Elettro-Celio SA
Via Industrie 23, 6512 Giubiasco
+41 91 857 36 41
www.celio.ch, info@celio.ch

CONTRATTO RELATIVO AL TRATTAMENTO DEI DATI
(Accordo)

tra

Cliente della «Dichiarazione di consenso al Contratto relativo al trattamento dei dati»
Cliente (Titolare del trattamento; committente)

e

Elettro-Celio SA
Via Industrie 23, 6512 Giubiasco in qualità di
Addetto al trattamento dei dati (Responsabile del trattamento; contraente)

Cliente e addetto al trattamento dei dati singolarmente «**la parte**» e congiuntamente «**le parti**»

riguardante il

trattamento dei dati in conformità al diritto svizzero

1 Oggetto

(a) Tra le parti sussiste un rapporto giuridico, la cui esecuzione richiede la trasmissione di dati personali dal cliente all'addetto al trattamento dei dati. Il presente accordo viene stipulato tra le parti per garantire un'adeguata protezione nella trasmissione di dati personali. In caso di conflitto tra il presente accordo e altri contratti, l'accordo prevarrà se e nella misura in cui si riferisce al trattamento di dati personali da parte del contraente nel quadro del contratto in essere.

1.1 Definizioni

(a) Salvo disposizioni contrarie nel presente accordo, tutti i termini avranno lo stesso significato previsto dalla Legge federale sulla protezione dei dati («**LPD**») del 19 giugno 1992 o del 20 settembre 2020, non appena quest'ultima entrerà in vigore. Ogni riferimento alla LPD deve sempre includere un riferimento all'attuale Ordinanza relativa alla LPD («**OLPD**») e a qualsiasi altra norma giuridica del diritto svizzero sulla protezione dei dati su cui si basa.

(b) Il presente accordo aiuta inoltre le parti a rispettare il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 («RGPD UE»). I rimandi al RGPD UE sono pertinenti solo per le modalità di trattamento dei dati alle quali è applicabile il RGPD UE. Qualora i rimandi al RGPD UE determinino un conflitto con il diritto svizzero sulla protezione dei dati, quest'ultimo avrà la precedenza.

1.2 Descrizione del trattamento dei dati

(a) I dati personali oggetto del trattamento e le finalità del trattamento sono descritti nell'Allegato 1 al presente accordo. L'Allegato 1 costituisce parte integrante del presente accordo e può subire periodicamente modifiche unilaterali da parte del cliente.

2 Obblighi del cliente

(a) Il cliente garantisce che

(1) la trasmissione dei dati personali e il trattamento degli stessi da parte dell'addetto al trattamento dei dati come stabilito nel presente accordo siano consentiti in base al diritto applicabile; inoltre, il cliente garantisce che la trasmissione al contraente sia conforme al diritto applicabile

(2) nessun'altra disposizione giuridica vieti la trasmissione per il trattamento dei dati

(b) Il cliente ha accertato che le misure tecniche e organizzative adottate dall'addetto al trattamento dei dati e descritte nell'Allegato 2 sono sufficienti per garantire un'adeguata protezione dei dati personali trasmessi.

3 Obblighi dell'addetto al trattamento dei dati

3.1 Aspetti generali

(a) Per quanto riguarda il trattamento dei dati personali in conformità all'Allegato 1, l'addetto al trattamento dei dati garantisce che

(1) tratterà i dati personali conformemente al presente accordo ed esclusivamente per le finalità perseguite dal cliente

(2) le finalità perseguite dal cliente risultino dall'Allegato 1 o da istruzioni esplicite del cliente oppure siano stabilite da un altro accordo stipulato con il cliente

(3) fornirà al cliente le informazioni necessarie per verificare il rispetto degli obblighi previsti dal presente accordo

(4) per le proprie attrezzature di lavoro e applicazioni nonché per i propri prodotti o servizi terrà conto dei principi di Privacy by design e Privacy by default

(5) informerà il cliente qualora non fosse più in grado di rispettare il presente accordo o se dovesse prevedere di non essere più in grado di rispettarlo in futuro

(6) fornirà al cliente l'indirizzo di contatto per richieste in materia di protezione dei dati e comunicherà di propria iniziativa eventuali modifiche

