Elementi dei dati utilizzati e misure tecniche e organizzative (MTO)

1 Elementi dei dati utilizzati

1.1 Cenni generali

Il cliente affida a Swisscom Broadcast SA (di seguito «Swisscom») dati personali e/o dati con vincolo di segretezza ai fini del trattamento degli stessi nell'ambito dei contratti stipulati a propria discrezione e per proprio conto.

1.2 Persone interessate

I dati possono essere dati personali, riferiti in particolare alle seguenti persone interessate:

- Clienti esistenti o potenziali, partner commerciali, venditori e rivenditori del cliente quali persone fisiche
- Collaboratori o altro personale ausiliario di clienti esistenti o potenziali, partner commerciali, venditori e rivenditori
- Collaboratori o altro personale ausiliario del cliente autorizzati da quest'ultimo ad utilizzare i servizi

1.3 Tipologie di dati personali

I dati personali possono rientrare in particolare nelle seguenti tipologie:

- Informazioni personali come nome, cognome, data di nascita, età, sesso, nazionalità ecc.
- Dati di contatto aziendali come indirizzo e-mail, numero di telefono, indirizzo
- Dati di contatto privati come indirizzo e-mail, numero di telefono, indirizzo
- Dettagli dei documenti d'identità
- Informazioni in merito alla carriera professionale come denominazione dell'incarico ricoperto, funzione ecc.
- Informazioni in merito alla vita privata come stato di famiglia, hobby ecc.
- Informazioni utente come credenziali di accesso, numero cliente, numero personale, comportamento dell'utente ecc.
- Informazioni tecniche come indirizzo IP, informazioni sugli apparecchi ecc.

1.4 Dati personali degni di particolare protezione

Queste categorie di dati includono dati personali in base ai quali è possibile individuare l'origine razziale ed etnica, le opinioni politiche, le convinzioni etico-religiose o l'affiliazione sindacale, nonché dati genetici e dati biometrici finalizzati a identificare in modo univoco una persona fisica, così come dati relativi alla salute o alla vita sessuale o all'orientamento sessuale.

1.5 Dati con vincolo di segretezza

In questa tipologia possono rientrare ad es. dati soggetti al segreto professionale, al segreto bancario, al segreto d'ufficio o all'obbligo di riservatezza ai sensi delle normative in materia di assicurazioni sociali.

2 Misure tecniche e organizzative

2.1 Aspetti generali

1 Le seguenti sezioni descrivono le misure tecniche e organizzative adottate da Swisscom per quanto riguarda la protezione dei dati personali nell'ambito del trattamento dei dati su commissione. È unicamente il cliente a dover valutare l'adeguatezza delle misure tecniche e organizzative descritte in seguito per la protezione dei dati affidati a Swisscom ai fini del trattamento degli stessi (segnatamente in caso di dati personali degni di particolare protezione o di dati con vincolo di segretezza).

2 Swisscom impiega un Information Security Management System (ISMS) conforme alla norma ISO 27001 e ad altre norme internazionali.

3 Le misure di seguito elencate sono da intendersi come generiche e troveranno applicazione ogniqualvolta il contratto non preveda altrimenti, ossia in assenza ad esempio di ulteriori misure specifiche per il rispettivo prodotto o cliente o di una clausola che escluda espressamente l'applicazione di alcune delle misure di seguito elencate. Le seguenti misure sono applicabili nei casi in cui il trattamento dei dati rilevanti è eseguito da Swisscom stessa. Quando il trattamento dei dati viene eseguito da terzi su incarico di Swisscom, quest'ultima stipula accordi contrattuali idonei per garantire il rispetto di misure equivalenti da parte di detti terzi.

2.2 Controllo degli accessi

1 Swisscom suddivide le aree in diverse zone caratterizzate da diversi livelli di sicurezza. Sono previste zone pubbliche, zone sicure e zone altamente sicure. Le zone pubbliche sono accessibili a chiunque. Rientrano in tali zone ad es. i locali adibiti a reception in un complesso di uffici. Per accedere alle zone protette occorre essere muniti di un badge o di una chiave. I badge dei collaboratori e dei fornitori di servizi sono personali. La consegna delle chiavi alle persone autorizzate viene annotata in un registro. I visitatori devono registrarsi e vengono accompagnati nelle zone sicure dal personale incaricato. In caso di utilizzo di badge non personali, viene nominato un responsabile che registra le attività della persona temporaneamente in possesso del badge.

