

Contrat de sous-traitance de données personnelles (CST)

selon l'art. 9 de la loi fédérale sur la protection des données (LPD) et l'art. 28 du Règlement général sur la protection des données (RGPD)

entre le client (ci-après «responsable du traitement») et FireStorm ISP GmbH, Kirchenrainstrasse 27, 8632 Tann, Suisse (ci-après «FireStorm» ou «sous-traitant»)

Version octobre 2026

1. Objet et durée

- 1.1 Le présent contrat régit le traitement des données personnelles que FireStorm traite pour le compte du responsable du traitement dans le cadre des services convenus (contrat principal), notamment l'hébergement web, les services e-mail, les vServer, les serveurs root, les serveurs dédiés, les services de stockage et de sauvegarde ainsi que les services de domaine et DNS.
- 1.2 La durée du présent contrat est déterminée par la durée du contrat principal. La fin du contrat principal met également fin au présent contrat; les obligations selon le chiffre 12 (restitution et effacement) et la confidentialité continuent de s'appliquer au-delà.
- 1.3 Le présent contrat complète les Conditions générales (CG) de FireStorm. En matière de protection des données, le présent contrat prime les CG.

2. Nature, finalité et étendue du traitement

- 2.1 FireStorm met à la disposition du responsable du traitement l'infrastructure pour l'enregistrement et le traitement de ses données (hébergement, serveurs, stockage, sauvegarde, réseau). Le traitement comprend notamment l'enregistrement, la sauvegarde, la transmission, la restauration et l'effacement de données, exclusivement en vue de fournir les services convenus.
- 2.2 La nature des données personnelles et le cercle des personnes concernées sont déterminés exclusivement par le responsable du traitement au travers de l'utilisation des services. Il peut s'agir de données de base de personnes, de données de communication, de données contractuelles, de données de journalisation ainsi que, selon l'application du responsable du traitement, de données personnelles sensibles (p. ex. données sur la santé). Les personnes concernées peuvent être notamment des clients, des patients, des collaborateurs et des fournisseurs du responsable du traitement.
- 2.3 Pour les vServer, les serveurs root et les serveurs dédiés, le responsable du traitement gère lui-même le système d'exploitation, les applications et les données. FireStorm ne dispose d'aucune donnée d'accès à ces systèmes et n'accède pas aux données qui y sont enregistrées. Le traitement par FireStorm se limite à l'exploitation de l'infrastructure ainsi qu'à la création et à la conservation des sauvegardes convenues. Les serveurs dédiés ne disposent d'aucune fonction de sauvegarde ; le responsable du traitement est seul responsable de la sauvegarde de leurs données.

3. Lieu du traitement

- 3.1 Les données de l'hébergement web, des services e-mail, des vServer, des serveurs root, des serveurs dédiés ainsi que l'ensemble des sauvegardes et snapshots sont enregistrés et traités exclusivement dans des centres de données situés en Suisse.
- 3.2 Pour la résolution de noms géo-redondante, FireStorm exploite en outre des serveurs DNS sur des sites en Allemagne et en France. Seules des données de zone DNS (noms de domaine, adresses IP et autres enregistrements DNS) y sont enregistrées, à l'exclusion de tout contenu

provenant de l'hébergement, des e-mails ou des serveurs. Selon l'annexe 1 de l'ordonnance sur la protection des données (OPDo), ces États disposent d'un niveau de protection des données adéquat.

- 3.3 Pour les produits de fournisseurs tiers que le responsable du traitement obtient par l'intermédiaire de FireStorm (p. ex. noms de domaine, certificats SSL, Microsoft 365), les lieux de traitement mentionnés à l'annexe 2 s'appliquent.
- 3.4 L'administration et le support sont assurés par des collaborateurs de FireStorm en Suisse. Les supports externes de fabricants (p. ex. fabricants de logiciels ou de matériel) obtiennent dans des cas particuliers, dans la mesure nécessaire à la résolution d'une perturbation, un accès limité dans le temps et surveillé à l'infrastructure, mais jamais aux données se trouvant à l'intérieur des vServer, des serveurs root et des serveurs dédiés.