(7) supporterà adeguatamente il cliente nelle Valutazioni d'impatto sulla protezione dei dati (in particolare ai sensi dell'art. 35 RGPD UE) o nelle consultazioni preliminari (in particolare ai sensi dell'art. 36 RGPD UE)

(8) collaborerà con le autorità di vigilanza competenti nella misura consentita dalla legge

(b) Le persone incaricate del cliente devono essere notificate all'addetto al trattamento dei dati in forma di testo all'inizio del trattamento stesso. In caso di sostituzione o prolungato impedimento della persona di contatto, il contraente sarà immediatamente informato per iscritto in merito al successore o al sostituto. Le istruzioni verbali sono vincolanti solo in caso di conferma immediata da parte del cliente in forma scritta. La posta elettronica è sufficiente per il rispetto della forma scritta.

(c) Il contraente deve informare immediatamente il committente se ritiene che un'istruzione violi le disposizioni di legge. Il contraente ha il diritto di sospendere l'esecuzione delle istruzioni pertinenti fino a quando la loro legalità non sia confermata dal cliente o l'istruzione interessata non venga modificata.

3.2 Sicurezza dei dati

(a) Durante il presente accordo, l'addetto al trattamento dei dati si avvarrà di adeguate misure tecniche e

organizzative così come richiesto dalla LPD e dall'art. 32 RGPD UE. L'addetto al trattamento dei dati ha tenuto conto dello stato della tecnica, dei costi di attuazione e del tipo, della portata e delle finalità del trattamento nonché della probabilità di accadimento e della gravità del rischio per i diritti fondamentali e della personalità dei soggetti interessati. Le misure sono descritte nell'Allegato 2 e vengono riesaminate periodicamente. Sono ammesse modifiche alle misure, a condizione che non comportino un livello di sicurezza inferiore rispetto al precedente livello.

(b) L'addetto al trattamento dei dati

(1) si avvarrà esclusivamente di dipendenti vincolati contrattualmente o legalmente alla riservatezza e che siano stati preventivamente informati sulle disposizioni in materia di protezione dei dati che li riguardano

(2) informerà e collaborerà tempestivamente con il cliente se ritiene di non essere più in grado o che potrebbe non essere più in grado di rispettare il presente accordo e, in particolare, gli obblighi relativi alla sicurezza dei dati

(3) sosterrà il cliente con misure che garantiscano un livello di protezione dei dati adeguato al rischio

(4) segnalerà tempestivamente al cliente e documenterà un'eventuale violazione della sicurezza dei dati (compreso l'accesso non autorizzato ai dati personali ai sensi dell'Allegato 1) in modo che il cliente possa segnalare la violazione entro 72 ore a un'autorità di vigilanza (in particolare ai sensi dell'art 33 RGPD UE) o alla persona interessata (in particolare ai sensi dell'art. 34 RGPD UE); la segnalazione deve includere almeno i) il tipo di violazione della sicurezza dei dati, ii) le conseguenze della violazione (in particolare per i dati come previsto dall'Allegato 1), iii) le misure adottate e iv) le misure previste.

(c) Previa richiesta legittima, il contraente metterà a disposizione del cliente i rapporti sulla sicurezza dei dati. Il cliente ha inoltre il diritto di verificare a proprie spese il rispetto della sicurezza dei dati concordata o di farla verificare da terzi tenuti al rispetto dell'obbligo di discrezione. I controlli devono essere notificati in tempo utile e concordati con il contraente.

3.3 Subappaltatori

(a) L'addetto al trattamento dei dati può trasferire il trattamento dei dati a subappaltatori solo previo consenso del cliente. Il cliente può rifiutare il consenso solo per giustificati motivi. Se il cliente accetta un subappaltatore, ciò non esonera in alcun modo il contraente dalla sua responsabilità per il trattamento dei dati in outsourcing.

(b) L'addetto al trattamento dei dati è tenuto a stipulare contratti con subappaltatori che garantiscano almeno un livello di protezione dei dati conforme al presente accordo.

(c) Di norma non sono considerati trattamento in subappaltato i servizi accessori per il contraente senza riferimento ai dati del cliente come da Allegato 1 (ad esempio servizi di telecomunicazioni, servizi postali / di trasporto, manutenzione e servizi per l'utente o smaltimento di supporti dati e altre misure volte a garantire la riservatezza, la disponibilità, l'integrità e la solidità dell'hardware e del software). Il contraente è tuttavia tenuto ad adottare misure di controllo adeguate per garantire la protezione e la sicurezza dei dati del committente anche in riferimento a servizi accessori.

