Regolamento sull'utilizzo dei sistemi informatici

Migros

Responsabile del documento (Document Owner)	Ruf, Lukas-MGB
Autore del documento	Marques, Raphael-MGB
Versione del documento	V1.2
Data del documento	28.06.2023
Ciclo di revisione	Annuale
Data di entrata in vigore	30.06.2023
Stato	Valida

Cronologia documento

Ver.	Data	Persona	Modifiche
0.1	22.12.2020	Raphael Marques	Documento iniziale basato sul modello
0.2	30.12.2020	Raphael Marques	Ripresa delle informazioni principali dai regolamenti precedenti. Prima bozza
0.3	14.01.2021	Raphael Marques	Revisione Björn Sieger, Dario Quattrocchi
0.4	15.01.2021	Raphael Marques	Aggiunta del capitolo su internet ed e-mail, cleanup per la revisione
0.5	17.02.2021	Raphael Marques	Integrazione serie di revisioni interne CU
0.6	19.03.2021	Raphael Marques	Integrazione revisione stakeholder
0.7	03.05.2021	Raphael Marques	Integrazione feedback dell'Information Security Board
0.8	21.06.2021	Lukas Ruf	Revisione FaKo IT e CT
1.0	28.06.2021	Lukas Ruf	Approvazione successiva a consultazione
1.1	01.10.2021	Dario Quattrocchi	Generalizzazione di alcune parole
1.1	09.01.2022	Lukas Ruf	Rilascio
1.1.1	14.12.2022	Dario Quattrocchi	Aggiunti i capitoli 7.5 e 7.6, adattamento dei link, adattamento e aggiunta 8.1 par. 1
1.1.2	23.01.2023	Lukas Ruf	Revisione v1.2 per tenere conto dei requisiti di sicurezza dei dati secondo la revisione dell’ordinanza sulla protezione dei dati
1.1.3	28.02.2023	Dario Qauttrocchi	Capitolo 7.11 Aggiunta all’inoltro di e-mail a indirizzi e-mail esterni
1.2	08.03.2023	ISB	Integrazione feedback ISB - rilascio
1.2	27.04.2023	Group CISO	Finalizzazione e rilascio CT

Indice

1. Introduzione

La Migros si impegna a creare un ambiente sicuro per i propri collaboratori e collaboratrici, informazioni e valori patrimoniali. Tutte le informazioni provenienti da clienti, partner e terze parti devono essere protette adeguatamente. La Migros punta su standard settoriali e su un approccio basato sul rischio per l'attuazione dei controlli di sicurezza e delle relative misure.

2. Contenuti e obiettivi

L’obiettivo di questo regolamento sull'utilizzo dei sistemi informatici è di definire i principi generali per

- Mantenere la riservatezza, l'integrità e la disponibilità di informazioni e valori patrimoniali;
- proteggere tutti i valori patrimoniali da minacce, interne o esterne, intenzionali o accidentali, sulla base di un approccio basato sul rischio;
- assicurare il rispetto dei requisiti previsti dalla legge, dalle autorità, nonché di natura operativa e contrattuale.

Il regolamento sull'utilizzo dei sistemi informatici è composto da un documento principale e da allegati. I fondamenti vengono definiti nel documento principale. I contenuti del documento principale hanno un impatto diretto sulle azioni delle collaboratrici e dei collaboratori e descrivono ciò che deve essere tenuto presente nell'utilizzo delle risorse informatiche (tutto l'hardware e il software) e dei dati. Temi supplementari, chiarimenti e precisazioni sui fondamenti descritti dal documento principale sono reperibili negli allegati.

Nel regolamento sull'utilizzo dei sistemi informatici il termine «risorse informatiche» comprende tutto l'hardware e tutto il software. Questo include per esempio, laptop e cellulari, ma anche server, dispositivi di rete, router, Office, Word, SAP e tutti i dati in essi memorizzati.

