REGOLAMENTO DI SICUREZZA DELLE INFORMAZIONI E PRIVACY

Informazioni sul documento		
Codice	Regolamento sicurezza delle informazioni	
Redatto da	Sandro Musarò	Responsabile servizi IT
Approvato da	Andrea Solimeno	RSGI
Approvato il	15/09/2023	

Sommario

1 Premessa

Questo regolamento specifica le misure di sicurezza delle informazioni e di privacy da adottare da parte di tutte le persone che trattano dati di cui Selexi è titolare o responsabile.

Le misure sono allineate alla politica per la qualità, l'ambiente, la sicurezza delle informazioni e la privacy.

Il presente Regolamento è diffuso a tutti i soci, dipendenti e collaboratori di Selexi.

La gestione delle informazioni deve avvenire nel rispetto della normativa a tutela della privacy, al fine di garantire la protezione dei diritti e delle libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

Il personale è tenuto a rispettare le disposizioni di questo documento. La violazione di tali norme può comportare sanzioni disciplinate nei rispettivi contratti in essere (contratti di incarico, CCNL, ecc.).

Si ricorda che è vietato aggirare o tentare di eludere i meccanismi di sicurezza aziendali.

2 Referente privacy

Selexi non ha la necessità di nominare un DPO (Data protection officer o Responsabile della protezione dei dati o RPD) con i compiti e le caratteristiche specificate dalla normativa vigente.

In Selexi, il Presidente del CdA ha i seguenti compiti in qualità di referente privacy:

- informare, aggiornare e fornire assistenza al personale;
- essere punto di riferimento dei clienti e degli enti esterni (p.e. Garante per la protezione dei dati personali) in materia di privacy;
- sorvegliare, attraverso audit, l'osservanza delle misure di sicurezza e della normativa vigente in materia di privacy.

Il referente privacy può avvalersi di consulenti esterni per lo svolgimento delle attività sopra descritte.

3 Controllo degli accessi alle risorse informatiche

Le regole seguenti sono applicate ai sistemi informatici di Selexi e comunque in qualsiasi sistema siano disponibili tali informazioni per i quali il personale ha accesso in ragione del suo ruolo in Selexi.

Sono inclusi:

- pc aziendali e personali (qualora usati per trattare informazioni aziendali);
- dispositivi aziendali e personali (qualora usati per trattare informazioni aziendali);
- server aziendali;
- software, database e altri strumenti software aziendali.

3.1 Credenziali

L'accesso alle risorse informatiche è personale deve essere consentito soltanto mediante credenziali personali (user-id e password).

La user-id deve identificare il singolo utente, la password è riservata e individuale. È fatto assoluto divieto all'utente di far conoscere le proprie password ad altri.

Le password utilizzate per accedere ai sistemi di Selexi non devono essere utilizzate per altri scopi (p.e. sistemi pubblici, *social network*, email personale).

Il personale deve modificare le password ogni qualvolta vi sia un'indicazione della loro possibile compromissione.

Si riportano di seguito le regole a cui devono essere soggette le password:

- l'utente sceglie direttamente le proprie password;
- lunghezza minima: 8 caratteri;
- durata massima di validità: 90 giorni, scaduti i quali devono essere modificate;
- la password soddisfa almeno 3 di queste condizioni di sintassi:
    - contenere almeno un carattere maiuscolo;
    - contenere almeno un carattere minuscolo;
    - contenere almeno un numero;
    - contenere almeno un carattere speciale (+,=,_,*_,&,…);
- la password non contiene la user-id.

L'utenza deve essere bloccata dopo non più di 10 tentativi sbagliati di inserire la password (tranne che per le password di amministrazione).

Dove possibile, i sistemi informatici sono configurati affinché i controlli sopra specificati siano eseguiti automaticamente.

Si ricorda che è espressamente vietato:

- detenere, utilizzare o diffondere abusivamente codici di accesso a sistemi informatici di terzi o di enti pubblici;
- tenere una registrazione (es. su carta, documenti software o dispositivi portatili) delle credenziali, a meno che siano memorizzate in modo sicuro (es. documenti o cartelle cifrate o strumenti di password management);
- porre in essere condotte, anche con l'ausilio di terzi, miranti all'accesso abusivo a sistemi informativi altrui.

