Allegato alla convenzione in merito al trattamento dei dati su commissione

Elementi dei dati utilizzati, misure tecniche e organizzative (TOM)

1 Elementi dei dati utilizzati

1.1 Generale

Il cliente affida a Swisscom nell'ambito dei contratti a propria discrezione e nel suo incarico i dati personali e/o dati vincolati dal segreto ai fini del trattamento dati.

1.2 Persone interessate

In tal caso può trattarsi di dati personali, in particolare dei seguenti gruppi interessati:

- potenziali clienti, clienti, partner commerciali, venditori e commercianti del cliente - quali persone fisiche;
- collaboratori o altre persone ausiliari di potenziali clienti, clienti, partner commer-ciali, venditori e commercianti;
- collaboratori o altre persone ausiliari, autorizzate dal cliente ad utilizzare i servizi

1.3 Tipo di dati personali

In tal caso può trattarsi in particolare dei seguenti tipi di dati personali:

- informazioni personali come nome, cognome, data di nascita, età, sesso, nazionalità, ecc.;
- dati di contatto commerciali come indirizzo e-mail, numero di telefono, indirizzo;
- dati di contatto privati come indirizzo e-mail, numero di telefono, indirizzo;
- dettagli di documenti d'identità;
- informazioni in merito alla vita professionale come designazione del posto, funzione, ecc.;
- informazioni in merito alla vita privata come stato di famiglia, hobby, ecc.;
- informazioni utente come dati del login, numero di cliente, numero personale, comportamento dell'utente, ecc.;
- informazioni tecniche come indirizzo IP, informazioni riguardo ai dispositivi, ecc.

1.4 Dati personali degni di particolare protezione

Queste categorie di dati sono dati personali che rivelano l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici e dati biometrici intesi a identificare in modo univo-co una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale.

1.5 Dati vincolati dal segreto

Può ad esempio trattarsi di dati soggetti al segre-to professionale, al segreto bancario, al segreto d'ufficio o all'obbligo di segretezza ai sensi della legislazione in materia di assicurazioni sociali.

1.6 Delimitazioni

[1] Se questi dati sono stati criptati dal cliente e dunque non sono accessibili a Swisscom, non si tratta di un trattamento dei dati su commissione di Swisscom. Quindi, la Convenzione in merito al trattamento dei dati su commissione non è ap-plicabile per questi dati.

[2] Il giudizio, se le misure tecniche e organizzative descritte in seguito per la protezione dei dati affidati a Swisscom per il trattamento (soprattutto dati personali degni di particolare protezione o dati vincolati dal segreto) sono adeguati, spetta esclusivamente al cliente.

[3] Ogni parte tratta nel quadro del rapporto contrattuale i dati personali sui collaboratori o altre persone ausiliari dell'altra parte.Questi includono, ad esempio, nome, indirizzo postale / e-mail / indirizzo IP, numero di telefono, professione / funzione, mezzi di identificazione, copie di carte d'identità, ecc. Ai fini dell'esecuzione del contratto e del mantenimento del rapporto contrattuale (ad esempio comunicazione, controllo d'entrata e d'accesso, segnalazioni di guasti, ordinazioni, fatturazioni, analisi di gradimento, informazioni su nuovi prodotti, inviti ad eventi, ecc.), le parti trattano questi dati personali sotto la responsabilità congiunta sui propri sistemi e utilizzando misure tecniche e organizzative adeguate per proteggere i dati. Questo tipo di trattamento dei dati non è soggetto alle disposizioni per il trattamento dei dati su commissione, tuttavia Swisscom adotta conforme al senso le seguenti misure tecniche e organizzative per proteggere questi dati.