3. Campo di applicazione

In quanto parte della normativa sulla sicurezza, il regolamento sull'utilizzo dei sistemi informatici vale per le collaboratrici e i collaboratori dell'intero Gruppo Migros nel quadro della Governance nazionale della sicurezza delle informazioni, ovvero per tutte le collaboratrici e tutti i collaboratori interni ed esterni di tutte le imprese del Gruppo Migros, fatta eccezione per Banca Migros. Terzi che usufruiscono degli strumenti di lavoro, delle prestazioni e dei servizi messi a disposizione o gestiti da Migros sono a loro volta obbligati a rispettare il regolamento di utilizzo.. Ai fini del presente regolamento sull'utilizzo dei sistemi informatici, per «imprese del Gruppo Migros» si intendono tutte le cooperative Migros e la Federazione delle cooperative Migros, nonché tutte le imprese dalle stesse direttamente o indirettamente controllate, a titolo individuale o congiunto.

La normativa costituisce una raccolta di documenti che definiscono principi, requisiti, procedure e standard vincolanti per la sicurezza delle informazioni. Tutti i documenti pubblicati di tale normativa sono reperibili su security.migros.net.

3.1 Politiche del Gruppo e specifiche alle imprese

Le società all'interno del Gruppo Migros possono rendere più rigoroso e precisare il regolamento sull'utilizzo dei sistemi informatici del Gruppo Migros (in questo contesto denominato anche «Politica del Gruppo») nel quadro di una politica specifica dell'impresa. Se le politiche specifiche delle imprese sono in contrasto con la politica del Gruppo, quest'ultima resta in vigore e avrà un peso maggiore.

3.2 Integrazione nella normativa Migros

Il regolamento sull'utilizzo dei sistemi informatici fa parte della normativa Migros. La normativa Migros è reperibile su security.migros.net. Il regolamento sull'utilizzo dei sistemi informatici è un documento classificato come «Politica».

4. Revisione, aggiornamento e manutenzione

Il regolamento sull'utilizzo dei sistemi informatici viene rivisto almeno una volta all'anno. Secondo il bisogno, può essere modificato dal Group CISO Migros per proteggere la Migros, qualora si identifichino nuovi pericoli o punti deboli oppure cambi il profilo di rischio dell'impresa.

5. Deroghe

In determinate circostanze sono ammesse deroghe al presente regolamento sull'utilizzo dei sistemi informatici, per es. nel caso in cui sia impossibile rispettare le disposizioni a causa di condizioni locali.

6. Applicazione

Nel caso si constati una violazione o un sospetto concreto di violazione contro il presente regolamento sull'utilizzo, possono essere disposte le seguenti misure:

- blocco preventivo dell'accesso agli strumenti di lavoro interessati, per es. blocco del relativo account utente;
- blocco dei dati abusivi e illeciti e loro salvataggio e conservazione a fini probatori;
- cancellazione di dati abusivi e illeciti, qualora necessaria per motivi di sicurezza e sempre che non vi si opponga la necessità di proteggere le prove sotto il profilo giuridico.

Un comportamento della collaboratrice o del collaboratore contrario alla politica o illecito costituisce una violazione degli obblighi del diritto del lavoro e può comportare l'adozione delle misure disciplinari previste da tale diritto (incluso il licenziamento), conseguenze di diritto civile e/o penale nonché pretese di risarcimento danni. Se sussiste un sospetto di reato giustificato (per esempio per pornografia infantile, razzismo, ecc.) può essere presentata denuncia all'autorità competente. Le perdite, i danni e i costi (comprese le spese di accertamento, investigazione, giustizia, patrocinio e sanzione) causati da un comportamento contrario alla politica o illecito possono essere trasferiti e addossati alla collaboratrice o al collaboratore che ha commesso l'errore.

7. Utilizzo delle risorse informatiche Migros

Alle collaboratrici e ai collaboratori vengono messe a disposizione risorse informatiche per uso aziendale. L'utilizzo di queste risorse informatiche rientra fondamentalmente nella responsabilità delle collaboratrici e dei collaboratori, che sono tenuti a utilizzarle in modo sicuro e cauto.