3.4 Divulgazione all'estero

(a) Il trattamento dei dati ai sensi dell'Allegato 1 ha luogo, in linea di principio, in Svizzera o in uno Stato membro dell'Unione europea o in un altro Stato che ha aderito all'accordo sullo Spazio economico europeo. Qualsiasi trasferimento in un altro Paese terzo può aver luogo solo in caso di adempimento dei requisiti di legge pertinenti (art. 6 LPD o art. 16 segg. LPD del 20 settembre 2020; art. 44 segg.

RGPD UE).

(b) Se l'addetto al trattamento dei dati ricorre a subappaltatori in Stati che non dispongono di un livello adeguato di protezione dei dati in base a quanto stabilito dall'Incaricato federale della protezione dei dati e della trasparenza (IFPDT), dall'Allegato alla OLPD o dalla Commissione dell'UE, l'addetto al trattamento dei dati garantisce che la divulgazione sia consentita ai sensi della Legge sulla protezione dei dati adottando misure adeguate per ciascun trasferimento dei dati. Di norma, l'addetto al trattamento dei dati concorda, a tal fine, con i subappaltatori le clausole contrattuali tipo conformemente alla decisione di esecuzione (UE) 2021/914 della Commissione europea («clausole contrattuali tipo aggiornate dell'UE»). Il contraente si accorda sul modulo corretto (di regola il modulo 3) delle clausole contrattuali tipo aggiornate, apportando in particolare le seguenti modifiche al trattamento dei dati soggetti al diritto svizzero sulla protezione dei dati:

(1) I riferimenti al RGPD UE vanno intesi come riferimenti alla LPD svizzera.

(2) L'Incaricato federale della protezione dei dati e della trasparenza (IFPDT) è designato come autorità di vigilanza.

(3) Il foro competente del luogo di domicilio delle persone interessate domiciliate in Svizzera non deve essere escluso.

(4) Fino all'entrata in vigore della LPD del 20 settembre 2020, il termine «dati personali» comprende anche i dati relativi alle persone giuridiche.

(c) Per la collaborazione esistente con subappaltatori in Paesi che non hanno un livello di protezione dei dati adeguato che si basa ancora sulle clausole contrattuali tipo adottate ai sensi della direttiva 95/46/CE, entro il 27 dicembre 2022 devono essere concordate le clausole contrattuali tipo aggiornate o un'altra garanzia adeguata.

4 Diritti delle persone interessate

(a) Il cliente è tenuto a garantire che i soggetti interessati ricevano le informazioni a cui hanno diritto in relazione ai propri diritti all'informazione (diritto di informazione/accesso), alla divulgazione e alla trasmissione dei dati, alla rettifica, al blocco, alla soppressione o alla cancellazione dei dati in conformità alla LPD o al capitolo III del RGPD UE. L'addetto al trattamento dei dati

(1) trasmetterà tempestivamente al cliente tutte le richieste relative ai dati di cui all'Allegato 1, senza rispondervi personalmente

(2) collaborerà con il cliente ed erogherà i servizi di assistenza necessari affinché quest'ultimo rispetti i diritti degli interessati ai sensi della LPD o del capitolo III del RGPD UE

(3) risponderà in modo completo e veritiero alle richieste del cliente in merito ai diritti degli interessati entro 15 giorni lavorativi o spiegherà, entro questo termine, perché la risposta richiede più tempo; in nessun caso, tuttavia, il ritardo può comportare il fatto che il cliente non sia in grado di adempiere ai propri obblighi

5 Durata e risoluzione

(a) Se non diversamente concordato per iscritto, il presente accordo terminerà automaticamente alla risoluzione del contratto principale o alla disdetta della «Dichiarazione di consenso al Contratto relativo al trattamento dei dati». Le disposizioni del presente accordo resteranno tuttavia in vigore anche dopo la risoluzione del contratto principale e rimarranno valide finché il contraente sarà in possesso dei dati personali.