2 Misure tecniche e organizzative

I seguenti capitoli descrivono le misure adottate da Swisscom per quanto riguarda la protezione dei dati personali nell'ambito dell'elaborazione dei dati dell'ordine. Swisscom mantiene un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conformemente allo standard ISO 270001:2013. Il SGSI di Swisscom è certificato; il certificato è consultabile pubblicamente sul sito internet di Swisscom (https://www.swisscom.ch/it/about/azienda/ritratto/rete/sicurezza.html).
Le misure elencate di seguito sono da intendersi come generiche e si applicano di volta in volta se nel contratto non è sancito niente in contrario, ad es. se sono stabilite ulteriori misure specifiche per il prodotto o il cliente oppure se certe delle misure seguenti sono esplicitamente escluse. Le seguenti misure si applicano nei casi in cui Swisscom stessa tratta i dati rilevanti. Qualora l'elaborazione dei dati viene effettuata da terzi su incarico di Swisscom, quest'ultima si impegna tramite accordi contrattuali adeguati affinché i terzi rispettino misure paragonabili.

2.1 Controllo degli accessi

[1] Swisscom suddivide le aree in zone di sicurezza protette da diversi livelli di sicurezza. Queste zone si suddividono in zone pubbliche, sicure e altamente sicure. Le zone pubbliche sono accessibili a chiunque, come ad es. gli Swisscom shop o locali adibiti alla ricezione in uno stabile di uffici. Per accedere nelle zone protette è necessario un badge o una chiave. I badge dei collaboratori e dei fornitori di servizi sono personalizzati. La consegna di chiavi a persone interessate viene verbalizzata. I visitatori devono registrarsi e vengono accompagnati nelle zone sicure dai collaboratori responsabili. Qualora si utilzzano badges non personalizzati, viene nominato un responsabile per verbalizzare i possessori temporanei.

[2] I centri di calcolo di Swisscom sono classificati come zone altamente sicure. Non vi è alcun accesso diretto dalle zone pubbliche a zone altamente sicure, vi si accede solo tramite una zona sicura. L'ingresso nella zona altamente sicura richiede un'identificazione a due fattori e viene verbalizzato. I centri di calcolo sono di proprietà di Swisscom o locati da terzi a lungo termine.

[3] I centri di calcolo di Swisscom dispongono di necessarie misure di protezione fisiche per individuare anticipatamente una violazione del perimetro dell'edificio ed attivare un relativo allarme. Nel caso di edifici occupati 24 ore su 24, i collaboratori responsabili della sicurezza sono adeguatamente formati per trattare tali allarmi rapidamente e professionalmente e per prendere le relative misure. Per edifici non occupati 24 ore su 24, gli allarmi sono trasmessi ad un fornitore di servizi di sicurezza o alla polizia per attivare un intervento.

[4] I centri di calcolo di Swisscom dispongono di ulteriori misure di sicurezza necessarie per ridurre il più possibile i rischi causati da eventi naturali quali fulmini, pioggia, inondazioni ecc., in modo che essi non siano più di rilievo per l'esercizio del centro di calcolo.

[5] Qualora siano utilizzati centri di calcolo di terzi per servizi di Swisscom con memorizzazione permanente di dati, Swisscom garantisce che i gestori di tali centri di calcolo adempiano a condizioni paragonabili a quelle dei centri di calcolo di Swisscom e dunque a un livello di sicurezza equivalente.

[6] Qualora il cliente memorizzi i propri dati presso di sé in loco, Swisscom può fornire suggerimenti per la protezione di questi locali. È responsabilità del cliente adottare le necessarie misure di protezione.

2.2 Controllo degli accessi al sistema

[1] L'accesso ai sistemi di Swisscom avviene sempre con identificazioni personalizzate delle persone incaricate da Swisscom.

[2] L'accesso ai sistemi è sempre protetto perlomeno con una password o da un elemento di autenticazione equivalente e dalla relativa identificazione digitale. I dati d'accesso sono memorizzati in maniera tale, che non sia possibile risalire in alcun modo direttamente al dato di autenticazione valido, nel caso in cui questi dati divenissero accessibili.

[3] Le password devono adempiere a requisiti complessi ed essere composte da almeno tre classi dei seguenti elementi: lettere maiuscole, lettere minuscole, numeri, caratteri speciali. Le password di conti personali non vengono mai rese accessibili a terzi.