Solo in casi specifici (es.: funzioni di help desk) sarà possibile utilizzare user-id "comuni" condivise tra più utenti (es.: operatori di help desk).

3.2 Autorizzazioni

Le autorizzazioni sono concesse dai membri della Direzione di Selexi.

Quando una persona non ha più la necessità di accedere ai sistemi di Selexi (p.e. al termine del rapporto di lavoro), su richiesta della Direzione:

1. l'utenza viene disabilitata (in caso di cambio di mansione) o rimossa (in caso di cessata collaborazione);

2. le password delle utenze “comuni” di tutti i sistemi a cui la persona non ha più necessità di accedere sono modificate dall’IT.

L’amministrazione conserva l’elenco del personale di Selexi e dei collaboratori.

Le autorizzazioni impostate sui sistemi informatici sono periodicamente (almeno ogni 12 mesi o durante gli audit interni descritti al paragrafo 15.1) riesaminate dalla Direzione, in modo da verificarne la corrispondenza con le mansioni e il rispetto del principio generale di segregazione dei compiti.

Dopo la conclusione del rapporto di lavoro, le mailbox personali sono conservate per un anno, nel caso in cui si renda necessario recuperare comunicazioni con clienti o fornitori. L’invio e la ricezione di email è comunque inibito.

3.3 Amministratori di sistema

Autorizzazioni particolari sono concesse agli amministratori di sistema, ossia le persone che possono gestire le configurazioni dei sistemi informatici (server, sistemi operativi, applicazioni).

Le autorizzazioni sono gestite come sopra riportato.

Gli amministratori di sistema (AdS) sono selezionati dal responsabile ICT in accordo con la Direzione Selexi e sono assicurate le seguenti:

- gli AdS sono selezionati considerandone le competenze acquisite attraverso esperienza, istruzione e formazione, oltre che per affidabilità, da rilevare attraverso le dichiarazioni fatte e la verifica sul campo;
- tutto il personale dell’ICT ha ruolo di amministratore di sistema;
- ogni AdS deve sottoscrivere la lettera di “Designazione amministratore di sistema”, in cui sono ribadite le istruzioni e in particolare di applicare questo stesso regolamento e le regole privacy stabilite per lo sviluppo; l’ambito di operatività è descritto sul file “Ruoli e permessi utente” per gli ambiti di dominio, file server e ProctorExam;
- gli AdS sono elencati nel file sopra indicato e mantenuto dal referente privacy in collaborazione con il responsabile ICT; tutto il personale, attraverso l’organigramma è a conoscenza degli AdS in quanto parte dell’ICT;
- registrazione delle attività di login e logout degli AdS come descritto in questo stesso regolamento al paragrafo 15.3;
- verifica periodica delle attività degli AdS nell’ambito degli audit interni come descritto in questo stesso regolamento al capitolo 15.

Per quanto riguarda attività sistemistiche affidate all’esterno, il fornitore è trattato come responsabile del trattamento dei dati personali e come tale deve mantenere un elenco dei propri AdS come sopra indicato e renderlo disponibile a Selexi in caso di necessità (p.e. richiesta da parte delle autorità).

3.4 In caso di assenza di un utente

In caso di assenze prolungate (per esempio oltre i 6 mesi), le utenze sono sospese.

Qualora, per esigenze di indifferibilità e urgenza o stato di necessità connesso all’attività aziendale, sia necessario accedere alla risorsa informatica assegnata a un utente assente, si segue la presente procedura:

- la Direzione cerca di contattare l'utente per esporgli le esigenze intervenute; se l'utente non è rintracciabile, è comunque cura della Direzione fare in modo che l'utente sappia di quanto avvenuto il prima possibile;
- se non sono percorribili strade alternative e per i sistemi che lo permettono, la Direzione (in presenza di un collega) re-imposta temporaneamente la password dell'utente e accede al sistema;
- al suo rientro, l'utente stesso cambia la password.

