Contrat de sous-traitance (CST).

Parties

Mandant (MD) :

Sous-traitant (ST) :

Contrat principal

Ce CST le complète.

Traitement de données effectué pour le MD par le ST (seul ce traitement est soumis au CST)

Objet/objectif :

Personnes concernées :

Catég. données personnelles :

Catég. données sensibles :

Activité du ST :

Durée (y.c. du CST) : ☐ LPD ☐ RGPD ☐

☐ Régi dans contrat principal : ☐ ST peut transférer vers :

Obligations (en plus du contrat principal)

1. Le ST ne traite les données qu'aux fins et conformément aux instructions documentées du MD (p. ex. configuration des services par le MD) ; s'il estime qu'une instruction est contraire au droit applicable, il en informe le MD.
2. Le ST assure une sécurité adéquate des données conformément au droit applicable, en mettant en œuvre au moins les mesures de protection des données convenues. Il signale sans délai toute violation de la sécurité des données, en fournissant les informations nécessaires.
3. Le ST oblige tous ses auxiliaires et employés à respecter la confidentialité, dans la mesure où ils n'y sont pas déjà tenus en vertu de la loi.
4. Le ST ne fait appel à des tiers sous-traitants qu'avec l'autorisation préalable du MD. Ils sont réputés avoir été autorisés par le MD si aucune objection n'est reçue de la part du MD dans les 30 jours. Les tiers sous-traitants doivent être soumis aux mêmes obligations que le ST.
5. Le ST ne transférera pas les données du MD sans son autorisation ; en cas de transfert, le ST se conformera aux exigences de la loi applicable en matière de protection des données.
6. Le ST assiste le MD dans le respect de la loi applicable en matière de protection des données, en particulier les obligations relatives au respect des droits des personnes concernées et à la réalisation d'analyses d'impact.
7. À la fin du CST, le ST devra restituer toutes les données au MD et les effacer s'il y est autorisé.
8. Le ST démontre le respect du CST, et le MD peut le vérifier dans son intégralité.

Tiers sous traitants autorisés

Nom	Pays	Fonction

☐ Selon liste séparée ☐ Selon site Web du ST

Mesures de protection des données(TOMS)

☐ Contrôle d'accès ☐ Vidéosurveillance
☐ Destruction sécurisées des documents ☐ ASI
☐ Contrôle de sécurité du personnel ☐ GIA
☐ Accès aux données seul. avec authentification
☐ AMF pour tous ☐ AMF pour les accès externes
☐ PAM ☐ Admin. seul. temporaire et ☐ AMF
☐ Règles MdP ☐ Principe du moindre privilège
☐ Principe du besoin de savoir ☐ Piste de vérification ☐ Sécurité zéro confiance ☐ VDI
☐ *At-rest* chiffré ☐ *In-transit* chiffré
☐ Terminaux chiffrés ☐ TLS mis en place
☐ E-mails seul. S/MIME ☐ ASVS Level 2
☐ Tests de pénétration, audits de sécurité externe ☐ ISMS (SMSI) ☐ Backups ☐ Concept BCM ☐ Pare-feu ☐ IDS ☐ DLP ☐ EDR/XDR
☐ MDM ☐ Inventorisation HW et SW
☐ Protection contre malwares ☐ Gestion des correctifs actuels
☐ Séparation systèmes productifs/autres
☐ Contrôle de l'installation de softwares
☐ Certif. ISO 27001 (CST inclus)
☐ Rapport SOC2 Typ II ☐ SOC ☐ SIEM
☐ Directive sur la sécurité de l'information
☐ Formation à la sécurité de l'information
☐ Selon liste séparée de TOMS :

Pour le MD : ☐ Remplace le CST précédent ☐ Annexes

Nom, fonction : Nom, fonction : Date

Pour le ST:

Nom, fonction : Nom, fonction : Date

08.01.2024 Auteur : David Rosenthal, drosenthal@vischer.com,
Contact : Samira Studer, sstuder@vischer.com

Un simple contrat de sous-traitance pour les PME.

Sur la page précédente figure un contrat très simple de sous traitance (**CST**). Un tel CST est obligatoire lorsque l'on engage des sous-traitants (**ST**). Le responsable du traitement de données qui néglige d'en conclure un s'expose à une amende selon la nouvelle Loi sur la protection des données (**LPD**).

Les sous-traitants professionnels ont leurs propres CST, qui sont certes rédigés en leur faveur, mais qui sont généralement suffisants pour les besoins de la protection des données. Souvent, ils ne sont même pas négociables. Le modèle proposé ci-dessus est conçu pour les cas où il n'y a pas de CST à disposition. Il contient ce qui est imposé par la LPD dans les cas simples, ainsi que ce qui peut être considéré comme un minimum en vertu du Règlement général sur la protection des données de l'UE (**RGPD**) (bien que certaines personnes voudraient certainement que les clauses soient en peu plus détaillées).