[4] In caso di login errato, l'identificazione viene bloccata, dapprima temporaneamente e dopo ulteriori tentativi errati, permanentemente. Uno sblocco è in seguito possibile solo con l'aiuto del Service Desk di Swisscom. In tal caso viene utilizzato il Mobile ID per l'identificazione dell'utente.

[5] Qualora l'utente necessiti di diritti d'amministratore con un'identità impersonale, esso deve eseguire una procedura "step up": il collaboratore effettua il login al sistema con il proprio account personale e successivamente amplia i propri diritti sul sistema. Sui sistemi Unix ciò avviene ad esempio utilizzando l'ordine sudo. Qualora non sia possibile una procedura "step up", Swisscom può accertare in qualsiasi momento, tramite la piattaforma amministrativa, quale utente ha utilizzato l'identità impersonale dell'amministratore. Tutti gli accessi amministrativi effettuano il login in maniera centralizzata presso Swisscom e vengono memorizzati per un periodo di tempo definito.

[6] Portali accessibili tramite internet richiedono, a secondo della classificazione degli utilizzatori, una forte autenticazione al momento dell'accesso ai dati rilevanti. L'autenticazione forte si basa sul Mobile ID, sull'utilizzo di un token elettronico per la generazione di password monouso o su altri mezzi sicuri quale secondo fattore.

[7] Il Mobile ID è un servizio di Swisscom basato sulla carta SIM adeguata specificatamente per Swisscom con un modulo di sicurezza per telefoni cellulari e costituisce dunque un'identificazione sicura dell'utente.

[8] I dispositivi aventi un accesso diretto alla rete aziendale sono identificati tramite un certificato leggibile a macchina. I collaboratori che utilizzano il loro dispositivo personale devono connettersi tramite un'infrastruttura virtuale per accedere ai dati rilevanti dei clienti.

2.3 Controllo degli accessi ai dati

[1] Le autorizzazioni sui sistemi sono strutturate per ruoli. A un'identità sono attribuiti uno o più ruoli necessari per l'esecuzione dei ruoli organizzativi della persona. I ruoli sono strutturati in maniera tale da accedere solo ai dati necessari per l'adempimento del compito.

[2] La descrizione dei ruoli e delle loro autorizzazioni sono documentate in concetti relativi ai ruoli. Questi concetti vengono regolarmente verificati e aggiornati. Il concetto del ruolo viene tenuto e aggiornato dal responsabile del sistema. Per tutti i ruoli viene regolarmente verificato se gli utenti associati hanno tuttora bisogno di questo ruolo.

[3] Qualora un collaboratore necessiti di diritti supplementari, esso può ordinare un ruolo supplementare. L'attivazione di questo ruolo supplementare è autorizzata dal superiore e dal possessore del ruolo. Il proprietario del ruolo può decidere se questa attivazione è effettivamente necessaria, o se può essere effettuata un'attivazione automatica. Al collaboratore viene attribuito automaticamente un numero molto limitato di ruoli; in questo contesto si tratta di ruoli risultanti dalla struttura organizzativa, come ad es. l'appartenenza a un'unità organizzativa.

[4] L'accesso con diritti superiori per la gestione dei sistemi di Swisscom avviene sempre tramite un'infrastruttura dedicata con un'autenticazione più forte. Tutti gli accessi, le disconnessioni e gli accessi errati sono verbalizzati in maniera centralizzata e memorizzati per un certo lasso di tempo. L'autenticazione forte si basa in questo contesto sul Mobile ID o sull'utilizzo di un token elettronico per la generazione di password monouso.

[5] Il traffico dati tra la rete del cliente e Swisscom è, se possibile, criptato o viene protetto da misure alternative. Misure alternative possono essere ad es. l'utilizzo di canali logici dedicati o l'utilizzo di connessioni in fibra ottica dirette. Il criptaggio della connessione si basa su protocolli e meccanismi di protezione attuali.

[6] Gli accessi ai sistemi sono verbalizzati in maniera centralizzata e analizzati con diverse procedure, nonché verificati dal punto di vista delle violazioni della sicurezza delle informazioni. Violazioni così constatate vengono analizzate da un team centrale e vengono adottate le relative misure.