4 Proprietà delle risorse informatiche e dei dati

Le risorse informatiche (hardware, software e dati) di Selexi, incluso il sistema di posta elettronica devono essere utilizzate esclusivamente nell'ambito delle attività lavorative per conto e/o in favore della società.

I dati, inclusi i messaggi di posta elettronica, i post e i documenti disponibili sui sistemi informatici di Selexi non sono proprietà privata del singolo utente.

Tutti i software in uso e non sviluppati internamente devono rispettare la normativa in materia di diritto d'autore, ossia avere licenza attiva e utilizzati come previsto dalla licenza stessa (si segnala che anche i software *free* sono offerti con licenza, per quanto gratuita).

I software con licenza Selexi non devono essere messi a disposizione di esterni non autorizzati.

5 Riservatezza delle informazioni aziendali

Informazioni, dati e applicazioni di Selexi e dei clienti sono normalmente da considerarsi riservate e strettamente attinenti all'attività di Selexi, nonché di proprietà della stessa e/o dei clienti.

È vietato copiare, trasferire, diffondere o usare per scopi diversi da quelli attinenti alla propria attività lavorativa per Selexi dette informazioni.

Le informazioni, soprattutto se includono dati personali, non possono essere conservate più del tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di sicurezza. Quando non più necessarie, tali informazioni sono distrutte o cancellate.

Sono previsti tre livelli di classificazione delle informazioni:

- pubblico;
- ad uso interno (per le procedure e le istruzioni, potenzialmente accessibili anche da clienti e auditor);
- riservato (con circolazione limitata).

Si raccomanda, dove opportuno, di specificare per iscritto l'ambito di circolazione di ciascuna informazione, soprattutto se non facilmente deducibile, in particolare se spedite e sui messaggi di accompagnamento (ossia nel corpo dell'email).

Le informazioni riservate devono essere:

- conservate in cartelle (logiche o fisiche) ad accesso limitato;
- trasferite ai soli destinatari previsti indicando, se non già evidenti, i limiti di circolazione;

- cancellate in modo sicuro dai supporti non più necessari;
- se su supporto cartaceo, distrutte con distruggi-documenti.

6 Dati dei clienti

I dati (personali e non personali) dei clienti sono da considerare come riservati e pertanto il personale è tenuto a:

- utilizzare con diligenza e per i soli fini lavorativi le risorse informatiche del cliente che gli vengano concesse in uso;
- accedere ai dati del cliente esclusivamente per le finalità previste dall'attività lavorativa in corso e rispettarne la confidenzialità prevenendone la divulgazione;
- accedere ai locali ed alle attrezzature del cliente solo previa autorizzazione, anche verbale, da parte del cliente stesso e per i soli fini lavorativi.

Al termine delle attività svolte per i clienti e del tempo di conservazione previsto:

- i dati personali sono cancellati tempestivamente o anonimizzati in modo tale da garantire che i dati non possano essere divulgati a soggetti non autorizzati (l'anonimizzazione si può rendere necessaria per elaborare statistiche in merito all'andamento delle prove di selezione o delle singole domane);
- i dati non personali (p.e. prove per la selezione, materiale di formazione) possono essere conservati da Selexi se si tratta di materiale prodotto nell'ambito di una commessa per il cliente.

Per la cancellazione dei supporti di memoria, vedere il paragrafo 10.3.

La divulgazione non autorizzata di dati dei clienti è severamente vietata e può comportare procedimenti disciplinari e penali.

7 Comunicazioni

Le comunicazioni con i clienti, fornitori e terzi avvengono solo con strumenti e riferimenti concordati, soprattutto quando si tratta di informazioni riservate.

Strumenti e riferimenti concordati possono essere:

- sistema di ticketing di Selexi;
- email con indirizzo fornito nella documentazione contrattuale;
- email con indirizzo ufficiale (p.e. le richieste del cliente devono pervenire solo da indirizzi ufficiali quali pippo@azienda.it e non indirizzi personali quali pippo@gmail.com, a meno di specifiche indicazione del cliente);
- posta cartacea inviata all'indirizzo ufficiale; per le informazioni confidenziali, viene usata la Raccomandata.

