

Accordo sul trattamento di dati personali per conto di terzi (ATD)

ai sensi dell'art. 9 della legge federale sulla protezione dei dati (LPD) e dell'art. 28 del regolamento generale sulla protezione dei dati (RGPD)

tra il cliente (di seguito «titolare del trattamento») e FireStorm ISP GmbH, Kirchenrainstrasse 27, 8632 Tann, Svizzera (di seguito «FireStorm» o «responsabile del trattamento»)

Versione ottobre 2026

1. Oggetto e durata

- 1.1 Il presente accordo disciplina il trattamento di dati personali che FireStorm effettua per conto del titolare del trattamento nell'ambito dei servizi convenuti (contratto principale), in particolare webhosting, servizi e-mail, vServer, root server, server dedicati, servizi di archiviazione e di backup nonché servizi di dominio e DNS.
- 1.2 La durata del presente accordo corrisponde alla durata del contratto principale. La cessazione del contratto principale pone fine anche al presente accordo; gli obblighi di cui alla cifra 12 (restituzione e cancellazione) e la riservatezza continuano ad applicarsi oltre tale termine.
- 1.3 Il presente accordo completa le Condizioni generali (CG) di FireStorm. Nelle questioni relative alla protezione dei dati, il presente accordo prevale sulle CG.

2. Natura, scopo ed estensione del trattamento

- 2.1 FireStorm mette a disposizione del titolare del trattamento l'infrastruttura per la memorizzazione e il trattamento dei suoi dati (hosting, server, archiviazione, backup, rete). Il trattamento comprende in particolare la memorizzazione, il salvataggio, la trasmissione, il ripristino e la cancellazione di dati, esclusivamente ai fini della fornitura dei servizi convenuti.
- 2.2 La natura dei dati personali e la cerchia delle persone interessate sono determinate esclusivamente dal titolare del trattamento mediante l'utilizzo dei servizi. Possono rientrarvi dati anagrafici, dati di comunicazione, dati contrattuali, dati di log nonché, a seconda dell'applicazione del titolare del trattamento, dati personali degni di particolare protezione (ad es. dati sulla salute). Le persone interessate possono essere in particolare clienti, pazienti, collaboratori e fornitori del titolare del trattamento.
- 2.3 Per i vServer, i root server e i server dedicati, il titolare del trattamento gestisce autonomamente il sistema operativo, le applicazioni e i dati. FireStorm non dispone di dati di accesso a tali sistemi e non accede ai dati in essi memorizzati. Il trattamento da parte di FireStorm si limita all'esercizio dell'infrastruttura nonché alla creazione e alla conservazione dei backup convenuti. I server dedicati non dispongono di alcuna funzione di backup; il titolare del trattamento è l'unico responsabile del backup dei relativi dati.

3. Luogo del trattamento

- 3.1 I dati provenienti da webhosting, servizi e-mail, vServer, root server, server dedicati nonché tutti i backup e gli snapshot vengono memorizzati e trattati esclusivamente in centri di calcolo in Svizzera.
- 3.2 Per la risoluzione dei nomi georidondante, FireStorm gestisce inoltre server DNS in sedi in Germania e in Francia. Ivi vengono memorizzati esclusivamente dati delle zone DNS (nomi di dominio, indirizzi IP e altre voci DNS), nessun contenuto proveniente da hosting, e-mail o server. Secondo l'allegato 1 dell'ordinanza sulla protezione dei dati (OPDa), tali Stati dispongono di una protezione adeguata dei dati.

- 3.3 Per i prodotti di fornitori terzi che il titolare del trattamento acquista tramite FireStorm (ad es. nomi di dominio, certificati SSL, Microsoft 365) si applicano i luoghi di trattamento indicati nell'allegato 2.
- 3.4 L'amministrazione e il supporto sono svolti da collaboratori di FireStorm in Svizzera. I servizi di supporto esterni dei produttori (ad es. produttori di software o di hardware) ricevono nel singolo caso, nella misura necessaria per l'eliminazione di un guasto, un accesso limitato nel tempo e sorvegliato all'infrastruttura, mai però ai dati all'interno di vServer, root server e server dedicati.

