

[Logo Pfarrei]

Protection des données

Contrat relatif au traitement de données personnelles

(contrat de sous-traitance)

entre

[Paroisse]

[Adresse]

[NPA, Lieu]

ci-après «la mandante»

et

[Contractant]

[Adresse]

[NPA, Lieu]

ci-après «le prestataire»

ensemble les «parties»

1 Situation

Dans le cadre de l'exécution d'un contrat (contrat principal), le prestataire reçoit, de la mandante ou d'une autre manière, accès à des données qui se rapportent à une personne identifiée ou identifiable (appelées ci-après « données personnelles » ou « données à caractère personnel »).

Le présent contrat concrétise les obligations des parties en matière de prescriptions légalement contraignantes sur la protection des données en vertu du Règlement général européen sur la protection des données (RGPD) ainsi que de la Loi fédérale sur la protection des données (LPD) et il est valable dans la même mesure que celles-ci sont applicables.

La mandante est soumise au droit suisse. La LPD fait donc foi pour le mandat attribué au prestataire par la mandante.

Le présent contrat complète le contrat principal entre la mandante et le prestataire.

2 Obligations du prestataire

Le prestataire s'engage à :

- a) traiter les données personnelles seulement pour les objectifs fixés dans l'annexe A et, dans tous les cas, selon d'éventuelles directives documentées de la mandante ;
- b) prendre toutes les mesures techniques et organisationnelles permises par l'évolution technique à ce moment pour empêcher un traitement indu, la perte ou la falsification d'informations et à les maintenir constamment au niveau le plus actuel. L'annexe C mentionne les mesures techniques et organisationnelles possibles au moment de la conclusion de ce contrat ;
- c) transférer à un tiers le traitement de données personnelles seulement sur accord préalable écrit de la mandante et à la seule condition que le prestataire ait imposé au tiers des obligations au moins équivalentes à celles de ce contrat. Le prestataire indiquera dans l'annexe B à ce contrat toutes les entreprises sous-traitantes déjà existantes au moment de la conclusion du contrat ;
- d) traiter des données personnelles uniquement en Suisse, dans les États membres de l'Union européenne (UE) ou de l'Espace économique européen (EEE). Un traitement de données personnelles dans un pays tiers doit recevoir l'autorisation préalable de la mandante, pour le moins sous forme écrite (un courriel suffit). Si, dans le cadre d'un traitement de données admissible selon ce contrat, des données personnelles sont transférées dans un pays tiers n'ayant pas un niveau de protection approprié, un accord n'est envisageable qu'avec une garantie que les mesures de sécurité des données seront suffisantes pour garantir une protection proportionnelle au risque ;
- e) interdire aux collaborateurs chargés du traitement des données importantes de la mandante et à tout autre personne travaillant pour le prestataire de traiter les données importantes en dehors du cadre du contrat principal et de cette convention. Le prestataire s'assure également que les personnes autorisées à traiter les données se soient engagées à la confidentialité ou soient légalement soumises au secret professionnel.

- f) communiquer sans retard à la mandante toute violation réelle ou présumée de la protection des données (y compris violations de ce contrat) ainsi que des accès aux données par les autorités ou des requêtes de transmissions de données ;
- g) aider la mandante, à sa première demande, à respecter les lois applicables en matière de protection des données (p.ex., mise en œuvre des droit des personnes concernées, signalement de violations de la protection des données et analyse d'impact relative à la protection des données) dans la mesure du possible et selon les informations à sa disposition ;
- h) faire contrôler le respect de cette clause par la mandante, que ce soit par la mandante elle-même ou par un tiers au nom et sur mandat de la mandante ;
- i) rendre ou supprimer les données personnelles à la résiliation du contrat principal ou à la requête de la mandante, sous réserve d'éventuelles obligations légales de les conserver, sans en garder une copie et à confirmer l'avoir fait.