2 I centri di calcolo di Swisscom sono classificati come zone altamente sicure. Le zone altamente sicure non sono mai direttamente accessibili dalle zone pubbliche, ma unicamente dalle zone sicure. L'ingresso in una zona altamente sicura richiede un'identificazione a due fattori e viene registrato. I centri di calcolo sono di proprietà di Swisscom o vincolati da contratti di locazione pluriennali con terzi.

3 I centri di calcolo Swisscom sono muniti dei necessari sistemi di protezione fisica per individuare tempestivamente eventuali tentativi di intrusione nel perimetro dell'edificio ed attivare il relativo allarme. Nel caso di edifici presidiati da personale 24 ore su 24, i collaboratori responsabili della sicurezza sono adeguatamente formati per poter reagire in modo rapido e professionale a tali allarmi e intervenire di conseguenza. Negli edifici non presidiati da personale 24 ore su 24, gli allarmi sono trasmessi ad un fornitore di servizi di sicurezza o alla polizia per consentire un intervento.

4 I centri di calcolo Swisscom dispongono anche dei sistemi di sicurezza necessari per ridurre il più possibile i rischi causati da eventi naturali quali fulmini, pioggia o inondazioni ed evitare così il più possibile eventuali ripercussioni sul corretto funzionamento dei centri stessi.

5 Se per i servizi Swisscom sono utilizzati centri di calcolo di terzi con memorizzazione permanente di dati, Swisscom garantisce il rispetto da parte dei rispettivi gestori di requisiti paragonabili a quelli dei centri di calcolo Swisscom e dunque di un livello di sicurezza equivalente.

6 Qualora il cliente memorizzi i propri dati in loco, Swisscom potrà consigliare misure idonee per la protezione dei locali interessati. È responsabilità del cliente adottare le necessarie misure di protezione.

2.3 Controllo degli accessi ai sistemi

1 L'accesso ai sistemi Swisscom prevede sempre l'impiego di identificativi personali delle persone incaricate da Swisscom.

2 L'accesso ai sistemi è sempre protetto perlomeno con una password o con un elemento di autenticazione equivalente, in combinazione con la relativa identificazione digitale. Le credenziali di accesso sono memorizzate in maniera tale da impedire a chiunque dovesse entrare in loro possesso di risalire direttamente all'elemento di autenticazione richiesto.

3 Le password devono soddisfare determinati criteri di complessità ed essere composte da almeno tre classi dei seguenti elementi: lettere maiuscole, lettere minuscole, numeri e caratteri speciali. Le password degli account personali non vengono mai rese accessibili a terzi.

4 In caso di inserimento di credenziali errate, l'accesso viene bloccato dapprima temporaneamente e in seguito permanentemente, qualora l'utente provi ad accedere più volte.

5 A seconda della classificazione degli utenti, i portali accessibili tramite internet possono richiedere un'autenticazione forte al momento dell'accesso ai dati rilevanti. L'autenticazione forte si basa sul Mobile ID e sull'utilizzo di un token elettronico per la generazione di una password one-time o di altri strumenti sicuri quale secondo fattore.

2.4 Controllo degli accessi ai dati

1 Le autorizzazioni all'interno dei sistemi sono strutturate per ruoli. A una data identità sono attribuiti uno o più ruoli necessari per lo svolgimento dei ruoli organizzativi della rispettiva persona. I ruoli sono strutturati in maniera tale da consentire unicamente l'accesso ai dati necessari per lo svolgimento del compito richiesto. La descrizione dei ruoli e delle rispettive autorizzazioni è documentata in appositi concetti.

2 Se un collaboratore necessita di diritti supplementari, può richiedere l'assegnazione di un ruolo aggiuntivo. L'abilitazione di tale ruolo aggiuntivo è autorizzata dal superiore e dal titolare del ruolo. Quest'ultimo può decidere se tale abilitazione è effettivamente necessaria, oppure se può essere gestita in automatico. Ai collaboratori viene assegnato automaticamente un numero molto limitato di ruoli, che sono legati alla struttura organizzativa. Tali ruoli possono includere ad es. l'appartenenza a una determinata unità organizzativa.