4. Istruzioni del titolare del trattamento

- 4.1 FireStorm tratta i dati personali esclusivamente nell'ambito del contratto principale, del presente accordo e delle istruzioni documentate del titolare del trattamento, salvo che FireStorm sia tenuta a un trattamento in virtù del diritto svizzero. In tal caso FireStorm comunica preventivamente al titolare del trattamento tali requisiti giuridici, nella misura consentita dalla legge.
- 4.2 Il titolare del trattamento impartisce le istruzioni via ticket o per iscritto. Se FireStorm ritiene che un'istruzione violi le prescrizioni sulla protezione dei dati, FireStorm ne informa senza indugio il titolare del trattamento e può sospendere l'esecuzione fino alla conferma o alla modifica dell'istruzione.
- 4.3 Le istruzioni che vanno oltre l'estensione delle prestazioni convenuta vengono fatturate secondo il dispendio.

5. Obblighi di FireStorm

- 5.1 FireStorm tutela la riservatezza dei dati personali. Tutti i collaboratori che hanno accesso all'infrastruttura sono vincolati per iscritto al segreto, anche dopo la fine del rapporto di lavoro, e vengono formati regolarmente in materia di protezione dei dati e di sicurezza delle informazioni.
- 5.2 Non vengono create copie di dati all'insaputa del titolare del trattamento. Fanno eccezione i backup convenuti nonché le copie tecnicamente necessarie per un regolare esercizio.
- 5.3 FireStorm comunica dati personali solo se sussiste un obbligo legale o un ordine di un'autorità svizzera competente o di un tribunale svizzero. Nella misura consentita dalla legge, FireStorm informa preventivamente il titolare del trattamento. Alle richieste di autorità estere viene data risposta solo per la via dell'assistenza giudiziaria.
- 5.4 Quale consulente per la protezione dei dati di FireStorm è designato il signor Christian Geissler (support@firestorm.ch, 0844 300 200). Un cambiamento viene comunicato al titolare del trattamento.

6. Misure tecniche e organizzative

- 6.1 FireStorm adotta le misure tecniche e organizzative descritte nell'allegato 1 al fine di garantire una sicurezza dei dati adeguata al rischio ai sensi dell'art. 8 LPD e dell'art. 32 RGPD.
- 6.2 Le misure vengono verificate regolarmente e adeguate allo stato della tecnica. Il livello di protezione non può essere ridotto. FireStorm comunica al titolare del trattamento le modifiche sostanziali.
- 6.3 Il titolare del trattamento è egli stesso responsabile della sicurezza all'interno di vServer, root server e server dedicati (sistema operativo, applicazioni, dati di accesso, cifratura dei dati delle applicazioni).

7. Notifica di violazioni della sicurezza dei dati

- 7.1 FireStorm informa senza indugio il titolare del trattamento, di regola entro 24 ore, dopo che è stata accertata una violazione della sicurezza dei dati nell'infrastruttura di FireStorm

(piattaforma di virtualizzazione, sistemi di archiviazione e di backup, pannello clienti, rete) che potrebbe riguardare i dati del titolare del trattamento.

- 7.2 Per quanto noto, la notifica contiene la natura della violazione, i sistemi e le categorie di dati interessati, le probabili conseguenze nonché le misure adottate o proposte. Le indicazioni non ancora note vengono fornite successivamente in modo continuo.
- 7.3 FireStorm assiste il titolare del trattamento nell'adempimento dei suoi obblighi di notifica nei confronti dell'IFPDT (art. 24 LPD) o dell'autorità di controllo (art. 33 e 34 RGPD), in particolare con log e marcature temporali.
- 7.4 Se FireStorm rileva traffico anomalo proveniente da sistemi del titolare del trattamento, ad esempio attacchi a terzi o spam, FireStorm informa il titolare del trattamento. Non sussiste alcun obbligo di sorveglianza dei sistemi del titolare del trattamento.

8. Assistenza al titolare del trattamento

- 8.1 Se una persona interessata si rivolge direttamente a FireStorm, FireStorm inoltra senza indugio la richiesta al titolare del trattamento.
- 8.2 Nei limiti di quanto ragionevolmente esigibile, FireStorm assiste il titolare del trattamento nel garantire i diritti delle persone interessate nonché nelle valutazioni d'impatto sulla protezione dei dati. Gli oneri che vanno oltre la messa a disposizione delle informazioni esistenti vengono fatturati secondo il dispendio.