3 Obligations de la mandante

La mandante s'engage à :

- a) mettre à disposition du prestataire, dans la forme convenue, les données à caractère personnel nommées dans le contrat et la convention ;
- b) garantir que le traitement des données personnelles transmises par la mandante ainsi que leur transfert au prestataire sont licites et respectent les dispositions légales en la matière ; que ces opérations ne sont pas interdites par la loi ou en raison d'une obligation de garder le secret ;
- c) documenter par écrit (les courriels sont également considérés comme des écrits) toutes les directives relatives au traitement de données à caractère personnel par le prestataire ;
- d) vérifier régulièrement et à contrôler si nécessaire comment les données sont traitées.

4 Dispositions finales

4.1 Durée du contrat

Ce contrat reste en vigueur durant toute la durée du contrat principal pour autant que certaines de ses dispositions ne contiennent pas des obligations de plus longue durée. Il ne peut pas être résilié séparément.

4.2 Clause salvatrice

Au cas où certaines dispositions de ce contrat s'avéraient inefficaces, incomplètes ou inapplicables, cela n'enlèvera rien à la validité des autres parties du contrat.

4.3 Signature électronique

Les parties acceptent que ce contrat et tout amendement ou complément puissent être signés électroniquement et que toutes les signatures électroniques qui paraissent sur ce contrat sont équivalentes à des signatures manuscrites en termes de validité, d'applicabilité et d'admissibilité.

4.4 Modifications du contrat

Les compléments et les amendements au présent contrat ou sa résiliation doivent être faits par écrit pour être valides juridiquement et doivent être signés par chaque partie à la main ou électroniquement.

4.5 Droit applicable et for juridique

Le droit suisse s'applique à ce contrat. Tout litige découlant de ce contrat sera réglé par le tribunal de [lieu].

Paroisse

Date

Date

[Prénom Nom] [Fonction]

[Prénom Nom] [Fonction]

[Prestataire]

Date

Date

[Prénom Nom] [Fonction]

[Prénom Nom] [Fonction]

Annexe A : Spécification du traitement de données personnelles et coordonnées

Forme et finalité du traitement
[...]

Catégories des personnes concernées
[...]

Sorte(s) de données personnelles traitées
[...]

Informations générales de contact	Nom	Adresse courriel	Numéro de téléphone
Mandante	[...]	[...]	[...]
Prestataire	[...]	[...]	[...]

Contacts en cas de violation de la sécurité des données	Nom	Adresse courriel	Numéro de téléphone
Mandante	[...]	[...]	[...]
Prestataire	[...]	[...]	[...]

Annexe B : Liste des sous-traitants impliqués

Le prestataire fait appel, pour le traitement des données de la mandante, aux services des tiers suivants qui traitent des données sur mandat du prestataire (sous-traitants) :

Sous-traitant (nom, forme juridique, siège de la société)	Catégories de données personnelles traitées par le sous-traitant	Forme et finalité du traitement	Lieu du traitement	Mécanisme de transfert (Comment les données sont-elles transférées ?)	Garanties supplémentaires pour le transfert de données hors de l'EEE et de la Suisse
[...]	[...]	[...]	[...]	[...]	[...]
[...]	[...]	[...]	[...]	[...]	[...]

Annexe C : mesures techniques et organisationnelles pour la sécurité des données

Indications détaillées des mesures techniques et organisationnelles prises par le prestataire :

