

Règlement sur la sous-traitance du traitement des données

Version de septembre 2024

Le présent règlement décrit les obligations des parties contractantes en matière de protection des données. CYP exécute certains mandats pour des clients et traite dans ce contexte des données personnelles au sens de la loi suisse sur la protection des données et/ou du règlement général sur la protection des données de l'UE (ensemble, les « dispositions relatives à la protection des données »). Le présent règlement s'applique à toutes les activités liées au contrat conclu, dans le cadre duquel des données à caractère personnel (« données ») du client sont traitées.

Le texte français est une traduction de l'original en langue allemande. En cas de doute, le texte allemand fait foi.

1. Rôle et responsabilités des parties

Conformément aux dispositions relatives à la protection des données, le mandant / la mandante est responsable du traitement des données, tandis que CYP est le sous-traitant. Le mandant / la mandante et CYP sont tous deux responsables du respect intégral de toutes les dispositions relatives à la protection des données qui leur sont applicables.

Le mandant / la mandante garantit qu'il/elle a informé les personnes au sujet desquelles il/elle fournit des données personnelles à CYP (ou dont CYP obtient les données personnelles d'une autre manière) du traitement effectué par CYP conformément au présent règlement. Il/elle les informe de manière complète, compréhensible et sous une forme et dans une langue aisément accessible en indiquant, si nécessaire, que ces personnes ont donné leur consentement au traitement correspondant ou qu'un autre motif justificatif est applicable.

Si le mandant / la mandante est soumis(e) à une obligation d'information plus étendue en vertu des dispositions relatives à la protection des données, il/elle fournit ces informations aux personnes concernées.

Le mandant / la mandante garantit en outre que le traitement effectué par CYP conformément au présent règlement est conforme aux dispositions applicables en matière de protection des données, et notamment qu'il ne va pas au-delà du traitement que le mandant / la mandante est autorisé(e) à effectuer et qu'il ne s'oppose à aucune obligation de confidentialité légale ou contractuelle.

2. Objet et durée

L'objet, la durée, la nature et la finalité du traitement découlent en principe du contrat principal.

La durée de ce règlement est déterminée par la durée du contrat principal entre CYP et le client. Sont exclues les dispositions du présent règlement qui impliquent des obligations supplémentaires.

CYP traite les données personnelles aussi longtemps que cela est nécessaire pour poursuivre les objectifs indiqués dans le présent règlement ou pour remplir des obligations contractuelles ou légales, ou plus longtemps si les données personnelles correspondantes sont soumises à une obligation légale de conservation ou sont nécessaires à des fins de preuve.

Dès que les données personnelles traitées dans le cadre de ce règlement ne sont plus nécessaires, elles sont supprimées ou anonymisées par CYP. Demeurent réservées les données personnelles qui sont également enregistrées par CYP au cours des sauvegardes opérationnelles habituelles.

La base juridique pour le traitement des données personnelles est, si la loi l'exige, le consentement de la personne concernée ou l'intérêt légitime du mandant / de la mandante à la sous-traitance du traitement des données pour la poursuite des objectifs décrits ci-dessus.

Le mandant / la mandante doit pouvoir prouver ce consentement ou l'intérêt légitime pour le traitement des données par CYP. Si la personne concernée révoque son consentement ou qu'il n'y a plus d'intérêt légitime, le mandant / la mandante en informe immédiatement CYP.

3. Catégories de données personnelles traitées

CYP traite les catégories de données personnelles suivantes :

- données personnelles de base (p. ex. nom, adresse, date de naissance)
- données de communication (p. ex. numéro de téléphone, adresse e-mail)
- données d'évaluation, de notation et de formation

Personnes concernées :

- personnes participant aux cours
- personnes encadrant les personnes participant aux cours
- administrateurs d'entreprise
- collaborateurs/collaboratrices
- personnes intéressées

4. Instructions du mandant / de la mandante

Le traitement des données décrit dans le présent règlement est considéré comme une consigne générale donnée par le mandant / la mandante à CYP pour le traitement des données personnelles. Les directives sont fixées par le contrat.

CYP peut recevoir des instructions spécifiques supplémentaires concernant le traitement des données personnelles si celles-ci sont proportionnées et que l'effort requis de la part de CYP est raisonnable.