7.1 Pratiche vietate

Sono vietate le seguenti pratiche:

- lasciare la postazione di lavoro senza blocchi o logout dell'utente;
- ogni utilizzo non autorizzato di risorse informatiche, informazioni Migros, informazioni dei clienti e/o dei partner;

- la partecipazione intenzionale o dovuta a negligenza ad attività che mettono in pericolo la sicurezza delle informazioni, le risorse informatiche o le reti della Migros, dei suoi partner o clienti;
- la violazione dei diritti di proprietà intellettuale di una persona o di un'impresa;
- i tentativi non autorizzati di modificare la configurazione di sicurezza di una risorsa informatica Migros o di eludere o disattivare le restrizioni di sicurezza al fine di procurarsi un accesso a informazioni o aree protette;
- l'utilizzo delle risorse informatiche Migros per scaricare, memorizzare, trasmettere o divulgare / distribuire contenuti indecenti. I contenuti indecenti comprendono i materiali pornografici, offensivi, discriminatori, razzisti o diffamatori;
- l'utilizzo di risorse informatiche Migros per creare, scaricare, memorizzare, vendere, distribuire, copiare o scambiare software, informazioni, musica o altri file multimediali illegali, protetti dal diritto di autore o senza licenza;
- la cancellazione o distruzione non autorizzata intenzionale o per negligenza grave di informazioni, comunicazioni o record Migros;
- l'installazione o l'utilizzo di software applicativo o servizi cloud non autorizzati dal Group IT Migros;
- l'utilizzo di qualsiasi tipo di tool, applicazione e dispositivo o exploit (sfruttamento di vulnerabilità) per arrecare danno alla Migros;
- la memorizzazione, l'esecuzione o la diffusione di qualsiasi software maligno;
- l'impiego di account privati su servizi cloud autorizzati (per es. account Microsoft 365 privato).

7.2 Utilizzo privato di risorse informatiche Migros

L'utilizzo privato dei dispositivi delle/degli utenti finali e di comunicazione Migros può essere ristretto. L'utilizzo privato delle risorse informatiche Migros non viene considerato tempo di lavoro.

Per l'utilizzo privato delle risorse informatiche Migros vigono le seguenti restrizioni:

- i file privati non possono essere memorizzati sui sistemi Migros;
- l'utilizzo privato dei dispositivi Migros non può ripercuotersi negativamente sulla produttività della collaboratrice o del collaboratore né sulla disponibilità del sistema;
- all'utilizzo privato di questi dispositivi e tecnologie si applicano le stesse disposizioni previste per l'utilizzo professionale;
- l'utilizzo privato di risorse informatiche Migros che vengono impiegate principalmente per l'elaborazione, l'archiviazione di massa e lo scambio di informazioni e dati Migros (per es. server, componenti di rete, dispositivi IoT) non è consentito.

7.3 Download, installazione e utilizzo di software

Tutti i programmi software e le applicazioni sulle risorse informatiche Migros devono essere acquistati tramite il servizio informatico ufficiale (per es. il Group IT Migros) e provvisti di adeguata licenza per l'utilizzo professionale. È vietato installare o utilizzare software applicativi o servizi cloud che non siano stati approvati dall'IT del Gruppo Migros o dalla rispettiva impresa M.

7.4 Protezione di risorse informatiche Migros

Le collaboratrici e i collaboratori devono proteggere le risorse informatiche Migros contro il furto e il danneggiamento usando la necessaria diligenza (sul posto di lavoro, in viaggio e a casa). Le collaboratrici e i collaboratori devono assicurarsi che lo schermo sia bloccato quando lasciano la postazione di lavoro e che per continuare a lavorare sia necessaria almeno una password. Lo stesso

vale per le risorse informatiche private, se contengono dati aziendali o se questi ultimi possono esserci memorizzati o consultati, vedere in merito anche il capitolo 8.1. La perdita di un dispositivo deve essere immediatamente segnalata al rispettivo service desk (per la FCM ad esempio servicedesk@mgb.ch).

7.5 Uso del badge aziendale

L'identificazione dei collaboratori all'interno degli edifici/dei locali o delle aree Migros avviene tramite il badge aziendale personale. Il badge aziendale personale deve essere indossato in modo visibile all'interno degli edifici/dei locali o nelle aree Migros. Fanno eccezione i locali appositamente contrassegnati (ad es. produzione igienica).