3 Il traffico dati tra la rete del cliente e Swisscom viene se possibile cifrato oppure protetto mediante misure alternative, tra cui ad es. l'utilizzo di canali logici dedicati o di connessioni in fibra ottica dirette. Per la cifratura della connessione vengono impiegati protocolli e meccanismi di protezione aggiornati.

4 Gli accessi ai sistemi sono registrati e possono essere analizzati mediante diversi procedimenti.

2.5 Controllo del trasferimento

1 L'accesso a dati rilevanti tramite internet prevede sempre l'uso di una connessione cifrata. Swisscom utilizza a tal fine protocolli e meccanismi di protezione aggiornati. Per la cifratura della connessione vengono impiegate apposite tecnologie a livello di rete, di sessione o di applicazione.

2 Previo accordo con il cliente, in caso di accesso diretto di quest'ultimo ai propri dati personali viene garantita la protezione dei dati in fase di trasferimento. A tal riguardo Swisscom offre servizi che permettono connessioni di rete virtuali con il cliente. Per queste connessioni possono inoltre essere impiegate tecniche di cifratura ulteriori.

2.6 Controllo delle memorie

1 Le memorie permanenti nei centri di calcolo sono protette con sistemi fisici contro la perdita di dati. Tali accorgimenti comprendono alimentazioni elettriche ridondanti e i sistemi necessari per consentire un determinato periodo di autonomia.

2 Per la protezione contro i danni da fumo o incendi, i locali altamente sicuri dispongono di rilevatori di fumo e di incendi. Il primo intervento è di competenza del personale preposto alla sicurezza o comunque presente nell'edificio. In alternativa viene attivato un impianto antincendio per ridurre al minimo i potenziali danni. Se non è presente personale in loco, l'allarme viene trasmesso ai pompieri locali.

3 I supporti dati difettosi vengono resi fisicamente inutilizzabili da Swisscom al fine di escludere qualsiasi possibilità di accesso ai dati.

4 I dati presenti nei supporti dati funzionanti vengono cancellati con procedure standard del settore, al fine di rendere essenzialmente impossibile il ripristino degli stessi. Se tale procedimento non è possibile, i supporti dati vengono resi fisicamente inutilizzabili ovvero distrutti.

5 La restituzione dei supporti dati al cliente è possibile a determinate condizioni, e unicamente se il sistema di memorizzazione ovvero il supporto dati è stato impiegato unicamente per lo specifico cliente in questione.

2.7 Controllo dell'inserimento dei dati

1 Se l'inserimento e il trattamento dei dati personali sono di competenza di Swisscom, quest'ultima adotta le misure necessarie per garantire che i dati siano registrati e trattati correttamente.

2 Swisscom registra ulteriori dati personali del cliente nei propri sistemi per la fornitura dei servizi. Tali sistemi servono ad es. alla registrazione delle notifiche di malfunzionamento (incident) o delle richieste di modifica, oppure ai fini della fatturazione. Swisscom garantisce tramite adeguate misure di controllo qualità che i dati rilevanti in tal modo registrati vengano verificati e all'occorrenza corretti.

2.8 Controllo del personale autorizzato

1 Swisscom seleziona accuratamente i possibili subfornitori con accesso a dati e impone ai fornitori l'osservanza delle relative responsabilità per la protezione dei dati.

2 Swisscom ha nominato un'organizzazione responsabile per la garanzia dei requisiti di protezione dei dati. Tale organizzazione è contattabile all'indirizzo datenschutz.sbc@swisscom.com. Il primo referente cui rivolgersi per eventuali 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 in materia di sicurezza prima del loro impiego. Tale verifica si articola su vari livelli ed è strutturata in maniera differente a seconda delle possibilità di accesso ai dati rilevanti. La procedura comprende come minimo la verifica dell'intero curriculum vitae e degli attestati più recenti, nonché l'ottenimento di una referenza personale.
Come ulteriori livelli di verifica sono previste la sottoscrizione di una dichiarazione di riservatezza o una verifica secondo il controllo di sicurezza relativo alle persone della Confederazione.

