**Allegato 2 all'ordine ai sensi dell'articolo 28 DS-GVO: misure tecniche e organizzative ai sensi dell'articolo 32 DS-GVO e allegato**

**Versione marzo 2019**

1. **Riservatezza**

**Controllo di accesso**

* **Centri dati**
	+ Sistema di controllo accessi elettronico con registrazione Recinzione ad alta sicurezza attorno all'intero parco del data center
	+ Assegnazione documentata delle chiavi ai dipendenti e ai clienti di colocation per i rack di colocation (ogni cliente esclusivamente per il proprio rack di colocation)
	+ Linee guida per l'accompagnamento e l'identificazione degli ospiti nell'edificio
	+ Personale 24 ore su 24, 7 giorni su 7 dei data center
	+ Videosorveglianza agli ingressi e alle uscite, varchi di sicurezza e sale server
	+ L'accesso alle sale da parte di persone esterne (es. Visitatori) è limitato come segue: solo in compagnia di un dipendente FireStorm ISP GmbH
* **amministrazione**
	+ Sistema di controllo accessi elettronico con registrazione
	+ Videosorveglianza agli ingressi e alle uscite
* **Controllo di accesso**
	+ per l' ordine principale " root server ", " server housing "

 Password del server, che vengono modificate dal cliente solo dopo la prima messa in servizio da lui stesso e non sono note al contraente

 La password per l'interfaccia di amministrazione viene assegnata dal client - le password devono soddisfare le linee guida predefinite.

* + per l' ordine principale " SiteDesigner ", "Webhosting", " Mailhosting ", "Reseller-Hosting", "Managed Server", "Domains", "DNS Service", "SMS Gateway", "SSL Certificate" e tutti gli altri

 L'accesso è protetto da password, l'accesso è possibile solo per i dipendenti autorizzati dell'appaltatore; le password utilizzate devono essere di lunghezza minima

* **Controllo di accesso**
	+ per i sistemi di gestione interna dell'appaltatore

 Tramite regolari aggiornamenti di sicurezza (secondo il rispettivo stato dell'arte) il contraente garantisce che l'accesso non autorizzato sia impedito.

 Procedura di autorizzazione vincolante e a prova di revisione per i dipendenti dell'appaltatore

* + per l' ordine principale " Rootserver ", " Serverhousing

 La responsabilità del controllo degli accessi è del cliente.

* + per l' ordine principale " SiteDesigner ", "Webhosting", " Mailhosting ", "Reseller-Hosting", "Managed Server", "Domains", "DNS Service", "SMS Gateway", "SSL Certificate" e tutti gli altri

 Tramite regolari aggiornamenti di sicurezza (secondo il rispettivo stato dell'arte), l'appaltatore garantisce che l'accesso non autorizzato sia impedito.

 Procedura vincolante di assegnazione dell'autorizzazione a prova di revisione per i dipendenti dell'appaltatore

 Per i dati / software trasferiti, il cliente è l'unico responsabile della sicurezza e degli aggiornamenti .

* **Controllo del supporto dati**
	+ Centri dati

 I dischi rigidi vengono sovrascritti (eliminati) più volte dopo la terminazione con una procedura definita. Dopo il controllo, i dischi rigidi vengono reinstallati.

 I dischi rigidi difettosi non possono essere eliminati in modo sicuro vengono distrutti (distrutti) direttamente nel datacenter.

* **Controllo della separazione**
	+ per i sistemi di gestione interna dell'appaltatore

 I dati vengono archiviati fisicamente o logicamente separati dagli altri dati.

 Viene inoltre eseguito il backup dei dati su sistemi separati logicamente e / o fisicamente.

* + per l' ordine principale " Rootserver ", " Serverhousing

 Il controllo della separazione è responsabilità del cliente.

* + per l' ordine principale " SiteDesigner ", "Webhosting", " Mailhosting ", "Reseller-Hosting", "Managed Server", "Domains", "DNS Service", "SMS Gateway", "SSL Certificate" e tutti gli altri

  I dati vengono archiviati fisicamente o logicamente separati dagli altri dati.

 Viene inoltre eseguito il backup dei dati su sistemi separati logicamente e / o fisicamente.