Per le comunicazioni telefoniche, non sono mai comunicati i dati oralmente a persone sconosciute, né si accetta di inviarli a indirizzi (email, fisici, di strumenti di instant messaging) non precedentemente concordati.

Con le parti esterne (tra cui i clienti e fornitori) è necessario stabilire il livello di riservatezza da assicurare. Per questo si pongono etichette sui messaggi, come ricordato al capitolo 5. Se i clienti richiedono l'uso

di specifici strumenti, anche insicuri (p.e. server FTP o strumenti cloud pubblici insicuri o che non garantiscono il rispetto della normativa in materia di privacy), è opportuno, prima di adempiere alle richieste, proporre loro alternative.

Si rammenta che, nell'ambito dell'impegno che Selexi si è assunta sui temi della parità di genere (o più in generale sui temi DEI), è stata definita la procedura P-13 avente lo scopo di definire le modalità di gestione delle comunicazioni aziendali e di fornire una guida all'utilizzo del linguaggio inclusivo, cioè un linguaggio rispettoso delle differenze di genere e non discriminatorio.

Per quanto riguarda il linguaggio da adottare in tutte le comunicazioni con clienti, fornitori e terzi in generale, si rimanda pertanto alla suddetta procedura P-13 "Gestione della comunicazione per la parità di genere".

8 Strumenti di messaggistica elettronica

Anche per le comunicazioni veicolate attraverso strumenti di messaggistica elettronica, si deve utilizzare un linguaggio rispettoso delle diversità ed inclusivo, come definito nella specifica procedura P-13 alla quale si rimanda.

8.1 Utilizzo della posta elettronica

Un messaggio di posta elettronica gestito con le utenze Selexi non deve essere considerato corrispondenza personale.

Gli utenti devono prestare attenzione agli invii di messaggi di posta elettronica affinché non siano recapitati per errore a un destinatario non autorizzato a ricevere le informazioni contenute.

Se il messaggio di posta elettronica contiene informazioni riservate, è necessario qualificare il messaggio come o "Riservato" o diciture similari, a meno che il livello di riservatezza non sia facilmente intuibile dal destinatario.

Alcune regole da seguire:

- non rispondere alle e-mail comunemente note con il nome di "catene di S. Antonio", nelle quali si richiede di inoltrare il contenuto della stessa a tutti i propri contatti nonché inviare materiale pubblicitario/non richiesto;
- evitare di inviare file di grandi dimensioni se non per ragioni lavorative (es. auguri per ricorrenze, scherzi, giochi, eccetera);
- non aprire i link presenti nei messaggi ricevuti da e-mail non sicure o da mittenti sconosciuti; è preferibile, in caso di necessità, digitare l'URL del sito nell'apposita barra;
- non creare o distribuire qualsiasi messaggio molesto, offensivo o discriminatorio (es. commenti offensivi su razza, orientamento sessuale, credo religioso);
- in caso di assenza programmata (ad esempio per ferie o attività di lavoro fuori sede che pregiudichino la visibilità della posta elettronica) è opportuno impostare all'interno del client di posta elettronica messaggi di risposta automatici per permettere ai mittenti delle mail di essere consapevoli dell'assenza dall'azienda nonché di ricevere indicazioni in merito a possibili referenti alternativi;

- è necessario prestare la massima attenzione nell'apertura degli allegati alle mail ricevute, indipendentemente dal fatto che si conosca o meno il mittente; in particolare non devono essere aperti messaggi contenenti documenti non attesi o di tipo eseguibile;
- è necessario prestare attenzione all'auto-completamento degli indirizzi, al fine di evitare di inviare l'email alla persona sbagliata.

Si segnala che la posta elettronica è controllata, oltre che da un antivirus, anche da un sistema di antispam. Il sistema può bloccare e-mail legittime e per questo ciascun utente è tenuto a prestare attenzione agli avvisi inoltrati dall'antispam.