(b) Il cliente ha il diritto di risolvere in qualsiasi momento il presente accordo per validi motivi, qualora l'addetto al trattamento dei dati, nonostante un sollecito, non ponga rimedio a tali validi motivi entro

un periodo di tempo ragionevole. Sussistono validi motivi quando il contraente

(1) viola gravemente i propri obblighi derivanti dal presente accordo

(2) viola intenzionalmente o per negligenza grave le disposizioni della Legge federale sulla protezione dei dati o del RGPD UE

(3) non esegue le istruzioni del cliente

(c) Al momento della risoluzione del presente accordo, indipendentemente dal motivo, l'addetto al trattamento dei dati:

(1) distruggerà o cancellerà irreversibilmente tutti i dati personali e le loro copie trasmessi nell'ambito del presente accordo, farà in modo che i subappaltatori li distruggano o li cancellino e confermerà al cliente tale operazione

(2) oppure, a discrezione del cliente, restituirà tempestivamente i dati personali trasmessi ai sensi del presente contratto e farà in modo che i subappaltatori li restituiscano

(d) Qualora la legislazione a cui è soggetto l'addetto al trattamento dei dati gli vieti di restituire o distruggere i dati personali o parte di essi, l'addetto al trattamento dei dati ne informerà il cliente, conserverà tali dati personali con riservatezza e non li tratterà attivamente.

6 Varie ed eventuali

6.1 Integrazioni

(a) Eventuali modifiche, integrazioni o cancellazioni delle disposizioni del presente accordo devono essere effettuate per iscritto per essere valide. Anche la modifica di tale obbligo richiede un accordo scritto perché sia valida. Eventuali cambiamenti di indirizzo devono essere comunicati tempestivamente all'altra parte secondo le modalità sopra concordate.

6.2 Registro delle attività di trattamento

(a) Ciascuna parte è responsabile della tenuta di un registro delle attività di trattamento dei dati, salvo il caso in cui si applichi una deroga.

6.3 Costi

(a) I costi associati all'esecuzione del presente accordo e all'adempimento degli obblighi ivi stabiliti sono inclusi nella remunerazione concordata tra le parti nel contratto principale.

6.4 Responsabilità

(a) Qualora l'inosservanza del presente accordo per negligenza grave o violazione intenzionale da parte del contraente comporti danni al cliente o richieste di risarcimento da parte di terzi nei confronti di quest'ultimo, il contraente dovrà tenere indenne il cliente da tali richieste.

6.5 Clausola salvatoria

(a) Se una disposizione del presente accordo non dovesse essere applicabile o valida, essa decadrà solo per la parte in cui è inapplicabile o non valida e sarà sostituita per il resto da una disposizione valida e applicabile che rifletta il più possibile lo scopo legale ed economico della disposizione non valida. Le restanti disposizioni del presente accordo resteranno valide e vincolanti.

6.6 Divieto di cessione

(a) L'ammissibilità della cessione dei diritti e degli obblighi derivanti dal presente accordo va valutata in

base alle norme del contratto principale. In assenza di norme specifiche nel contratto principale, alle parti non è consentito cedere o trasferire a terzi, in tutto o in parte, il presente contratto o qualsiasi diritto e obbligo derivante da esso senza previo consenso scritto dell'altra parte. Qualsiasi cessione o trasferimento effettuati senza previo consenso scritto saranno nulli.

6.7 Diritto applicabile

(a) Il presente accordo è soggetto al diritto sostanziale svizzero, a esclusione delle disposizioni in materia di diritto di collisione e della Convenzione di Vienna sulla compravendita internazionale di merci.

6.8 Foro competente

Per ogni controversia derivante da o connessa al presente accordo saranno competenti in via esclusiva i tribunali ordinari della sede del cliente.

Elettro-Celio SA
Via Industrie 23, 6512 Giubiasco
+41 91 857 36 41
www.celio.ch, info@celio.ch

Allegato 1

Finalità del trattamento	L'oggetto del trattamento dei dati personali da parte dell'addetto al trattamento dei dati è la fornitura dei servizi di manutenzione e assistenza descritti nel contratto principale a favore del cliente.
Durata del trattamento	I dati personali saranno trattati solo per la durata del contratto principale o per la durata della «Dichiarazione di consenso al Contratto relativo al trattamento dei dati».
Categorie delle persone interessate	Dipendenti, clienti, partner.
Categorie di dati personali	Nome, e-mail, numero di telefono, indirizzo, data di nascita, professione o altre informazioni, dichiarazioni che si riferiscono a una persona identificata o identificabile tramite tali informazioni.
Luogo di conservazione e trattamento	Presso l'indirizzo aziendale del cliente e dei suoi subappaltatori autorizzati.
Verifiche in loco	No
Subaddetto al trattamento dei dati	Subaddetti al trattamento dei dati autorizzati per la fornitura dei servizi di manutenzione e assistenza descritti nel contratto principale a favore del cliente.
Trasferimento al di fuori dell'UE/SEE Svizzera	Non consentito
Istruzioni specifiche o altre disposizioni speciali	Nessuna