5. Sous-traitants secondaires et lieu de traitement

CYP transmet elle-même des données personnelles à des tiers qu'ils les traitent (« sous-traitants secondaires »). La liste de ces sous-traitants secondaires peut être consultée sur le site Internet de CYP à l'adresse suivante : <https://cyp.ch/fr/prot-donnees>. Elle est considérée comme approuvée par le mandant / la mandante lors de la conclusion du contrat.

En outre, le mandant / la mandante autorise de manière générale CYP à faire appel à des sous-traitants secondaires supplémentaires ou à remplacer des sous-traitants secondaires existants à sa seule discrétion. CYP informe au préalable le mandant / la mandante du recours éventuel à des sous-traitants secondaires ou de leur remplacement. Le mandant / la mandante peut s'y opposer. Si le mandant / la mandante ne s'y oppose pas dans les 10 jours suivant la notification correspondante, le recours/remplacement est considéré comme approuvé. En cas d'opposition du mandant / de la mandante, CYP peut renoncer au recours/remplacement ou proposer une alternative et, si cela n'est pas possible ou pas raisonnable, le service correspondant est suspendu.

Le traitement des données a lieu en Suisse, au sein de l'UE, au sein de l'EEE ou dans un pays considéré par la Commission européenne et le Conseil fédéral comme offrant un niveau de protection adéquat et garantissant une protection appropriée des données personnelles au sens de la loi suisse sur la protection des données. Toute délocalisation du traitement des données vers un pays situé en dehors de ce territoire ne peut se faire qu'avec l'accord préalable du mandant / de la mandante et conformément aux dispositions légales applicables (notamment en respectant les conditions indiquées dans le chapitre V du RGPD de l'UE et dans la loi suisse sur la protection des données). Dans un tel cas, le mandant / la mandante s'engage, en particulier avant la transmission ou la communication de données, à conclure des contrats complémentaires appropriés et, si nécessaire, à prendre des mesures juridiques, techniques ou organisationnelles adéquates.

CYP impose par contrat aux sous-traitants secondaires de protéger de manière appropriée toutes les données personnelles qui leur parviennent dans le cadre de la sous-traitance du traitement des données et de les utiliser exclusivement à cette fin.

6. Sécurité des données

CYP prend toutes les mesures techniques et organisationnelles nécessaires pour protéger de manière adéquate (notamment contre la manipulation, la divulgation, la perte, l'effacement ou la destruction) les données personnelles traitées dans le cadre du présent règlement. Pour ce faire, CYP édicte des directives, forme les responsables et met en œuvre des dispositifs de sécurité appropriés ainsi que des solutions de sécurité informatique et de réseau.

CYP limite l'accès aux données personnelles aux seules personnes qui en ont besoin pour accomplir leur tâche et s'assure que l'ensemble des collaborateurs et collaboratrices, sous-traitants ou prestataires de services impliqués dans le traitement des données respectent la confidentialité des données personnelles. Les personnes concernées doivent garantir le respect de cette obligation de confidentialité avant de commencer leur activité.

7. Violation de la sécurité des données

CYP informe le mandant / la mandante le plus rapidement possible s'il constate une violation de la sécurité des données au sens des dispositions relatives à la protection des données.

CYP aide le mandant / la mandante, dans la mesure du possible et du raisonnable, à gérer les violations de la sécurité des données qu'elle a constatées, à condition que le mandant / la mandante indemnise CYP de manière appropriée.

CYP transmet à ces fins les informations pertinentes, si elles sont disponibles, au mandant / à la mandante. Le mandant / la mandante reste responsable, pour sa part, de toutes les notifications nécessaires aux autorités de contrôle de la protection des données et aux personnes concernées. De son côté, CYP effectue une déclaration auprès des autorités de contrôle de la protection des données lorsqu'il existe une telle obligation.

8. Demandes de personnes concernées

Les personnes dont les données personnelles sont traitées dans le cadre du présent règlement peuvent faire valoir leurs droits individuels vis-à-vis des deux parties. Si une personne s'adresse à CYP pour faire valoir un droit individuel et que CYP n'est pas elle-même la partie chargée du traitement, CYP transmet la demande au mandant / à la mandante indépendamment de l'obligation de fournir une prestation subséquente. Le mandant / la mandante répond et traite les demandes correspondantes. Sur demande du mandant / de la mandante et si elles sont disponibles, CYP fournit au mandant / à la mandante les informations nécessaires à cet effet. Le mandant / la mandante s'assure que les personnes exercent correctement leurs droits individuels et demande les informations qui permettent d'identifier la personne sans aucun doute. CYP décline toute responsabilité en cas de réponse erronée ou hors délai.