* **Pseudonimizzazione**
	+ Il cliente è responsabile della pseudonimizzazione

1. **Integrità (art. 32 cpv. 1 lett. B DS-GVO)**
* **Controllo inoltro**
	+ Tutti i dipendenti sono istruiti ai sensi dell'articolo 32 cpv. 4 DS-GVO e sono obbligati a garantire che i dati personali siano trattati nel rispetto delle normative sulla protezione dei dati.
	+ Cancellazione dei dati in conformità con le norme sulla protezione dei dati dopo il completamento dell'ordine.
	+ Le possibilità per la trasmissione di dati crittografati sono fornite nell'ambito della descrizione del servizio dell'ordine principale.
* **Controllo dell'input**
	+ per i sistemi di gestione interna dell'appaltatore

 I dati vengono inseriti o raccolti dal cliente stesso.

 Le modifiche ai dati vengono registrate.

* + per l' ordine principale " root server ", " server housing "

 La responsabilità del controllo degli input spetta al cliente.

* + per l' ordine principale " SiteDesigner ", "Webhosting", " Mailhosting ", "Reseller-Hosting", "Managed Server", "Domains", "DNS Service", "SMS Gateway", "SSL Certificate" e tutti gli altri

 I dati vengono inseriti o raccolti dal cliente stesso.

 Le modifiche ai dati vengono registrate.

1. **Disponibilità e resilienza (art. 32 cpv. 1 lett. B DS-GVO)**
* **Controllo della disponibilità**
	+ per i sistemi di gestione interna dell'appaltatore

 Concetto di backup e ripristino con backup giornaliero di tutti i dati rilevanti.

 Uso esperto di programmi di protezione (scanner antivirus, firewall, programmi di crittografia, filtri SPAM).

 Utilizzo del mirroring del disco rigido per tutti i server rilevanti.

 Monitoraggio di tutti i server rilevanti

 Uso di gruppi di continuità, sistema di alimentazione di emergenza

 Protezione DDoS sempre attiva

* + Con il server principale dell'ordine principale , l' alloggiamento del server ^

  backup dei dati è responsabilità del cliente

 Uso di gruppi di continuità, sistema di alimentazione di emergenza

 Protezione DDoS sempre attiva

* + per l'ordine principale " SiteDesigner ", "Webhosting", " Mailhosting ", "Reseller-Hosting", "Managed Server", "Domains", "DNS Service", "SMS Gateway", "SSL Certificate" e tutti gli altri

 Concetto di backup e ripristino con backup giornaliero dei dati a seconda dei servizi prenotati del contratto principale.

 Uso del mirroring del disco rigido.

 Uso di un gruppo di continuità, sistema di backup di rete.

 Utilizzo di firewall hardware e software, firewall per applicazioni Web (WAF) e normative sulle porte.

 Protezione DDoS sempre attiva .

* **Recupero rapido (art. 32 cpv. 1 lett. C DS-GVO);**
	+ Per tutti i sistemi interni viene definita una catena di escalation che specifica chi deve essere informato in caso di errore per poter ripristinare il sistema il più rapidamente possibile.

1. **Procedure per la revisione, la valutazione e la valutazione periodiche (art. 32 cpv. 1 lett. D DS-GVO; art. 25 cpv. 1 DS-GVO)**
	* Il sistema di gestione della protezione dei dati e il sistema di gestione della sicurezza delle informazioni sono stati combinati in un DIMS (Data Protection Information Security Management System).
	* È disponibile la gestione della risposta agli incidenti.
	* Durante lo sviluppo del software vengono prese in considerazione preimpostazioni favorevoli alla protezione dei dati (art. 25 cpv. 2 DS-GVO).
* **Controllo degli ordini**
	+ I nostri dipendenti vengono istruiti a intervalli regolari sulla legislazione sulla protezione dei dati e conoscono le istruzioni procedurali e le linee guida per l'utente per il trattamento dei dati per conto del cliente, anche per quanto riguarda il diritto del cliente di impartire istruzioni. I termini e le condizioni generali contengono informazioni dettagliate sul tipo e l'ambito del trattamento e dell'utilizzo commissionati dei dati personali del cliente.
	+ Le CG contengono informazioni dettagliate sullo scopo dei dati personali del cliente.
	+ FireStorm ISP GmbH ha nominato un responsabile della protezione dei dati della società e un responsabile della sicurezza delle informazioni. Entrambi sono integrati nei processi operativi rilevanti dall'organizzazione per la protezione dei dati e dal sistema di gestione della sicurezza delle informazioni.