8.2 Altri strumenti di messaggistica

Gli strumenti di messaggistica istantanea (p.e. WhatsApp e Slack) non garantiscono i livelli di sicurezza richiesti dalla normativa vigente, soprattutto per quanto riguarda i dati personali. Inoltre le comunicazioni non sono tracciabili se non per i due interlocutori.

Per questi motivi devono essere utilizzati solo per inviare dati non confidenziali e non personali e senza caratteristiche di tracciabilità.

9 Uso di Internet

Il PC assegnato al singolo utente e abilitato alla navigazione in Internet costituisce uno strumento professionale utilizzabile esclusivamente per lo svolgimento dell'attività lavorativa. È vietata la navigazione in Internet con strumenti di Selexi per motivi diversi da quelli legati all'attività lavorativa.

A titolo meramente esemplificativo, l'utente non può utilizzare la strumentazione aziendale per:

- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web, ivi inclusi filmati e musica, se non attinenti all'attività lavorativa;
- ogni forma di registrazione o partecipazione attiva e/o passiva a siti i cui contenuti non siano riconducibili all'attività lavorativa;
- la partecipazione a forum, blog o social network per scopi non professionali;
- l'effettuazione di transazioni finanziarie e commerciale personali ivi comprese le operazioni di remote banking e acquisti on-line;
- usare servizi per scopi ingiuriosi o comunque potenzialmente dannosi per l'immagine aziendale;
- svolgere attività illegali (per esempio, scaricamento di file in contrasto con la normativa in materia di diritto d'autore), comunque sconvenienti (per esempio, accesso a siti pornografici, di estremismo religioso o politico).

Per l'uso di social network, forum e simili, anche in modalità privata si richiede di:

- evitare di qualificarsi come persona collegata a Selexi o esprimere opinioni in modo che possano essere intese come opinioni espresse per conto di Selexi (questa regola può essere derogata quando ciò sia necessario per le proprie specifiche funzioni, per esempio per attività commerciali, e previa autorizzazione della Direzione);

- **non inviare commenti ingiuriosi, in particolare verso il proprio datore di lavoro e i suoi clienti e fornitori;**
- non inviare dati riservati di Selexi.

10 Dispositivi informatici

Per tutti i dispositivi informatici usati per trattare informazioni di Selexi (pc portatile, cellulare o smarpthone, tablet; assegnato da Selexi o di proprietà e usati anche in caso di lavoro da remoto o *smart working*) valgono le seguenti regole:

- non lasciare mai il dispositivo incustodito, se non in luoghi sicuri (l'automobile NON è un luogo sicuro);
- custodire i dispositivi con la massima cura in modo da evitare incidenti (cadute accidentali, danneggiamento dello schermo, sottrazione indebita, danneggiamento causa acqua o calore, ecc.);
- attivare il blocco con username e password prima di allontanarsi dal dispositivo (se possibile, anche in caso di evacuazione ed emergenza, ma sempre considerando che la priorità è la salvaguardia della vita umana);
- attivare il blocco automatico non oltre 10 minuti di inattività.
- in caso di viaggi, trasportare i dispositivi come bagaglio a mano e sistemarli in custodia adeguata;
- configurare l'accesso ai dispositivi affinché sia controllato da password o meccanismo simile;
- attivare la cifratura completa dei dischi;
- ove possibile, prevedere almeno due utenze sul dispositivo: utente generico, senza possibilità di installare software o modificare le configurazioni e utente amministratore; accedere quindi solo come utente senza autorizzazioni di amministrazione, tranne quando necessario;
- quando si usa il dispositivo (pc portatile o tablet) in luoghi pubblici, prestare attenzione che lo schermo non possa essere visto da altri;
- aggiornare regolarmente il dispositivo e i software installati con le patch di sicurezza e, quando possibile, impostare l'aggiornamento automatico;
- per i pc, mantenere attivo un antivirus con aggiornamento automatico delle definizioni e del motore;
- per i pc, mantenere attivo e aggiornato un firewall personale;
- usare solo software licenziato;
- usare immagini non sconvenienti o comunque contrari al Codice Etico per i desktop;
- non concedere in uso a terzi (inclusi famigliari) i dispositivi e i servizi messi a disposizione da Selexi;
- disabilitare i servizi di trasmissione e comunicazione dati (ad esempio bluetooth, wi-fi, ecc.) quando non utilizzati;

