, date de naissance et/ou âge

i. Données personnelles spéciales (par exemple, race, origine ethnique, casier judiciaire, convictions politiques, appartenance syndicale, religion, vie sexuelle, données médicales)
j. Autres données, (saisir)

- Quel est l'impact potentiel de la violation sur la vie privée des personnes concernées ? (Vous pouvez cocher plusieurs options)
  a. Stigmatisation ou exclusion
  b. Dommages à la santé
  c. Exposition à la fraude (d'identité)
  d. Exposition au spam ou à l'hameçonnage
  e. Autre, (entrer)

Mesures de suivi découlant de l'atteinte à la protection des données

- Quelles mesures techniques et organisationnelles avez-vous prises pour remédier à la violation et éviter d'autres violations ?

Mesures techniques de sécurité

- Les données personnelles sont-elles cryptées, rendues illisibles ou inaccessibles à des personnes non autorisées ? (Choisissez l'une des options suivantes et complétez si nécessaire)
  a. Oui
  b. Non
  c. En partie, de la manière suivante : (entrez)

- Si les données personnelles ont été totalement ou partiellement rendues illisibles ou inaccessibles, comment cela a-t-il été fait ? (Répondez à cette question si vous avez sélectionné l'option (a) ou (c) dans la dernière question. Expliquez également la méthode de cryptage, le cas échéant)

Aspects internationaux

- La violation affecte-t-elle des personnes dans d'autres pays de l'UE ? (Choisissez l'une des options suivantes)
  a. Oui
  b. Non
  c. Pas encore connu

Remerciements

Nous adressons des remerciements particuliers à M. Raoul Diez de la FER Genève pour ses conseils et son soutien dans la création de ce livre blanc ainsi qu'au service juridique de la FER Genève SAJEC pour sa relecture.

Information et questions

En cas de questions, n'hésitez pas à contacter le Clusis, nous ferons le maximum pour vous aider.

https://clusis.com/

Personne de contact : Brigitte Ansermet, Secrétaire Générale du Clusis

Adresse : Avenue du Général Guisan 48a, 1009 Pully

Mail : info@clusis.ch
Tél : +41 77 535 02 77

Notes