4 All'inizio della loro attività lavorativa, i nuovi collaboratori apprendono innanzitutto le disposizioni rilevanti per la sicurezza propria e per la sicurezza dei dati.

5 I collaboratori di Swisscom già in carica vengono regolarmente aggiornati in merito alle corrette modalità di gestione dei dati. Tali aggiornamenti vengono comunicati tramite intranet, blog, iniziative di sensibilizzazione online sulla piattaforma di apprendimento di Swisscom e corsi di formazione in sede.

6 Se un collaboratore Swisscom lascia l'azienda, la sua identità principale nei sistemi Swisscom viene automaticamente bloccata. Al termine dell'ultimo giorno di lavoro viene inoltre bloccato l'accesso alle strutture aziendali. Il responsabile è tenuto a disabilitare tutti gli ulteriori canali di accesso e a ritirare il badge e i dispositivi di lavoro Swisscom, che deve farsi consegnare l'ultimo giorno di lavoro.

2.9 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.

2 Per garantire la disponibilità dei dati, i sistemi di memorizzazione Swisscom sono configurati in modo tale che l'eventuale guasto a uno o più componenti non pregiudichi la disponibilità dei dati richiesti. A tal fine vengono impiegati supporti dati suddivisi e ridondanti, nonché reti e alimentazioni elettriche ridondanti.

3 Swisscom provvede al salvataggio dei dati conformemente alla descrizione del servizio, appoggiandosi all'occorrenza a sistemi di archiviazione disposti in un ulteriore centro di calcolo sufficientemente distante da un punto di vista geografico. Il ricorso a punti geograficamente separati serve a circoscrivere il più possibile localmente i possibili danni causati da eventi naturali quali fulmini, pioggia, inondazioni o frane.

4 A seconda del servizio previsto, il cliente può richiedere a titolo integrativo livelli diversi di backup dei dati. Per informazioni in merito è possibile consultare la descrizione del servizio o rivolgersi all'Account Manager di Swisscom.

5 Swisscom ha implementato i processi necessari per individuare e valutare le segnalazioni in merito ai punti deboli dei software e ai patch, in modo da poter stabilire le necessarie misure da attuare.

2.10 Obbligo di separazione

1 Swisscom adotta misure per garantire che i dati dei clienti non siano reciprocamente consultabili. A tal fine sono impiegate procedure di sicurezza che assicurano la separazione dei dati dei clienti a livello logico o fisico.

2 Le procedure fisiche sono applicate se il servizio e i rispettivi sistemi non permettono un'adeguata separazione logica. Swisscom predilige ogniqualvolta possibile il ricorso a procedure logiche per ragioni economiche.

3 A seconda del servizio offerto, il cliente può chiedere che i suoi dati siano separati fisicamente da quelli di altri clienti. Non tutte le offerte consentono questa opzione.

4 Swisscom ha verificato le procedure logiche per assicurare che non possano essere aggirate. Se ciononostante dovesse emergere che tali procedure non garantiscono la sicurezza prevista, Swisscom adotterà le necessarie contromisure per ripristinare un grado di protezione equivalente.

2.11 Verifica, analisi e valutazione

1 Swisscom esegue regolarmente audit di sistema. Da un punto di vista tecnico ciò può prevedere ad es. un controllo regolare del perimetro IP o una verifica della sicurezza delle piattaforme.

2 Le nuove prestazioni e i nuovi servizi sono sottoposti a una verifica tecnica in base a un'analisi dei rischi. I difetti riscontrati sono eliminati dagli uffici responsabili. A seconda della gravità dei difetti, può essere eseguita una verifica integrativa per attestare l'efficacia dell'eliminazione degli stessi.

3 Swisscom impiega un sistema di gestione dei rischi esteso all'intera l'azienda per individuare i rischi, quantificarli e introdurre misure per la riduzione degli stessi in collaborazione con le organizzazioni responsabili.

4 Swisscom partecipa a un programma Bug Bounty, che permette a chiunque di segnalare in maniera centralizzata le lacune di sicurezza individuate nei servizi di Swisscom. Le segnalazioni vengono valutate al fine di adottare le necessarie contromisure. Queste possono includere ad es. il rilascio di un patch software o l'ottimizzazione del codice di una pagina web.