9. Relations avec les autorités de contrôle de la protection des données

Si une autorité de surveillance de la protection des données s'adresse à CYP au sujet de données personnelles traitées dans le cadre du présent règlement, CYP transmet la demande ou la décision correspondante au mandant / à la mandante, indépendamment de l'obligation de fournir une prestation subséquente. Le mandant / la mandante correspond avec l'autorité de contrôle qui a posé la question ou pris la décision et répond à ses questions ou se conforme à sa décision, toujours en concertation avec CYP. Sur demande du mandant / de la mandante et si elles sont disponibles, CYP fournit au mandant / à la mandante les informations nécessaires à cet effet (voir également le chiffre 7).

10. Responsabilité et dommages-intérêts

Le mandant / la mandante et CYP sont responsables vis-à-vis des personnes concernées conformément aux dispositions légales de l'art. 82 RGPD ou aux dispositions applicables du droit suisse.

11. Communications

Toute communication d'une partie à l'autre dans le cadre du présent règlement se fait par écrit (y compris par e-mail).

- Pour CYP : CYP Association, Giessereistrasse 18, 8005 Zurich / datenschutz@cyp.ch
- Pour le mandant / la mandante : une personne ou un service responsable des demandes relatives à la protection des données est indiqué(e) lors de la conclusion du contrat.

12. Droit applicable et for

Ce règlement est soumis au droit matériel suisse.

Les éventuels litiges découlant du présent règlement ou en lien avec celui-ci relèvent de la compétence exclusive des tribunaux ordinaires de Zurich, en Suisse.

13. Dispositions finales

Chaque partie est responsable du respect du présent règlement par ses employés, sous-traitants, agents et autres tiers auxquels elle fait appel.

Toute modification ou tout complément au présent règlement doit, pour être valable, être effectué par écrit et mentionner expressément qu'il s'agit d'une modification ou d'un complément aux présentes conditions.

Aperçu des mesures techniques et organisationnelles

Contrôle de l'accès aux systèmes

Le contrôle de l'accès aux systèmes comprend des mesures visant à empêcher l'accès non autorisé aux systèmes de traitement des données.

Mesures

- Les comptes utilisateurs et les ordinateurs sont sécurisés par des mesures techniques actuelles et appropriées.
- L'accès à partir de smartphones privés nécessite un code PIN sécurisé et requiert un système d'exploitation à jour.
- Utilisation obligatoire d'un gestionnaire de mots de passe
- Accès aux bureaux contrôlé par la sécurisation des portes et l'enregistrement des clés

Contrôle de l'accès aux données

Le contrôle de l'accès aux données comprend des mesures qui garantissent que seuls les utilisateurs autorisés peuvent accéder aux données correspondantes.

Mesures

- Concept d'autorisation strict et contrôle régulier, y compris dans le cadre d'audits.
- Processus d'autorisation pour le partage d'accès
- Les accès administratifs sont fortement limités à un groupe de personnes défini.

Contrôle de la transmission des données

Le contrôle de la transmission des données doit garantir que les données ne peuvent pas être lues, modifiées ou supprimées de manière non autorisée lors de la transmission électronique.

Mesures

- Cryptage des ordinateurs portables via Bitlocker
- Cryptage des transmissions de données (TLS/SSL)
- Wi-Fi sécurisé

Contrôle de la sous-traitance

Le contrôle de la sous-traitance comprend des mesures qui garantissent que les données personnelles ne sont traitées que conformément aux instructions du mandant / de la mandante.

Mesures

- Contrat de sous-traitance du traitement des données avec des prestataires de services, si possible
- Contrôle régulier des sous-traitants chargés du traitement des données

Contrôle de la disponibilité

Le contrôle de la disponibilité est une mesure technique visant à restaurer les données stockées après une perte de données, un dommage ou une panne.

Mesures

- Sauvegarde des données et des services
- Conservation des sauvegardes dans des endroits distincts
- Protection contre les menaces
- Information et formation régulières des collaborateurs et collaboratrices (au moins 3 fois par an)