- cancellare in modo sicuro il dispositivo quando dismesso per smaltimento o uso da parte di altri (formattando in modo “completo” e non “veloce”); in caso di smaltimento per guasti che ne impediscono la formattazione, distruggere il disco (p.e. punzonando l’hard disk con un cacciavite). Si rammenta che per la dismissione/smaltimento di dispositivi e materiali di ufficio, si applica la procedura P-11 Gestione Ambientale, alla quale si rimanda per ulteriori dettagli.

Per accedere ai server e alle applicazioni Selexi da remoto è necessario usare VPN, come stabilito dai sistemisti.

Le regole sopra elencato devono essere seguite anche per i dispositivi personali usati per accedere e trattare i dati di Selexi (pratica nota come BYOD o *Bring your own device*) e di quelli di altre organizzazioni (p.e. società di consulenza).

10.1 Cellulari o smartphone

Si raccomanda di porre particolare attenzione alle comunicazioni telefoniche in ambienti pubblici, quali ad esempio locali, stazioni e mezzi di trasporto, al fine di evitare la diffusione di informazioni aziendali a terzi.

Quando il cellulare o smartphone è trasferito ad altri o smaltito, è necessario preventivamente cancellare i dati utilizzando la funzione di ripristino alle condizioni di fabbrica.

10.2 Backup

I file di Selexi devono essere archiviati solo sui sistemi autorizzati da Selexi, in modo tale che ne sia garantito il backup periodico.

I backup devono essere oggetto di verifica (prove di *restore*) almeno annuale, in modo da assicurare il ripristino delle informazioni in caso di necessità.

10.3 Supporti di memorizzazione rimovibili

Se sono usati supporti di memorizzazione rimovibili (chiavi USB, SD card, CD, DVD) per scopi aziendali:

- i dati aziendali sono conservati in partizioni o cartelle cifrate o protette almeno con password;
- se scambiati con altri, in particolar modo esterni, solo i dati oggetto di scambio sono tecnicamente accessibili;
- il contenuto dei supporti è cancellato (formattato in modo “completo” e non “veloce”) prima di riutilizzarli; se ciò non fosse possibile, i supporti sono distrutti.

Si ricorda che è vietato collegare ai dispositivi assegnati per le attività lavorative supporti di memorizzazione di origine ignota.

11 Controllo dei dati in formato non elettronico

Si segnalano di seguito alcune misure da seguire per garantire la sicurezza delle informazioni in formato non elettronico, da seguire anche in caso di lavoro da remoto e *smart working*.

<u>Scrivania pulita</u>

Sulle scrivanie all'interno degli uffici sono presenti i soli documenti necessari per svolgere le proprie attività in corso. A fine giornata lavorativa le scrivanie devono essere lasciate libere e i documenti cartacei riposti negli appositi archivi chiusi a chiave.

Fotocopiatrici, stampanti e fax

Tali strumenti sono aziendali e sono utilizzati solo per lo svolgimento dell'attività lavorativa.

Non si lasciano incustoditi fax, fotocopie, stampe presso le apposite apparecchiature perché, oltre a creare disagio ad altri utenti, potrebbero essere letti da persone non autorizzate.

In caso di stampe multiple, particolare attenzione è posta alla verifica della coda di stampa, al fine di accertare che nessuno dei documenti inviati sia rimasto in sospeso.

In caso di trasferimento o dismissione, è necessario preventivamente cancellare i dati utilizzando la funzione di ripristino alle condizioni di fabbrica.

Si raccomanda di ridurre al minimo le stampe di dati riservati e personali.

Archivi

Conservare il materiale cartaceo con dati personali (archivi, documenti, faldoni, elenchi, fatture, preventivi, offerte, buste paga, ecc.) in armadi provvisti di chiusura con chiave.

Chiudere gli archivi o i locali dove sono posizionati con chiave. Questo, se possibile, anche in caso di evacuazione ed emergenza, ma sempre considerando che la priorità è la salvaguardia della vita umana.