4. Instructions du responsable du traitement

- 4.1 FireStorm traite les données personnelles exclusivement dans le cadre du contrat principal, du présent contrat et des instructions documentées du responsable du traitement, à moins que FireStorm ne soit tenue d'effectuer un traitement en vertu du droit suisse. Dans ce cas, FireStorm informe préalablement le responsable du traitement de ces exigences légales, dans la mesure où la loi le permet.
- 4.2 Le responsable du traitement donne ses instructions par ticket ou par écrit. Si FireStorm estime qu'une instruction enfreint des prescriptions en matière de protection des données, FireStorm en informe sans délai le responsable du traitement et peut suspendre l'exécution jusqu'à la confirmation ou la modification de l'instruction.
- 4.3 Les instructions qui vont au-delà de l'étendue des prestations convenues sont facturées selon le travail effectué.

5. Obligations de FireStorm

- 5.1 FireStorm préserve la confidentialité des données personnelles. Tous les collaborateurs ayant accès à l'infrastructure sont tenus par écrit au secret, également au-delà de la fin des rapports de travail, et sont régulièrement formés à la protection des données et à la sécurité de l'information.
- 5.2 Aucune copie de données n'est effectuée à l'insu du responsable du traitement. Font exception les sauvegardes convenues ainsi que les copies techniquement nécessaires à une exploitation conforme.
- 5.3 FireStorm ne communique des données personnelles que s'il existe une obligation légale ou un ordre d'une autorité suisse compétente ou d'un tribunal suisse. Dans la mesure permise par la loi, FireStorm en informe préalablement le responsable du traitement. Les demandes d'autorités étrangères ne reçoivent de réponse que par la voie de l'entraide judiciaire.
- 5.4 M. Christian Geissler est désigné en qualité de conseiller à la protection des données de FireStorm (support@firestorm.ch, 0844 300 200). Tout changement est communiqué au responsable du traitement.

6. Mesures techniques et organisationnelles

- 6.1 FireStorm prend les mesures techniques et organisationnelles décrites à l'annexe 1 afin de garantir une sécurité des données adaptée au risque conformément à l'art. 8 LPD et à l'art. 32 RGPD.
- 6.2 Les mesures sont régulièrement vérifiées et adaptées à l'état de la technique. Le niveau de protection ne doit pas être abaissé. FireStorm communique au responsable du traitement les modifications importantes.

- 6.3 Le responsable du traitement est lui-même responsable de la sécurité à l'intérieur des vServer, des serveurs root et des serveurs dédiés (système d'exploitation, applications, données d'accès, chiffrement des données d'application).

7. Annonce des violations de la sécurité des données

- 7.1 FireStorm informe sans délai le responsable du traitement, en règle générale dans les 24 heures, dès qu'est confirmée une violation de la sécurité des données dans l'infrastructure de FireStorm (plateforme de virtualisation, systèmes de stockage et de sauvegarde, panneau client, réseau) susceptible de concerner les données du responsable du traitement.
- 7.2 Dans la mesure où ces éléments sont connus, l'annonce indique la nature de la violation, les systèmes et catégories de données concernés, les conséquences probables ainsi que les mesures prises ou proposées. Les indications qui ne sont pas encore connues sont communiquées au fur et à mesure.
- 7.3 FireStorm assiste le responsable du traitement dans l'exécution de ses obligations d'annonce envers le PFPDT (art. 24 LPD) ou l'autorité de contrôle (art. 33 et 34 RGPD), notamment au moyen de journaux et d'horodatages.
- 7.4 Si FireStorm constate un trafic suspect provenant de systèmes du responsable du traitement, par exemple des attaques contre des tiers ou du spam, FireStorm en informe le responsable du traitement. Il n'existe aucune obligation de surveiller les systèmes du responsable du traitement.

8. Assistance au responsable du traitement

- 8.1 Si une personne concernée s'adresse directement à FireStorm, FireStorm transmet sans délai la demande au responsable du traitement.
- 8.2 FireStorm assiste le responsable du traitement, dans la mesure de ce qui peut raisonnablement être exigé, dans l'exercice des droits des personnes concernées ainsi que lors d'analyses d'impact relatives à la protection des données. Les prestations qui vont au-delà de la mise à disposition d'informations existantes sont facturées selon le travail effectué.