La première difficulté est d'**identifier** un cas de sous-traitance. Il y a toujours une sous-traitance lorsqu'une personne fait exécuter son propre traitement de données par un tiers. Cela signifie que cette personne décide de ce qui doit être fait, même si le sous-traitant (p. ex. un prestataire IT) propose un choix de services définis (p. ex. M365, Google Analytics, une solution CRM de Salesforce, etc.), car le choix des services proposés revient au client et il s'agit de ses données. Quelques exemples typiques sont : la société fiduciaire qui envoie des certificats de salaire, le fournisseurs de newsletters, les sociétés qui collectent/analysent des données pour le compte de tiers, les fournisseurs de services informatiques et de cloud (mais pas les simples fournisseurs de services télécoms ou postaux ni les simples fournisseurs de matériels informatiques et logiciels).

Un prestataire qui reçoit des données uniquement pour fournir ses propres services n'est **pas un sous-traitant** (p. ex. une banque, un assureur, un consultant, un avocat). Un CST serait alors inapproprié. Il faudrait tout au plus un accord de confidentialité, le cas échéant, avec l'obligation pour le prestataire de ne pas utiliser les données à d'autres fins que celui du mandant. Deux articles en allemand destinés aux spécialistes expliquent cette distinction : bit.ly/3Y4fANB, bit.ly/3ruAUQb.

Ne sont **pas non plus considérées comme des sous-traitants** les personnes qui, aux côtés des employés, sont intégrées dans l'entreprise et travaillent sous les instructions de celles-ci. Elles sont tenues de respecter les instructions, la confidentialité et les autres règles de protection des données applicables dans l'entreprise et doivent être supervisées en conséquence.

Le responsable du traitement qui fait appel à un sous-traitant demeure **responsable** du traitement des données. Il ne doit donc pas seulement conclure un CST, mais doit aussi choisir, instruire et surveiller soigneusement son ST.

Le CST **complète le contrat principal** et en fait partie. Il ne régit donc qu'un minimum d'éléments.

Pour compléter le modèle ci-dessus, il convient de procéder de la manière suivante :

1. Indiquer les **parties** ; le nom suffit dans la mesure où il existe déjà un contrat principal (p. ex. un contrat de service) dans lequel les données de contact sont mentionnées. Il convient d'y faire référence, p. ex. avec la date du contrat principal et la désignation.

2. **Décrire** le traitement de données. S'il est défini dans le contrat principal, indiquez la référence et laissez le reste du champ vide. Dans le cas contraire, décrivez-le dans les grandes lignes et indiquez les données personnelles (c.-à-d. les données qui se rapportent à une personne identifiée ou identifiable, pas les données matérielles) qui sont confiées au sous-traitant. Les données sensibles sont, par ex., les données de santé et autres données sensibles. Les personnes concernées sont celles dont les données font l'objet d'un traitement. Il faut indiquer si la LPD et, le cas échéant, le RGPD (ou encore une autre loi) s'appliquent, et si le ST est autorisé à transférer des données à l'étranger et, le cas échéant, dans quels pays (p. ex. EEE, "monde entier"). L'"activité" est p. ex. "exploiter un site Web". La durée est en principe régie dans le contrat principal et pourra être référée "selon le contrat principal".

3. Conformément au droit applicable, chaque **tiers sous-traitant** engagé par le ST pour le traitement des données doit être répertorié et autorisé (p. ex. "Microsoft (MIOL)", "IRL" et "hébergement" si le ST recourt pour sa solution au cloud de Microsoft). Selon les cas, le ST peut fournir une liste séparée ou la mettre à disposition sur son site Web. Le cas échéant, il est possible d'y faire référence.

4. Les **mesures** prises par le ST pour la protection des données (**TOMS**) doivent être cochées. Ces mesures relèvent du ST mais doivent satisfaire le mandant (**MD**), car il s'agit de ses données. Le modèle mentionne certaines mesures typiques (elles ne sont jamais toutes cochées). Certains ST ont leurs propres listes de mesures. Dans ce cas, il est également possible d'y faire référence.

Ne sont pas mentionnées les autres clauses relatives à la responsabilité, à la résiliation ou encore au droit applicable. Elles ne sont pas obligatoires du point de vue de la protection des données et peuvent être reprises du contrat principal. Cela vaut aussi pour la réglementation des coûts résultant du CST, p. ex. lorsque le MD donne des instructions ou sollicite de l'assistance.

Avez-vous des questions ou besoin de modèles plus complets ou de l'aide ? Adressez-vous à votre interlocuteur de confiance ou directement à nous à l'adresse e-mail dataprivacy@vischer.com.

Auteur : David Rosenthal, drosenthal@vischer.com Contact : Samira Studer, sstuder@vischer.com.

by VISCHER