2.4 Controllo del trasferimento

[1] L'accesso a dati rilevanti tramite internet avviene sempre mediante una connessione criptata. Swisscom utilizza protocolli e meccanismi di protezione attuali. Questa connessione criptata si basa su tecnologie a livello di rete, di sessione o di applicazione.

[2] L'accesso diretto del cliente ai propri dati personali viene protetto, in accordo con il cliente, durante il trasferimento. A questo scopo Swisscom offre relativi servizi che permettono connessioni di rete al cliente virtuali. Inoltre, per queste connessioni possono essere impiegate anche ulteriori tecniche di criptaggio.

[3] Per impedire la fuga di dati, Swisscom ha introdotto misure di protezione presso le interfacce tra e-mail e web, verificando così se dati personali sono trasferiti in grandi quantità, rappresentando dunque una possibilità di fuga di dati verso l'internet.

2.5 Controllo delle memorie

[1] Le memorie permanenti nei centri di calcolo sono protette con misure fisiche di protezione contro le perdite. Esse comprendono alimentazioni elettriche ridondanti ed i necessari sistemi per permettere un esercizio autosufficiente per un certo lasso di tempo.

[2] Per la protezione da danni da fumo o incendio, i locali altamente sicuri dispongono di impianti di allarme per fumo e incendi. Per un primo intervento viene impiegato il personale preposto alla sicurezza presente rispettivamente il personale dell'edificio, oppure viene attivato un impianto di spegnimento per ridurre al minimo il danno potenziale. Qualora non sia presente personale in loco, l'allarme viene trasmesso ai vigili del fuoco locali.

[3] In caso di difetto, i supporti dati vengono resi fisicamente inutilizzabili da Swisscom al fine di escludere completamente un possibile accesso agli stessi.

[4] I supporti dati funzionanti vengono cancellati con procedure di cancellazione standard del settore, ciò rende praticamente impossibile una ricostruzione dei dati contenuti dagli stessi. Qualora un procedimento di questo genere non sia possibile, i supporti dati vengono resi fisicamente inutilizzabili, rispettivamente distrutti.

[5] Una restituzione dei supporti dati al cliente è possibile a determinate condizioni. Questo impone che il sistema di memorizzatione, rispettivamente il supporto dati sia stato impiegato solo per questo singolo cliente. In questo caso Swisscom dispone di un processo definito per effettuare una consegna verbalizzata dei supporti dati in un edificio di Swisscom.

2.6 Controllo d'immissione

[1] Nel caso in cui Swisscom sia responsabile per l'immissione ed il trattamento dei dati personali, essa assicura con le necessarie misure tecniche e organizzative che questi dati siano registrati e trattati correttamente. Con l'impiego di misure tecniche viene accertata la validità dei dati, ad es. viene verificata la presenza di un riferimento della persona in un ulteriore sistema rilevante. Misure organizzative per la verifica della correttezza sono ad es. un controllo successivo delle immissioni e degli adeguamenti, o una verifica a campione della correttezza dei dati.

[2] Swisscom registra ulteriori dati personali del cliente nei propri sistemi per la prestazione dei servizi. Questi sistemi servono ad es. alla registrazione di notifiche di errore (incident), alla registrazione di modifiche desiderate o alla fatturazione. Swisscom garantisce tramite adeguate misure di qualità che i dati rilevanti registrati in questo contesto vengano verificati e corretti.

2.7 Controllo dei mandati

[1] Swisscom seleziona accuratamente i possibili subfornitori con accesso a dati e impone le rile-vanti responsabilità di protezione dei dati ai fornitori.

[2] Swisscom ha nominato un'organizzazione responsabile per garantire i requisiti di protezione dei dati. Essa è raggiungibile all'indirizzo datenschutz@swisscom.com per domande. Il primo punto di contatto per domande in merito alla protezione dei dati presso Swisscom è l'Account Manager di Swisscom.