7.6 Clean-Desk Policy

Prima di lasciare il posto di lavoro verificare quanto segue:

- Tutti i documenti/supporti dati contenenti informazioni aziendali riservate e sensibili devono essere tolti dalla scrivania al momento di allontanarsi dal posto di lavoro. Questi includono, a titolo non esaustivo, chiavette USB, biglietti da visita e documenti stampati.
- Computer/notebook devono essere bloccati prima di abbandonare il posto di lavoro.
- Eventuali documenti sensibili e riservati da conservare devono essere custoditi al sicuro sotto chiave (ad es. in una cassetta/un armadietto chiuso a chiave).
  Qualora non sia necessario conservarli, i documenti devono essere eliminati senza indugio e in modo sicuro (ad es. con il trituratore o il distruggi-documenti). Tutti i rifiuti cartacei contenenti informazioni sensibili o riservate devono essere smaltiti negli appositi trituratori. Tali dati non devono essere smaltiti in nessun caso nei rifiuti comuni.

7.7 Utilizzo di stampanti e fotocopiatrici

Se possibile e se l'attrezzatura necessaria è disponibile, i documenti devono essere stampati nei locali aziendali in modo sicuro. Tutti i documenti stampati devono essere rimossi immediatamente dalla stampante. I documenti con contenuto riservato o segreto eventualmente trovati presso una stampante vanno immediatamente consegnati all'autore o distrutti.

7.8 Segnalazioni di casi di emergenza

Il Gruppo Migros gestisce diverse infrastrutture di servizio locali e una infrastruttura di servizio centrale per la Federazione delle cooperative (servicedesk@mgb.ch). In caso di emergenza correlata all'utilizzo di una risorsa informatica, si rende necessaria una segnalazione immediata al service desk dell'impresa interessata o a quello della Federazione delle cooperative Migros (servicedesk@mgb.ch).

Gli incidenti tecnici sospetti (per es. possibili infezioni di un computer da parte di virus, phishing, hacking, ecc.) devono essere segnalate immediatamente, vale a dire al momento della constatazione del sospetto, a security@migros.ch e ai service desk locali interessati.

7.9 Sicurezza all'esterno dei locali aziendali

Le collaboratrici e i collaboratori in viaggio devono osservare i punti seguenti.

- Nei luoghi pubblici (aeroporti e stazioni, ristoranti, parchi, treni e altri luoghi molto affollati) occorre prestare particolare attenzione se si discute di informazioni riservate. Non è consentita la discussione di informazioni segrete in luoghi pubblici.

- Quando si lavora al notebook, i terzi non devono poter leggere informazioni riservate o segrete. All'occorrenza il servizio informatico può procurare un filtro protettivo (privacy filter).
- In caso di connessioni a WLAN pubbliche o private, lo scambio di dati deve essere protetto mediante un collegamento sicuro (ad es. VPN).

7.10 Utilizzo di internet

Internet serve alle collaboratrici e ai collaboratori della Migros per acquisire informazioni, scambiare dati e documenti con i partner commerciali, la clientela, le autorità e altri uffici tenendo conto dei requisiti di sicurezza delle informazioni e per procurare servizi e merci in considerazione delle regolamentazioni in vigore sulle firme. Le collaboratrici e i collaboratori Migros devono utilizzare internet in maniera da tutelare la Migros da rischi giuridici, normativi e operativi nonché da rischi alla reputazione. L'utilizzo privato di internet durante l'orario di lavoro deve essere ridotto al minimo.

È vietato ogni utilizzo illecito o inadeguato di internet, tra cui:

- l'accesso a siti di gioco di qualsiasi tipo (per es. giochi d'azzardo) o di negoziazioni private di borsa
- l'apertura di siti web con contenuto indecente o illegale

7.11 E-mail

Una mailbox personale può essere utilizzata solo dalla relativa collaboratrice o dal relativo collaboratore. Le e-mail professionali importanti, che devono essere accessibili anche per altre persone, devono essere conservate in posizioni concordate in un apposito archivio dati.