Posizionare gli archivi in luoghi che non ne possano compromettere la conservazione (p.e. non in scantinati e lontani da caloriferi o caldaie a gas).

Documenti fuori sede

I documenti aziendali, se portati al di fuori delle sedi aziendali, non sono lasciati incustoditi in luoghi pubblici o in casa o in altri luoghi.

Distruzione dei documenti

La documentazione non più necessaria è eliminata con distruggi-documenti se riporta dati particolarmente riservati.

Trasferimenti e spedizioni

I dati riservati devono essere spediti:

- usando spedizionieri già valutati come affidabili (o comunque in prova);
- tracciando la spedizione;
- apponendo etichette in modo da richiamare la necessità di assicurare l'integrità di quanto spedito;
- usando buste o involucri opachi in modo che non sia possibile vedere o leggere il contenuto;
- evitare, nell'invio di pacchi con i questionari, riferimenti a Selexi;
- nel caso di materiale numeroso, con liste per il controllo di completezza.

Comunicazioni orali

Per le comunicazioni non si intrattengono conversazioni (di persona o al telefono) su materie riservate in luoghi dove si può essere ascoltati da persone non autorizzate e non si lasciano messaggi vocali con informazioni riservate.

Smaltimenti e dismissioni

Per dismissioni di materiale informatico (o altre attrezzature di ufficio) e per smaltimenti di rifiuti, si applica la procedura P-11 Gestione Ambientale, alla quale si rimanda per ulteriori dettagli.

12 Visitatori

L'accesso agli uffici è vietato a visitatori (clienti, fornitori, manutentori, ecc.) non espressamente autorizzati.

Solo coloro che svolgono attività lavorativa continuativa per Selexi possono accogliere visitatori e ospiti.

Il visitatore deve essere identificato da chi lo accoglie, in modo da evitare l'ingresso di malintenzionati. Per questo va richiesto un documento di identità per accertarne l'identità. Nel caso in cui il visitatore sia già noto a un'altra persona di Selexi, è sufficiente il suo riconoscimento.

Ai visitatori è presentato il documento "Regole ai visitatori – Selexi" perché prendano atto delle regole da seguire.

Il personale ospitante deve sempre accompagnare i visitatori e deve assicurarsi che non accedano a locali se non necessario per l'attività. I visitatori non vanno lasciati soli negli uffici, ma solo nelle sale riunioni o nelle aule.

Nel caso in cui si presentino funzionari di Agenzia delle Entrate, Guardia di Finanza, ecc., chi li accoglie deve seguire le stesse indicazioni e, appena fatti accomodare in una sala riunioni disponibile, deve contattare tempestivamente la Direzione.

13 Gestione delle richieste relative ai dati personali

Le persone a cui si riferiscono i dati personali (*interessati*) possono essere: dipendenti, amministratori, consulenti e collaboratori di Selexi, clienti, fornitori, candidati o, più in generale, persone fisiche di cui Selexi tratta i dati per conto proprio (in qualità di Titolare del trattamento) o per conto di uno o più clienti (in qualità di Responsabile del trattamento).

Gli interessati hanno il diritto di:

- ottenere, se non impedito da leggi o regolamenti, l'accesso ai propri dati personali (in formato facilmente interpretabile e leggibile dai software più diffusi), la loro correzione o cancellazione e la limitazione del loro trattamento;
- revocare, se non impedito da leggi o regolamenti, il consenso al trattamento;
- inviare un reclamo a Selexi o al Garante per la protezione dei dati personali.

Le richieste devono pervenire attraverso canali riconosciuti (vedere capitolo 7).

La richiesta inviata a Selexi viene soddisfatta entro un mese e, alla sua conclusione, ne viene dato riscontro all'interessato.

Se la richiesta proviene da un interessato per cui il cliente è titolare del trattamento, viene fornita esclusivamente l'indicazione di rivolgersi al titolare del trattamento o, se responsabile, al cliente di Selexi. In tutti questi casi, Selexi avvisa il proprio cliente (titolare o responsabile) e il titolare del trattamento se previsto dalle istruzioni ricevute.