[3] I nuovi collaboratori di Swisscom vengono sottoposti a una verifica della sicurezza prima dell'inizio del loro impiego. Essa considera vari livelli ed è strutturata in maniera differente a seconda delle possibilità di accesso ai dati rilevanti. Il controllo comprende al minimo la verifica dell'intero curriculum vitae, degli ultimi attestati e la richiesta di una referenza personale.
Negli ulteriori livelli si aggiungono la sottoscrizione di una dichiarazione di riservatezza, nonché la verifica di un estratto attuale del casellario giudiziario e un estratto attuale del registro esecuzioni e fallimenti.

[4] All'inizio del loro lavoro i nuovi collaboratori si familiarizzano con le disposizioni rilevanti per la loro sicurezza e la sicurezza dei dati. Ciò avviene tramite un Awareness Training basato sulla piattaforma elettronica di apprendimento di Swisscom. Nel caso di una mancata partecipazione viene effettuato un richiamo dal diretto superiore del collaboratore.

[5] I collaboratori esistenti di Swisscom sono regolarmente istruiti sull'uso accurato di dati. A tal fine vengono impiegati comunicazioni in intranet, contributi blog, formazioni di Awareness online sulla piattaforma di apprendimento di Swisscom, nonché formazioni sul posto.

[6] Se il collaboratore di Swisscom lascia l'azienda, viene bloccata automaticamente l'identità principale sui sistemi di Swisscom. L'ingresso negli edifici viene altresì bloccato alla fine dell'ultimo giorno di lavoro. È compito del superiore di cancellare tutti gli ulteriori accessi e di ritirare il badge ed i dispositivi di lavoro di Swisscom l'ultimo giorno di lavoro del collaboratore.

2.8 Controllo della disponibilità

[1] Swisscom memorizza i dati nei centri di calcolo con il necessario livello di protezione conformemente all'accordo contrattuale. Può trattarsi di centri di calcolo di Swisscom o di terzi (si veda 2.2).

[2] Per garantire la disponibilità dei dati, i sistemi di memorizzazione di Swisscom sono configurati in modo tale che può venire a mancare anche più di una componente, mentre i dati sono tuttora disponibili. Ciò viene realizzato tramite supporti dati divisi e ridondanti, nonché reti e alimentazioni elettriche ridondanti.

[3] Swisscom salvaguarda i dati conformemente alla descrizione delle prestazioni. In proposito, il salvataggio avviene sempre su sistemi hard disk in un ulteriore centro di calcolo, con una sufficiente distanza geografica tra i due posti. I locali in posizioni geografiche diverse servono a circoscrivere possibilmente a un posto possibili danni causati da eventi naturali come fulmini, pioggia, inondazioni o frane.

[4] A seconda delle prestazioni ricevute, il cliente può ordinare in aggiunta diversi livelli di protezione dei dati. Ciò risulta dalla descrizione delle prestazioni o può essere richiesto all'Account Manager di Swisscom.

[5] Swisscom ha sviluppato un framework basato su suggerimenti dei produttori, nonché di fonti esterne per rafforzare i propri sistemi. Questo framework descrive in dettaglio quali misure devono essere implementate per i vari sistemi. L'implementazione viene regolarmente verificata e comunicata tramite rapporti in maniera centralizzata. Le unità aziendali responsabili possono consultare i risultati della verifica in ogni momento ed effettuare le necessarie correzioni sulla base degli stessi. Un rendiconto mensile delle verifiche viene inviata alle unità aziendali rilevanti.

[6] Swisscom ha implementato i processi necessari per identificare le segnalazioni in merito ai punti deboli dei software e dei patch, per valutarle e trarne ulteriori provvedimenti necessari. Il processo standard di patch management garantisce che gli avvisi di patch relativi ai sistemi siano valutati e, dopo una verifica, installati sui sistemi rilevanti. L'installazione di patch necessita eventualmente di una collaborazione e un'attivazione da parte del cliente. Ciò è tenuto in considerazione nei processi standardizzati di Swisscom. Qualora un patch debba essere installato urgentemente, vi è, a seconda del servizio, un cosiddetto processo di emercency patch.

2.9 Obbligo di separazione

[1] Swisscom assicura che i dati dei clienti non siano consultabili reciprocamente. A questo proposito sono impiegate procedure di sicurezza assicurando la separazione dei dati dei clienti a livello logico o fisico.