9. Sub-responsabili del trattamento

- 9.1 I sub-responsabili del trattamento impiegati al momento della conclusione del contratto sono elencati nell'allegato 2. Con la conclusione del presente accordo, il titolare del trattamento acconsente al loro impiego.
- 9.2 FireStorm ricorre a nuovi sub-responsabili del trattamento che ottengono accesso a dati provenienti da hosting, e-mail, server o backup solo con il previo consenso scritto del titolare del trattamento. Il consenso può essere dato per e-mail e può essere rifiutato solo per un motivo grave inerente alla protezione dei dati.
- 9.3 Per i prodotti di fornitori terzi (nomi di dominio, certificati SSL, Microsoft 365 e prodotti analoghi), il consenso al rispettivo fornitore si considera dato con l'ordinazione del prodotto. FireStorm informa preventivamente in merito a un cambiamento di tali fornitori; il titolare del trattamento può opporvisi.
- 9.4 FireStorm sceglie i sub-responsabili del trattamento con diligenza e impone loro contrattualmente obblighi corrispondenti al presente accordo.
- 9.5 Le mere prestazioni accessorie senza accesso a dati personali, in particolare spazio, energia elettrica, raffreddamento, sicurezza fisica e connessione di rete da parte dei gestori di centri di calcolo, non sono considerate trattamento da parte di sub-responsabili. Per motivi di trasparenza sono elencate nell'allegato 2.

10. Diritti di controllo

- 10.1 Su richiesta, FireStorm mette a disposizione del titolare del trattamento le informazioni necessarie a comprovare il rispetto del presente accordo.
- 10.2 Il titolare del trattamento ha il diritto di controllare il rispetto del presente accordo, previo appuntamento (di regola con almeno 14 giorni di anticipo), durante gli orari d'ufficio, personalmente o tramite un terzo vincolato al segreto. I controlli non devono pregiudicare l'esercizio e la sicurezza di altri clienti. Il dispendio di FireStorm viene fatturato secondo le tariffe orarie di volta in volta valide.

11. Obblighi del titolare del trattamento

- 11.1 Il titolare del trattamento è l'unico responsabile della liceità del trattamento dei dati e della tutela dei diritti delle persone interessate.
- 11.2 Il titolare del trattamento informa senza indugio FireStorm se constata errori o irregolarità nel trattamento.

12. Restituzione e cancellazione

- 12.1 Fino alla fine del contratto il titolare del trattamento può esportare autonomamente i propri dati in qualsiasi momento; per i server con pieno accesso root anche come immagine completa. Su richiesta, FireStorm assiste il titolare del trattamento a tal fine contro fatturazione secondo il dispendio.
- 12.2 Al più tardi 30 giorni dopo la fine del contratto o dopo l'autorizzazione del titolare del trattamento, FireStorm cancella tutti i dati del titolare del trattamento, inclusi server, supporti di dati, snapshot e backup, a meno che vi si opponga un obbligo legale di conservazione. Su richiesta, FireStorm conferma la cancellazione per iscritto.
- 12.3 I dati vengono memorizzati in forma cifrata sui supporti di dati. I supporti di dati difettosi o dismessi vengono cancellati a regola d'arte o distrutti fisicamente prima dello smaltimento.

13. Responsabilità

- 13.1 Per la responsabilità si applicano le disposizioni delle CG di FireStorm (in particolare la cifra 12).
- 13.2 Dei danni subiti da una persona interessata a causa di un trattamento dei dati illecito o inesatto risponde, nei rapporti con la persona interessata, il titolare del trattamento. Un regresso del titolare del trattamento nei confronti di FireStorm è ammesso solo se FireStorm ha violato il presente accordo intenzionalmente o per negligenza grave.
- 13.3 Le pene convenzionali sono escluse.

14. Diritto di disdetta straordinaria

- 14.1 In caso di gravi violazioni del presente accordo da parte di FireStorm, in particolare delle prescrizioni applicabili in materia di protezione dei dati, il titolare del trattamento può disdire senza preavviso il contratto principale per i servizi interessati. In caso di violazioni irrilevanti, il titolare del trattamento fissa dapprima un termine adeguato per porvi rimedio.