La deviazione automatica o l'inoltro automatico a indirizzi e-mail esterni o interni è vietato. In casi specifici è possibile allestire l'inoltro esterno. Le domande vanno indirizzate a servicedesk@mgb.ch o al service desk nell'impresa Migros. Al riguardo:

l'inoltro può essere effettuato solo da un indirizzo e-mail personale interno a un unico indirizzo e-mail personale direttamente associato alla persona. Pertanto, si fa divieto di inoltrare e-mail: 1) in generale, da un indirizzo e-mail funzionale/collettivo a uno esterno; 2) da un indirizzo e-mail interno a più indirizzi esterni; 3) da un indirizzo e-mail interno a persone prive di qualsivoglia rapporto contrattuale con un'impresa M.

In caso di assenza o di uscita dal servizio, le collaboratrici e i collaboratori sono tenuti ad allestire una notifica di assenza. Se la posta in entrata viene gestita da un sostituto, l'attività deve essere preventivamente e bilateralmente concordata. In circostanze speciali (per es. malattia della collaboratrice o del collaboratore), la Migros si riserva il diritto di allestire una notifica di assenza tenendo conto degli aspetti relativi alla protezione dei dati.

Particolare cautela va prestata in caso di e-mail con mittente sospetto o formulazioni strane nella riga dell'oggetto o, in generale, nel testo. E-mail di questo tipo devono essere immediatamente cancellate. Per motivi di sicurezza, non si devono aprire gli allegati di queste e-mail né cliccare sui loro link.

I dati e i documenti elettronici dei collaboratori riguardanti l'attività commerciale possono essere salvati e consultati nell'ambito di un'indagine interna. Pertanto tutti gli elementi Outlook (e-mail, voci di calendario, attività, chat di Teams e contatti) vengono conservati per 10 anni con questa finalità e con protezione dell'accesso.

8. Utilizzo di risorse informatiche private

8.1 Utilizzo professionale di risorse informatiche private

Le risorse informatiche private (per es. il proprio smartphone) possono essere utilizzate a fini professionali. Le collaboratrici e i collaboratori non hanno alcun diritto a beneficiare di supporto o assistenza per le risorse di lavoro private. Le imprese M possono prevedere regole differenti per quanto riguarda sia l'indennizzo sia i servizi di supporto e installazione.

Le risorse informatiche private possono essere collegate esclusivamente alla rete appositamente prevista del Gruppo Migros. L'utente è tenuto a garantire la sicurezza delle risorse informatiche private. I dati aziendali archiviati localmente sul dispositivo devono essere cancellati immediatamente dopo l'utilizzo.

Se vengono impiegate a fini aziendali, le risorse informatiche private devono essere protette dall'accesso non autorizzato con password o con una protezione biometrica e crittografia della memoria. Gli aggiornamenti del software (ovvero sistema operativo, applicazioni, app, ecc.) devono essere effettuati, non appena il produttore del software li mette a disposizione.

Nel caso di risorse informatiche private (ad es. laptop o tablet), quando si accede ai dati all'interno della rete Migros è necessario verificare che il collegamento venga stabilito tramite una connessione sicura (ad es. VPN) e ricorrendo a un'autenticazione a più fattori. Ciò non si applica al semplice utilizzo delle funzionalità Exchange con risorse informatiche private (ad es. il proprio smartphone), a condizione che questo avvenga tramite un metodo consentito dall'impresa Migros (ad es. Active Sync, app di Outlook).

9. Gestione dei dati Migros

9.1 Classificazione dei dati

Nel contesto del presente regolamento sull'utilizzo dei sistemi informatici, i dati aziendali vengono classificati nelle seguenti categorie:

- Dati pubblici: i dati sono accessibili a tutti.
- Dati interni: i dati sono accessibili a tutte le collaboratrici e a tutti i collaboratori della Migros.
- Dati riservati: i dati sono accessibili a un gruppo circoscritto di collaboratrici e collaboratori della Migros e necessitano di una protezione superiore. L'autorizzazione è limitata e prevista solo per un determinato gruppo. I dati devono essere trattati con una cautela superiore. Si tratta per esempio di dati personali o finanziari.
- Dati segreti: i dati sono accessibili solo a un piccolo gruppo di persone conosciute per nome e sono completamente protetti. I dati vengono codificati individualmente a livello di file. Sono dati segreti, per esempio, le informazioni su grandi operazioni di M&A.