[2] Procedure fisiche sono applicate se il servizio ed i sistemi associati impiegati non permettono un'adeguata separazione logica., Dove possibile, Swisscom tenta di impiegare sempre procedure logiche per motivi di costi.

[3] A seconda del servizio offerto, il cliente può fare richiesta di propria iniziativa che i suoi dati siano separati fisicamente da quelli di altri clienti. Quest'opzione non è disponibile per tutte le offerte.

[4] Swisscom ha verificato che le procedure logiche non possano essere aggirate. Qualora Swisscom constatasse che ciò non è più garantito dalle procedure, essa adotterà le necessarie contromisure per ripristinare una protezione equivalente.

2.10 Verifica, analisi e valutazione

[1] Swisscom effettua regolarmente audit dei sistemi. Nell'ambito tecnico ciò consiste in una verifica regolare che le misure di protezione di base siano implementate e rispettate sui sistemi conformemente ai requisiti di Group Security.

[2] Sulla base di un'analisi dei rischi, nuove prestazioni e nuovi servizi sono sottoposti ad una verifica tecnica. I difetti constatati sono eliminati dai responsabili di Swisscom. A seconda delle gravità dei difetti, viene effettuata una verifica integrativa per dimostrare l'efficienza dell'eliminazione.

[3] Nell'ambito dei processi l'ufficio interno di audit effettua le verifiche secondo un piano basato sui rischi. Le verifiche possono essere effettuate in qualsiasi momento anche ad hoc dall'ufficio interno di audit o su richiesta del consiglio di amministrazione di Swisscom. I difetti constatati sono eliminati entro il limite di tempo definito e, a seconda della gravità, verificati di nuovo dall'ufficio interno di audit.

[4] Group Security mantiene un sistema di gestione dei rischi su tutta l'azienda per individuare rischi alla sicurezza delle informazioni, quantificarli e introdurre, congiuntamente alle organizzazioni responsabili, misure per la riduzione dei rischi. Group Security assicura in proposito che i rischi alla sicurezza delle informazioni siano comunicati e assunti al livello appropriato. Group Security assicura altresì che tutte le funzioni di gestione del rischio rilevanti si scambino informazioni in merito ai rischi constatati e, se sensato, stabiliscano congiuntamente le misure.

[5] Group Security è responsabile per Swisscom di un programma di bug bounty. Esso permette a chiunque di segnalare in maniera centralizzata le lacune alla sicurezza individuate nelle prestazioni di Swisscom. Le segnalazioni vengono valutate e le necessarie contromisure adottate, ad es. l'esecuzione di un patch per un software o il miglioramento di un codice di una pagina internet. In conclusione, la segnalazione di vulnerabilità viene pubblicata dal segnalatore e questi viene indennizzato a seconda della gravità della lacuna.

[6] Group Security impiega un "Red team". Il "Red team" attacca le infrastrutture di Swisscom e verifica in tal modo l'efficacia delle misure di sicurezza adottate. Gli attacchi avvengono all'insaputa dei collaboratori di Swisscom responsabili per i sistemi e permettono così una verifica in base alle condizioni di reali di un attacco. Gli attacchi sono ripetuti sino a quando non vi è un possibile accesso ai dati o al sistema preso di mira. Successivamente, l'attacco viene fermato e documentato. La sicurezza dei dati è garantita in ogni momento. Con questi interventi Swisscom assicura test complessivi a tutta l'infrastruttura. Dai risultati vengono tratte misure per il miglioramento del livello di sicurezza presso Swisscom.

[7] L'organizzazione di protezione dei dati di Swisscom mantiene un sistema di gestione del rischio per individuare i rischi alla protezione dei dati di Swisscom, per documentarli e per garantire un relativo trattamento dei rischi individuati. L'organizzazione di protezione dei dati garantisce in questo contesto che vi sia una comunicazione e attribuzione al livello appropriato della responsabilità per i rischi alla protezione dei dati. L'organizzazione di protezione dei dati è in proposito in continuo contatto con altre funzioni di gestione del rischio di Swisscom.