Confidentialité
<u>Contrôle de l'accès aux lieux</u> : le prestataire veille à ce que ses bureaux et locaux professionnels soient en principe fermés en dehors des heures de bureau. Durant les heures de bureau, il est garanti que visiteurs et tiers ne peuvent se déplacer seuls dans des lieux où ils peuvent avoir accès à des données à caractère personnel. La remise et la gestion des clefs se déroulent selon un processus défini qui règle l'attribution ou le retrait des droits d'accès aux espaces aussi bien au début qu'à la fin des rapports de travail.
<u>Contrôle de l'accès aux systèmes</u> : pour avoir accès à des systèmes TI, le prestataire et son personnel doivent disposer d'une autorisation d'accès correspondante. Un ou plusieurs administrateurs attribuent à cet effet les autorisations d'utilisateurs idoines. Les instructions de mot de passe contiennent une longueur minimale de mot de passe de 12 signes avec des majuscules/minuscules, chiffres et signes spéciaux. Un changement de mot de passe n'est pas obligatoire. Un historique des mots de passe est en arrière-plan. Il assure que les 10 derniers mots de passe ne puissent plus être réutilisés. Des tentatives erronées d'entrer dans le système sont protocolées. Après trois erreurs, le compte utilisateur correspondant est bloqué. Les accès à distance sur les systèmes TI du prestataire se font toujours par connexions cryptées. Tous les serveurs et systèmes clients utilisés pour remplir des prestations pour la mandante sont protégés avec des pare-feu dont la maintenance est assurée et qui sont équipés des dernières mises à jour et correctifs. Tous les collaborateurs et collaboratrices sont tenus de verrouiller leurs systèmes TI lorsqu'ils les quittent. Les systèmes TI se verrouillent automatiquement après un certain temps d'inactivité et sont protégés par mot de passe.

Les mots de passe que le prestataire reçoit de la mandante ou qu'il utilise pour ses systèmes TI sont en principe enregistrés sous forme cryptée et ne doivent être rendus accessibles qu'aux personnes à qui il a été confié de fournir concrètement des prestations à la mandante.

Contrôle d'accès aux données : les autorisations pour les systèmes TI et les applications du prestataire sont distribués sur la base du besoin d'en connaître. Les droits d'accès aux données, banque de données ou applications ne sont donc accordés qu'aux personnes qui s'occupent de la maintenance et de la gestion de ces données, applications ou banques de données ou qui travaillent dans le développement.

Les supports de données et le papier sont détruits par un prestataire de services qui garantit que ce travail est exécuté selon la norme DIN 66399.

Séparation : si le prestataire reçoit de la mandante des données à caractère personnel dans le cadre de son mandat, il les traitera séparément des données d'autres clients.

Pseudonymisation & cryptage : tout accès administratif aux systèmes TI de la mandante se fait par connexions cryptées.

Intégrité

Contrôle de saisie : le prestataire documentera de manière appropriée les saisies, modifications ou suppressions de données à caractère personnel auxquelles il procède sur mandat de la mandante, s'il n'est pas garanti que le système TI utilisé protège automatiquement de telles activités.

Contrôle de transmission : une transmission de données à caractère personnel effectué sur mandat de la mandante ne portera que sur le volume convenu et de la manière convenue précédemment avec la mandante. L'utilisation de supports de données privés dans le cadre de la sous-traitance pour la mandante est interdite au prestataire.

Disponibilité et résistance

Pour autant que le prestataire enregistre ou administre des données à caractère personnel ou des données d'accès pour la mandante, il veille à ce que ces données soit sauvegardées au moins chaque jour de manière incrémentielle et une fois par semaine « de manière complète ». Il existe un concept de sauvegarde des données impliquant aussi de réussir le test de rétablissement des données.

Procédure de régularité du contrôle et de l'évaluation

Le prestataire donne à ses employés des lignes directrices et/ou des directives qui garantissent que les données à caractère personnel sont traitées de manière à répondre aux exigences légales.

Cela implique notamment de contrôler régulièrement l'efficacité des mesures prises pour protéger les données à caractère personnel et éventuellement de les adapter.

Il est notamment veillé à ce que tous les employés sachent reconnaître des violations de la protection des données et à ce que celles-ci soient annoncées immédiatement à la mandante si elles concernent des données qui sont traitées dans le cadre de la sous-traitance pour la mandante.

Contrôle du mandat

L'intégration de prestataires ou de tiers externes exige la conclusion d'un contrat de sous-traitance, conformément aux directives du droit applicable relatif à la protection des données. Les prestataires sont aussi contrôlés régulièrement durant les rapports contractuels.

Certifications du prestataire :

Certificat	Unité organisationnelle de référence pour la certification	Durée de validité du certificat