Oltre alle categorie dei dati aziendali, esistono dati privati che non vengono trattati separatamente sotto un profilo tecnico. Per i dati delle/degli utenti e delle collaboratrici/collaboratori non direttamente correlati alla Migros sussiste la presunzione confutabile che si tratti di dati privati. I dati privati non possono essere memorizzati sui sistemi Migros.

9.2 Gestione dei dati

I collaboratori devono gestire i dati e le informazioni in modo responsabile.

Le informazioni e i dati devono essere trattati in modo scrupoloso e attento, comunicati o resi accessibili solo a quelle persone che ne hanno bisogno per espletare la loro funzione e i loro compiti, sempre protetti in modo adeguato. Possono inoltre essere utilizzati solo in modo conforme alle disposizioni legali e alle normative interne applicabili.

Nell'ambito della loro sfera d'influenza, le collaboratrici e i collaboratori sono tenute/i ad assicurare il rispetto delle disposizioni legali e delea normative interne applicabili.

Nel trattamento di dati personali vigono in particolare la direttiva sulla protezione dei dati nonché altri requisiti relativi alla protezione dei dati previsti dal servizio Legal & Compliance FCM.

I dati aziendali vengono memorizzati esclusivamente su supporti tecnologici di memorizzazione forniti e autorizzati dalla Migros o su suo incarico. Se ai sensi del capitolo 8.1 vengono impiegate risorse informatiche private, la collaboratrice o il collaboratore deve assicurare la cancellazione dei dati sul dispositivo privato immediatamente dopo l'utilizzo.

Prima di uscire dal servizio, la collaboratrice o il collaboratore deve riordinare l'archivio dati personale. I dati privati devono essere cancellati e gli altri dati spostati d'intesa con il superiore. Dopo la data di uscita dal servizio, l'accesso agli archivi di dati personali viene bloccato.

Per ogni posizione di archiviazione deve essere definito un responsabile di directory, che ha il compito di definire inizialmente le persone autorizzate all'accesso e di effettuare le relative modifiche nel corso dell'attività.

I dati aziendali non pubblici possono essere memorizzati su chiavette USB e supporti dati esterni solo dopo essere stati codificati (per es. CD, DVD, chiavette USB, dischi rigidi esterni / dischi rigidi USB e simili). Dopo l'utilizzo, i dati devono essere cancellati dalla chiavetta USB. I CD e i DVD con dati aziendali devono essere smaltiti in modo sicuro dopo l'utilizzo.

9.3 Gestione di password

Le connessioni alle risorse informatiche Migros devono essere effettuate solo con l'ID utente personale e la password personale. Vigono le seguenti regole sulle password:

- La password, il login e i certificati sono personali e devono essere mantenuti segreti nei confronti dei terzi. È dunque vietato comunicare ad altri la propria password o renderla loro accessibile. È vietato prendere nota di password e PIN, a meno che le annotazioni non vengano conservate in un luogo chiuso a chiave (per es in una busta in una cassaforte).
- La password deve almeno soddisfare i requisiti dello Standard password (vedere MSS001, capitolo «Password vietate»).
- La password non deve essere indovinata facilmente. Non può quindi contenere, per esempio, l'ID utente, il nome dell'organizzazione, altre informazioni personali, numeri di telefono, password comuni (per es. «passw0rd», «pass1234», ecc.).
- Le password che vengono utilizzate nel Gruppo Migros non possono essere utilizzate presso altre istituzioni e per applicazioni esterne a Migros (per es. per account e-mail privati, su portali web, ecc.).
- All'interno del Gruppo Migros è possibile utilizzare più volte la stessa password se viene utilizzata nello stesso ruolo.
- Se sussiste il sospetto che la password sia nota a terzi, le collaboratrici e i collaboratori sono tenuti a cambiare la password immediatamente.
- Se la password viene cambiata, non si deve selezionare una password già precedentemente impiegata.
- Le password non possono essere trasmesse con testo in chiaro (per es. in un'e-mail).