14 Segnalazione e rilevazione anomalie (*data breach*)

Vedere la procedura di gestione degli incidenti di sicurezza delle informazioni e privacy.

15 Audit e controllo dell'utilizzo delle risorse informatiche

15.1 Audit

Gli audit sono condotti in modo integrato e secondo quanto specificato dalla procedura del sistema di gestione per la qualità.

Il referente privacy di Selexi programma, anche con il supporto di personale esterno, audit in merito al rispetto del presente Regolamento e delle procedure privacy applicabili. Il programma di audit include tutte le attività di Selexi.

Di norma il referente privacy comunica in anticipo il piano di audit e i nominativi delle persone incaricate di svolgerlo, in modo da assicurare la presenza delle parti interessate, ma in caso di necessità possono essere svolti audit senza previa comunicazione

Gli auditor sono nominati dal referente privacy dopo averne valutate le competenze, l'esperienza e l'assenza di conflitti d'interesse con l'attività di audit.

Alla conclusione dell'audit, l'auditor segnala al personale coinvolto eventuali anomalie riscontrate e redige un rapporto di audit. Il personale può segnalare punti di disaccordo in merito alle conclusioni dell'audit, che vengono riportati nel rapporto.

Per ogni anomalia, la Direzione o il Referente privacy devono riportare per iscritto, con le relative responsabilità, come intende assicurarne la soluzione ed evitarne la ripetizione in futuro. Le azioni correttive devono essere chiuse entro 3 mesi dalla data dell'audit. In caso di anomalie gravi potrebbe rendersi necessario un audit straordinario di verifica della chiusura delle anomalie.

15.2 Audit dei clienti

I clienti, titolari del trattamento dei dati, per conto dei quali Selexi esegue un trattamento (in veste di Responsabile) possono svolgere audit seguendo le regole stabilite contrattualmente.

È compito del personale assicurare la riservatezza delle informazioni non pertinenti l'audit specifico (p.e. deve mostrare solo documentazione relativa al cliente per cui si svolge l'audit).

15.3 Controlli sui sistemi informatici

I sistemi informatici di Selexi registrano alcune azioni degli utenti (p.e. login e logout). I log sui file e sui record (p.e. l'autore dell'ultima modifica) possono essere letti dagli utenti che accedono esclusivamente per svolgere le proprie mansioni.

Tutti i sistemi registrano log di alcune attività (p.e. navigazione su Internet, sistemi di configurazione del software, prestazioni dei sistemi). Eventuali dati personali raccolti da questi log non sono oggetto di monitoraggio. In caso di segnalazione di abusi potrebbero essere letti da personale indicato dalla Direzione di Selexi.

Altri dati sono registrati dai sistemi di monitoraggio per la sicurezza e le prestazioni dei sistemi IT (in particolare, il sistema di logging sul NAS traccia le azioni sui singoli file); questi dati non sono raccolti per valutare il personale.

Solo quando si rendesse necessario per tutelare l'azienda, i dati potrebbero essere analizzati per raccogliere prove di abusi e ciò solo in modo puntuale, limitato nel tempo e con ambiti precisi.

Le finalità sopra riportate sono necessarie per adempiere a obblighi normativi o per garantire la sicurezza dei beni di Selexi o dei clienti.

16 Sanzioni disciplinari

In caso di mancata osservanza di questo regolamento e delle procedure applicabili, si applicano le sanzioni previste da:

- contratti nel caso di fornitori;
- CCNL, nel caso di dipendenti.

17 Storia delle modifiche

DATA	MODIFICHE APPORTATE
Maggio 2018	Prima emissione.
Novembre 2021	Migliorati alcuni paragrafi (p.e. gestione degli incidenti) su richiesta di Regione Lombardia.
Ottobre 2022	Tolta la politica perché integrata con le altre (qualità, ambiente).
Aprile 2023	Tolta la procedura di gestione degli incidenti perché creata procedura apposita Fatto riferimento alla procedura P-13 Gestione della comunicazione per la parità di genere ed alla procedura P-11 Gestione Ambientale.