9. Sous-traitants ultérieurs

- 9.1 Les sous-traitants ultérieurs auxquels il est fait appel au moment de la conclusion du contrat sont énumérés à l'annexe 2. En concluant le présent contrat, le responsable du traitement consent à leur intervention.
- 9.2 FireStorm ne fait appel à de nouveaux sous-traitants ultérieurs ayant accès à des données provenant de l'hébergement, des e-mails, des serveurs ou des sauvegardes qu'avec le consentement écrit préalable du responsable du traitement. Le consentement peut être donné par e-mail et ne peut être refusé que pour un motif important relevant de la protection des données.
- 9.3 Pour les produits de fournisseurs tiers (noms de domaine, certificats SSL, Microsoft 365 et produits comparables), le consentement au fournisseur concerné est réputé donné par la commande du produit. FireStorm informe préalablement de tout changement de ces fournisseurs; le responsable du traitement peut s'y opposer.
- 9.4 FireStorm choisit les sous-traitants ultérieurs avec soin et leur impose contractuellement des obligations correspondant au présent contrat.
- 9.5 Les simples prestations auxiliaires sans accès à des données personnelles, notamment la surface, l'électricité, le refroidissement, la sécurité physique et la connexion réseau fournies par les exploitants de centres de données, ne sont pas considérées comme de la sous-traitance. Elles sont énumérées à l'annexe 2 par souci de transparence.

10. Droits de contrôle

- 10.1 Sur demande, FireStorm met à la disposition du responsable du traitement les informations nécessaires pour démontrer le respect du présent contrat.
- 10.2 Le responsable du traitement est en droit de contrôler le respect du présent contrat, après avoir convenu préalablement d'une date (en règle générale au moins 14 jours à l'avance), pendant les heures d'ouverture, lui-même ou par l'intermédiaire d'un tiers tenu au secret. Les contrôles ne doivent pas porter atteinte à l'exploitation ni à la sécurité des autres clients. Le travail de FireStorm est facturé selon les tarifs horaires en vigueur.

11. Obligations du responsable du traitement

- 11.1 Le responsable du traitement est seul responsable de la licéité du traitement des données et du respect des droits des personnes concernées.
- 11.2 Le responsable du traitement informe sans délai FireStorm s'il constate des erreurs ou des irrégularités dans le traitement.

12. Restitution et effacement

- 12.1 Jusqu'à la fin du contrat, le responsable du traitement peut exporter lui-même ses données à tout moment, pour les serveurs avec accès root complet également sous forme d'image complète. Sur demande, FireStorm assiste le responsable du traitement à cet effet, contre facturation selon le travail effectué.
- 12.2 Au plus tard 30 jours après la fin du contrat ou après autorisation du responsable du traitement, FireStorm efface l'ensemble des données du responsable du traitement, y compris les serveurs, supports de données, snapshots et sauvegardes, pour autant qu'aucune obligation légale de conservation ne s'y oppose. Sur demande, FireStorm confirme l'effacement par écrit.
- 12.3 Les données sont enregistrées sous forme chiffrée sur les supports de données. Les supports de données défectueux ou mis hors service sont effacés selon les règles de l'art ou détruits physiquement avant leur élimination.

13. Responsabilité

- 13.1 Les dispositions des CG de FireStorm (en particulier le chiffre 12) s'appliquent à la responsabilité.
- 13.2 Dans le rapport avec la personne concernée, le responsable du traitement répond des dommages qu'une personne concernée subit en raison d'un traitement de données illicite ou inexact. Un recours du responsable du traitement contre FireStorm n'est admissible que si FireStorm a enfreint le présent contrat intentionnellement ou par négligence grave.
- 13.3 Les peines conventionnelles sont exclues.

14. Droit de résiliation extraordinaire

- 14.1 En cas de violations graves du présent contrat par FireStorm, en particulier des prescriptions applicables en matière de protection des données, le responsable du traitement peut résilier le contrat principal avec effet immédiat pour les services concernés. En cas de violations mineures, le responsable du traitement fixe d'abord un délai raisonnable pour y remédier.

15. Dispositions finales

- 15.1 Les deux parties traitent de manière confidentielle toutes les connaissances acquises dans le cadre du présent contrat concernant les secrets d'affaires et les mesures de sécurité des données de l'autre partie, également au-delà de la fin du contrat.