- Le password possono essere inserite solo quando non si è osservati da altre persone.
- Le password iniziali devono tassativamente essere modificate dopo la prima connessione.
- Le password e gli ID utente predefiniti, per esempio quelli del produttore al momento della consegna delle risorse informatiche, devono essere sostituiti da password e, se possibile, da ID utente individuali prima della messa in servizio operativa del sistema o del dispositivo.
- Ogni collaboratrice e collaboratore è responsabile per tutte le operazioni condotte con il proprio ID utente.
- L'accesso in remoto a fini di supporto deve tassativamente essere confermato dall'utente al momento in cui la connessione viene stabilita. Durante la sessione in remoto le attività dell'operatore del supporto devono essere monitorate e dopo la conclusione dei lavori occorre accertarsi della corretta uscita dalla sessione in remoto.

9.4 Registrazione e analisi di dati elettronici

La Migros può utilizzare sistemi che generano registri e segnali di avviso per mantenere il funzionamento, la sicurezza, l'integrità e la disponibilità delle risorse informatiche, dei dati e delle informazioni, per assicurare la qualità del servizio, per rispettare e controllare le disposizioni legislative applicabili e/o le normative interne, per controllare il rispetto delle condizioni di licenza, per scopi di fatturazione e per controllare i costi, nonché per identificare e correggere i guasti di funzionamento e gli usi impropri.

Le collaboratrici e i collaboratori sono consapevoli del fatto che la Migros registra i dati sull'utilizzo delle risorse informatiche, in particolare i dati sul traffico e di log relativi all'utilizzo di internet e delle e-mail, dati analoghi sulle chiamate in uscita e in entrata nonché dati di log relativi agli accessi ai file, alle loro modifiche e cancellazione e che dispone di dati generali sugli utenti di tutti gli account e che può analizzarli per gli scopi menzionati. In linea di principio l'analisi avviene in modo anonimizzato o pseudonimizzato.

In caso di incidenti o di casi sospetti gravi, d'intesa con il reparto del personale e Legal & Compliance nonché nel rispetto del principio di proporzionalità, possono essere condotte analisi di dati con riferimenti personali o effettuate ulteriori registrazioni. Per maggiori informazioni sulla messa in sicurezza e sull'esame di dati e documenti si rinvia alla direttiva sulle segnalazioni e indagini interne.

I dati vengono conservati in forma personalizzata per tutto il tempo necessario allo scopo per il quale sono stati raccolti o nel quale sussiste un interesse legittimo alla loro conservazione. Si tratta in particolare del caso in cui i dati personali sono necessari per far valere le proprie pretese o per difendersi dalle pretese altrui, per motivi probatori, a fini di archiviazione e per garantire la sicurezza informatica. I dati registrati vengono inoltre conservati in forma personalizzata per tutto il tempo in cui soggiacciono a un obbligo di conservazione legale o in cui sussiste un altro motivo eccezionale valido secondo il diritto applicabile. Per determinati dati vige per esempio un termine di conservazione di dieci anni. Per gli altri dati si applicano termini di conservazione più brevi, per esempio per le registrazioni di determinate operazioni su internet (dati di log).

10. Documenti di riferimento

Oltre alle istruzioni generali per il rispetto della sicurezza delle informazioni, esistono ulteriori regolamenti che valgono per tutte le collaboratrici e tutti i collaboratori. In aggiunta a tutte le linee di indirizzo, le politiche, le direttive, gli standard e le istruzioni, per le collaboratrici e i collaboratori Migros sono vincolanti anche tutti gli allegati al regolamento sull'utilizzo dei sistemi informatici. Tutti i documenti si trovano su security.migros.net.

Ulteriori documenti di Legal & Compliance sono reperibili sull'intranet. I documenti HR rilevanti sono pubblicati qui.

Maggiori informazioni sul trattamento di dati personali sono reperibili nella dichiarazione sulla protezione dei dati per le collaboratrici e i collaboratori.