Allegato 2: Misure tecniche e organizzative

Descrizione delle misure di sicurezza tecniche e organizzative adottate dall'addetto o dagli addetti al trattamento dei dati:

1 Misure di sicurezza organizzative

1.1 Gestione della sicurezza

(a) Piano e procedura di sicurezza: l'addetto al trattamento dei dati dispone di un piano di sicurezza documentato per il trattamento dei dati personali.

(b) Ruoli e responsabilità:

(1) I ruoli e le responsabilità associati al trattamento dei dati personali sono chiaramente definiti e assegnati in conformità al piano di sicurezza.

(2) In caso di riorganizzazioni interne o licenziamenti e di cambio di mansione, la revoca dei diritti e delle responsabilità è chiaramente definita con idonee procedure di passaggio di consegne.

(c) Politica dei controlli degli accessi: a ogni ruolo coinvolto nel trattamento dei dati personali vengono assegnati specifici diritti di controllo degli accessi sulla base del principio «need to know».

(d) Gestione delle risorse / dei beni: l'addetto al trattamento dei dati dispone di un registro delle risorse IT (hardware, software e rete) utilizzate per il trattamento dei dati personali. La gestione e l'aggiornamento del registro sono affidati a una persona specifica.

(e) Gestione delle modifiche: l'addetto al trattamento dei dati garantisce che tutte le modifiche al sistema IT siano registrate e controllate da una persona specifica (ad esempio Responsabile IT o Responsabile della sicurezza). Tale processo viene costantemente monitorato.

1.2 Risposta in caso di incidenti e continuità operativa

(a) Gestione di incidenti / violazioni della protezione dei dati personali:

(1) Viene stabilito un piano di risposta agli incidenti con procedure dettagliate per garantire un intervento efficace e adeguato in caso di incidenti relativi ai dati personali.

(2) L'addetto al trattamento dei dati segnalerà tempestivamente al cliente qualsiasi incidente di sicurezza che abbia causato la perdita, l'uso improprio o l'accesso non autorizzato ai dati personali del cliente.

(b) Continuità operativa: L'addetto al trattamento dei dati ha definito le principali procedure da seguire e i controlli da effettuare per garantire il necessario livello di continuità e disponibilità del sistema IT per il trattamento dei dati personali (in caso di incidente / violazione della protezione dei dati personali).

1.3 Risorse umane

(a) Riservatezza del personale: L'addetto al trattamento dei dati si accerta che tutto il personale sia consapevole delle proprie responsabilità e dei propri obblighi in relazione al trattamento dei dati personali. Ruoli e responsabilità vengono chiaramente comunicati durante la procedura precedente l'assunzione e/o in fase di inserimento.

(b) Formazione: L'addetto al trattamento dei dati si accerta che tutto il personale sia adeguatamente informato in merito ai controlli di sicurezza del sistema IT relativi alla propria attività lavorata quotidiana. Il personale coinvolto nel trattamento dei dati personali viene inoltre adeguatamente informato mediante campagne di sensibilizzazione periodiche sui requisiti di protezione dei dati pertinenti e sugli obblighi di legge.

2 Misure di sicurezza tecniche

2.1 Controllo degli accessi e autenticazione

(a) È stato adottato un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema informatico. Il sistema consente di creare, approvare, verificare e cancellare gli account utente.

(b) Va evitato l'utilizzo di account utente condivisi. Nei casi in cui ciò sia necessario si deve garantire che tutti gli utenti dell'account condiviso abbiano gli stessi ruoli e le stesse responsabilità.

(c) Nel concedere l'accesso o nell'assegnare i ruoli agli utenti si osserverà il principio della «necessità di conoscere» al fine di limitare il numero di utenti che hanno accesso ai dati personali a quelli che necessitano di tale accesso per adempiere alle finalità di trattamento dell'addetto al trattamento dei dati.