15. Disposizioni finali

- 15.1 Entrambe le parti trattano in modo confidenziale, anche dopo la fine del contratto, tutte le conoscenze acquisite nell'ambito del presente accordo in merito a segreti d'affari e misure di sicurezza dei dati dell'altra parte.
- 15.2 Per il presente accordo non viene riscosso alcun corrispettivo supplementare, salvo diversa disposizione esplicita.
- 15.3 Le modifiche e le integrazioni richiedono la forma scritta; è sufficiente l'e-mail. Gli accordi individuali con singoli titolari del trattamento prevalgono sul presente accordo.
- 15.4 Qualora singole disposizioni fossero inefficaci, l'efficacia delle restanti disposizioni rimane impregiudicata. Esse sono sostituite da una regolamentazione efficace che si avvicini il più possibile allo scopo economico.
- 15.5 Si applica esclusivamente il diritto svizzero. Il foro competente è Hinwil.
- 15.6 I termini sono utilizzati ai sensi della LPD; nella misura in cui sia applicabile il RGPD, ai sensi del RGPD.

Allegato 1: Misure tecniche e organizzative

Sicurezza fisica (controllo degli accessi fisici)

- Esercizio dei server in centri di calcolo in Svizzera certificati secondo ISO/IEC 27001
- Accesso solo per persone autorizzate, sorveglianza dei centri di calcolo 24 ore su 24
- Alimentazione elettrica e connessione di rete ridondanti
- Server di backup in un centro di calcolo separato in Svizzera

Controllo degli accessi ai sistemi e ai dati

- Accesso amministrativo all'infrastruttura da parte di collaboratori propri di FireStorm in Svizzera; servizi di supporto esterni dei produttori solo nel singolo caso, limitati nel tempo e sorvegliati
- Le interfacce di gestione della piattaforma di virtualizzazione e di backup non sono raggiungibili direttamente da Internet
- Autenticazione a due fattori disponibile per il pannello clienti
- Nessun dato di accesso di FireStorm ai vServer, ai root server e ai server dedicati dei clienti; i dati di accesso sono impostati dal cliente stesso
- Registrazione delle azioni a livello di piattaforma (accesso alla console, avvio e arresto, snapshot, backup, ripristini) con utente e marcatura temporale

Cifratura e separazione

- Memorizzazione cifrata dei dati sui supporti di dati
- Trasmissione cifrata (TLS) per pannello clienti, servizi e-mail e amministrazione
- Separazione logica dei clienti mediante macchine virtuali proprie o account di hosting propri

Disponibilità e resilienza

- Backup giornalieri su sistemi di backup separati, non raggiungibili dai sistemi dei clienti (incluso: backup giornaliero con più stati di salvataggio dell'ultima settimana; salvataggi più frequenti e conservazione più lunga con supplemento di prezzo). I server dedicati non dispongono di alcuna funzione di backup.
- Protezione DDoS a livello di rete, firewall a monte con WAF di base
- Sorveglianza dei sistemi 24 ore su 24, servizio guasti 24/7

Integrità e manutenzione

- Installazione degli aggiornamenti di sicurezza dei produttori per l'infrastruttura senza indugio, al più tardi non appena è disponibile una patch
- Cancellazione a regola d'arte o distruzione fisica dei supporti di dati difettosi e dismessi

Organizzazione

- Impegno scritto al segreto di tutti i collaboratori
- Collaboratori con certificazione personale ISO/IEC 27001 Foundation
- Consulente per la protezione dei dati designato
- Assicurazione di responsabilità civile professionale per fornitori di servizi informatici e di telecomunicazione, inclusa copertura cyber

Allegato 2: Sub-responsabili del trattamento e fornitori di servizi

Per tutti i prodotti

- Gestori di centri di calcolo in Svizzera (colocation, ISO/IEC 27001): spazio, energia elettrica, raffreddamento, sicurezza fisica e connessione di rete. Nessun accesso logico a sistemi o

dati. Non sono sub-responsabili del trattamento ai sensi della cifra 9.5; indicazioni su richiesta con vincolo di riservatezza.

Solo per i servizi DNS

- Server DNS in sedi in Germania e in Francia (georidondanza). Vengono memorizzati esclusivamente dati delle zone DNS.

Solo in caso di ordinazione del rispettivo prodotto

- Nomi di dominio: le autorità di registrazione e i registrar competenti per la rispettiva estensione di dominio (ad es. SWITCH per .ch e .li, DENIC per .de, nic.at per .at, registrar accreditati ICANN). Vengono trattati i dati del titolare del dominio.
- Certificati SSL: la rispettiva autorità di certificazione e i suoi partner di distribuzione. Vengono trattati i dati della richiesta del certificato.
- Microsoft 365: Microsoft e il distributore Pax8. Si applicano le disposizioni sulla protezione dei dati di Microsoft.