- 15.2 Aucune rémunération supplémentaire n'est perçue pour le présent contrat, sauf disposition expresse contraire.
- 15.3 Les modifications et compléments requièrent la forme écrite; un e-mail suffit. Les accords individuels conclus avec certains responsables du traitement priment le présent contrat.
- 15.4 Si certaines dispositions devaient être sans effet, la validité des autres dispositions n'en serait pas affectée. Elles sont remplacées par une réglementation valable qui se rapproche le plus possible du but économique.
- 15.5 Le droit suisse est exclusivement applicable. Le for est Hinwil.
- 15.6 Les termes sont utilisés au sens de la LPD et, dans la mesure où le RGPD est applicable, au sens du RGPD.

Annexe 1: Mesures techniques et organisationnelles

Sécurité physique (contrôle de l'accès aux locaux)

- Exploitation des serveurs dans des centres de données certifiés ISO/IEC 27001 situés en Suisse
- Accès réservé aux personnes autorisées, surveillance des centres de données 24 heures sur 24
- Alimentation électrique et connexion réseau redondantes
- Serveurs de sauvegarde dans un centre de données distinct situé en Suisse

Contrôle de l'accès aux systèmes et aux données

- Accès administratif à l'infrastructure par les propres collaborateurs de FireStorm en Suisse; supports externes de fabricants uniquement dans des cas particuliers, limités dans le temps et surveillés
- Les interfaces de gestion de la plateforme de virtualisation et de sauvegarde ne sont pas directement accessibles depuis Internet
- Authentification à deux facteurs disponible pour le panneau client
- FireStorm ne dispose d'aucune donnée d'accès aux vServer, serveurs root et serveurs dédiés des clients; le client définit lui-même les données d'accès
- Journalisation des actions au niveau de la plateforme (accès à la console, démarrage et arrêt, snapshots, sauvegardes, restaurations) avec utilisateur et horodatage

Chiffrement et séparation

- Enregistrement chiffré des données sur les supports de données
- Transmission chiffrée (TLS) pour le panneau client, les services e-mail et l'administration
- Séparation logique des clients par des machines virtuelles propres ou des comptes d'hébergement propres

Disponibilité et résilience

- Sauvegardes quotidiennes sur des systèmes de sauvegarde distincts, inaccessibles depuis les systèmes des clients (inclus: sauvegarde quotidienne avec plusieurs points de restauration de la dernière semaine; sauvegardes plus fréquentes et conservation plus longue moyennant supplément). Les serveurs dédiés ne disposent d'aucune fonction de sauvegarde.
- Protection DDoS au niveau du réseau, pare-feu en amont avec WAF de base
- Surveillance des systèmes 24 heures sur 24, service de dépannage 24/7

Intégrité et maintenance

- Installation immédiate des mises à jour de sécurité des fabricants pour l'infrastructure, au plus tard dès qu'un correctif est disponible
- Effacement selon les règles de l'art ou destruction physique des supports de données défectueux et mis hors service

Organisation

- Engagement écrit de confidentialité de tous les collaborateurs
- Collaborateurs titulaires d'une certification personnelle ISO/IEC 27001 Foundation
- Conseiller à la protection des données désigné
- Assurance responsabilité civile professionnelle pour prestataires de services informatiques et de télécommunication, couverture cyber incluse

Annexe 2: Sous-traitants ultérieurs et prestataires de services

Pour tous les produits

- Exploitants de centres de données en Suisse (colocation, ISO/IEC 27001): surface, électricité, refroidissement, sécurité physique et connexion réseau. Aucun accès logique aux systèmes ou aux données. Pas de sous-traitant ultérieur au sens du chiffre 9.5; informations sur demande sous réserve de confidentialité.

Uniquement pour les services DNS

- Serveurs DNS sur des sites en Allemagne et en France (géo-redondance). Seules des données de zone DNS y sont enregistrées.

Uniquement en cas de commande du produit concerné

- Noms de domaine: les services d'enregistrement et registraires compétents pour l'extension de domaine concernée (p. ex. SWITCH pour .ch et .li, DENIC pour .de, nic.at pour .at, registraires accrédités par l'ICANN). Les données du titulaire du domaine sont traitées.
- Certificats SSL: l'autorité de certification concernée et ses partenaires de distribution. Les données de demande du certificat sont traitées.
- Microsoft 365: Microsoft et le distributeur Pax8. Les dispositions de Microsoft en matière de protection des données s'appliquent.