(d) Se i meccanismi di autenticazione si basano su password, l'addetto al trattamento dei dati richiede che la password sia composta da almeno otto caratteri e che soddisfi parametri di controllo molto severi, tra cui la lunghezza, la complessità e la non ripetibilità dei caratteri.

(e) I dati di autenticazione (ad esempio ID utente e password) non devono mai essere trasmessi in rete senza protezione.

(f) I dati di autenticazione e i controlli degli accessi ai sistemi del cliente esulano dal controllo dell'addetto al trattamento dei dati.

2.2 Protocollo e monitoraggio

(a) Per ogni sistema/applicazione utilizzati per il trattamento di dati personali vengono attivati dei file di protocollo. Tali file riguardano tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione).

(b) La registrazione dell'autenticazione / degli accessi è effettuata dal cliente.

2.3 Sicurezza dei dati in stato di inattività

(a) Sicurezza del server / della banca dati

(1) I server della banca dati e delle applicazioni sono configurati per operare con un account separato con privilegi minimi del sistema operativo per funzionare correttamente.

(2) I server della banca dati e delle applicazioni elaborano solo i dati personali il cui trattamento è effettivamente necessario per raggiungere le finalità specifiche previste.

(3) La sicurezza delle banche dati e dei server produttivi è garantita dal cliente ed esula dal controllo dell'addetto al trattamento dei dati.

(b) Sicurezza sul posto di lavoro:

(1) Gli utenti non possono disattivare né aggirare le impostazioni di sicurezza.

(2) Le applicazioni antivirus e le firme di riconoscimento vanno configurate regolarmente.

(3) Gli utenti non hanno il permesso di installare o disattivare applicazioni software non autorizzate.

(4) Il sistema prevede un timeout di sessione se l'utente non è attivo per un determinato periodo di tempo.

(5) Gli aggiornamenti di sicurezza critici rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente.

2.4 Sicurezza della rete/comunicazione

(a) Per ogni accesso tramite Internet, le comunicazioni sono crittografate utilizzando protocolli crittografici.

(b) Il traffico da e verso il sistema informatico è monitorato e controllato da firewall e sistemi di rilevamento delle intrusioni.

2.5 Backup

(a) Le procedure di backup e ripristino dei dati sono definite, documentate e chiaramente associate a ruoli e responsabilità.

(b) I backup sono adeguatamente protetti dal punto di vista fisico e ambientale in base agli standard validi per i dati originali.

(c) L'esecuzione dei backup viene controllata per verificarne la completezza.

(d) La strategia di backup dei sistemi è stabilita dal cliente ed esula dal controllo dell'addetto al trattamento dei dati.

2.6 Dispositivi mobili/portatili

(a) Le procedure per la gestione dei dispositivi mobili e portatili sono stabilite e documentate con regole chiare per il loro corretto utilizzo.

(b) I dispositivi mobili a cui è consentito l'accesso al sistema informatico vengono precedentemente registrati e autorizzati.

(c) La gestione e l'autenticazione risp. l'accesso tramite dispositivi mobili sono garantiti dal cliente.

2.7 Sicurezza nel ciclo di vita delle applicazioni

Durante il ciclo di sviluppo si seguono le migliori pratiche, lo stato della tecnica e procedure o standard di sviluppo sicuri e riconosciuti.

2.8 Cancellazione/eliminazione dei dati

(a) Prima dello smaltimento, i supporti dati vanno sovrascritti tramite software. Nei casi in cui ciò non sia possibile (CD, DVD ecc.) vanno distrutti fisicamente.

(b) I supporti dati cartacei e portatili su cui sono memorizzati i dati personali vanno distrutti.

2.9 Sicurezza fisica

(a) L'ambiente fisico dell'infrastruttura del sistema IT è accessibile solo a personale autorizzato. Le aree di sicurezza e i relativi punti di accesso devono essere protetti da accessi non autorizzati mediante adeguate misure tecniche (ad esempio sistema antieffrazione, tornello controllato da carta con chip, sistema di accesso di sicurezza per una persona, impianto di chiusura) o misure organizzative (ad esempio servizio di sorveglianza).

(b) La sicurezza fisica dell'infrastruttura del sistema IT è garantita dal cliente ed esula dal controllo dell'addetto al trattamento dei dati.