Istruzioni Generali per il Trattamento dei Dati Personali

INDICE

1. SCOPO

In questo allegato vengono descritte le modalità operative generali adottate dalla scrivente Società, in qualità di Titolare del Trattamento, nell'ambito dell'applicazione delle misure adeguate alla protezione della sicurezza delle aree, dei dati e delle trasmissioni, al fine di ridurre al minimo i rischi di trattamento, dei dati personali degli Interessati, non in conformità alle norme di Legge.

2. APPLICABILITÀ

Le istruzioni contenute nel presente documento devono essere eseguite da tutti i destinatari della scrivente Società, al fine di limitare i rischi generali connessi a qualunque attività di trattamento dei dati personali affidati alla medesima dagli interessati.

3. RIFERIMENTI NORMATIVI

Articolo	*Norma*
Art.29	Regolamento UE 2016/679
Art. 32, par. 4	Regolamento UE 2016/679

4. RESPONSABILITÀ

Il Titolare è responsabile dell'individuazione e dell'adozione delle misure di seguito ri-portate. Il Titolare si avvale dei Responsabili e dell'RPD per l'attuazione delle presenti istruzioni generali qualora vengano nominati tali organi. Responsabili ed Incaricati sono tenuti all'applicazione delle istruzioni operative di seguito riportate.

5. DEFINIZIONI

Acronimo	*Definizione*
SIA	Servizio Sistemi Informativi della scrivente Società
RPD	Responsabile della Protezione dei Dati

6. TRATTAMENTI DI DATI PERSONALI EFFETTUATI CON STRUMENTI ELETTRONICI

6.1. Accesso ai dati attraverso i sistemi informatici aziendali

Per svolgere la propria attività lavorativa la scrivente Società ha affidato al proprio Responsabile/Incaricato un personal computer (fisso o mobile) ed i relativi programmi/applicazioni. Essi sono strumenti di lavoro e, pertanto, devono essere:

a) utilizzati solo per scopi inerenti alle mansioni lavorative attribuite;

b) custoditi in modo appropriato;

c) utilizzati, se non previsto diversamente, in modo esclusivo da un solo utente;

d) configurati in modo che sia presente esclusivamente software fornito/approvato dalla scrivente Società;

e) coerenti ai requisititi hardware e software definiti dal SIA in relazione alle finalità aziendali.

Sulla base di quanto sopra detto i Responsabili e gli Incaricati che accedono a dati personali in formato elettronico devono adottare le seguenti cautele:

a) utilizzare una password di accesso alle risorse di rete insieme alla propria user-id;

b) non lasciare incustodito la postazione di lavoro senza prima aver bloccato l'account;

c) segnalare prontamente il furto, il danneggiamento o lo smarrimento di tali strumenti.

Non è consentito:

a) modificare le configurazioni impostate secondo gli standard della scrivente Società sul PC in uso senza la preventiva autorizzazione del SIA;

b) installare sul PC software privo di licenza, non relativo alla propria attività o pericoloso;

c) installare sul PC mezzi di comunicazione propri (ad es. chiavette UMTS, Wi-Fi, 3G, ecc.);

d) ascoltare programmi, file audio o musicali, se non a fini prettamente lavorativi.

6.2. Gestione delle password

Per una corretta gestione delle password ciascun Responsabile o Incaricato deve avere cura di:

a) modificare la password al primo login;

b) utilizzare password di almeno 8 caratteri;

c) non basare la password su informazioni facilmente deducibili, quali il proprio nome, il nome dei familiari, la data di nascita, il proprio codice fiscale e numero di matricola ovvero il nome dalla scrivente Società;

d) mantenere la password riservata non rivelandola a nessuno;

e) non trascrivere la password su fogli, agendine, post-it facilmente accessibili a terzi;

f) sostituire la password almeno una volta ogni 90 giorni, qualora non indicato diversamente dal SIA;

g) in caso di modifica della password non utilizzare le precedenti 5;

h) non includere la password in alcun processo di connessione automatica;

i) nel caso in cui una password perda di segretezza, provvedere alla sua immediata sostituzione. Quando questo non risulti possibile, deve comunicare tale circostanza al SIA che provvederà alla sostituzione della stessa.

È opportuno che il Responsabile e l'Incaricato sappiano che:

a) è opportuno che il salva schermo venga impostato in modo che si attivi automaticamente dopo circa 15 minuti di inattività;

b) in caso di mancato utilizzo per un periodo superiore a sei mesi la user-id è disabilitata;

c) in caso di revoca/esclusione dall'incarico che consentiva l'accesso all'elaboratore o all'applicazione, la user-id è resa immediatamente inattiva a seguito di pronta comunicazione al SIA;

d) in caso di prolungata assenza o impedimento del Responsabile o dell'Incaricato, qualora fosse indispensabile e indifferibile intervenire per garantire la disponibilità dei dati personali il personale del SIA, su indicazione del Titolare, potrà accedere alla postazione di lavoro affidata per mantenere la necessaria operatività e sicurezza del sistema attraverso una forzatura e riassetto della relativa password di accesso. Al suo rientro, al Responsabile o all'Incaricato verrà assegnata una nuova password.

6.3. Antivirus

Il virus informatico è un programma non autorizzato che si insedia nel computer causando danni alle informazioni in esso contenute ovvero all'apparecchio stesso, impedendone l'utilizzo. I virus possono trasmettersi tramite download di file da Internet, messaggi di posta elettronica, chiavette USB.

Tutti i server e i PC client collegati alla rete della scrivente Società sono protetti da software antivirus in grado di intercettare i virus informatici.

È responsabilità del SIA implementare e garantire il corretto funzionamento delle procedure necessarie per il download e la distribuzione degli aggiornamenti a tutti i server e client

della rete aziendale. L'aggiornamento del software antivirus ha luogo attraverso un processo automatico su tutti i server e client "attivi" collegati alla rete aziendale.

Al fine di evitare possibili danneggiamenti dovuti all'introduzione nel sistema informativo dalla scrivente Società di programmi contenenti virus, è necessaria l'adozione di alcune misure di sicurezza.

Per questi motivi il Responsabile e l' Incaricato debbono:

a) evitare di introdurre applicazioni/software che non siano state preventivamente approvate dal SIA;

b) verificare con frequenza giornaliera la versione e la data dell'ultimo aggiornamento del software antivirus;

c) non aprire mai allegati provenienti da un indirizzo di posta elettronica sconosciuto o su cui si sia in dubbio. In questo caso occorre spostare il messaggio nel cestino e svuotare quest'ultimo;

d) prestare sempre debita attenzione agli eventuali messaggi di segnalazione di virus e, in caso di anomalie, contattare immediatamente il SIA.

6.4. Supporti informatici rimovibili per la memorizzazione dei dati

I supporti informatici rimovibili quali CD-ROM, chiavette USB, flash memory utilizzati per la memorizzazione di dati personali devono essere custoditi con diligenza in modo che siano evitati accessi non autorizzati e trattamenti non consentiti.

I supporti rimovibili contenenti dati sensibili devono essere distrutti o resi inutilizzabili quando non sono più utilizzabili, ovvero possono essere riutilizzati da altri Responsabili o Incaricati, non autorizzati al trattamento degli stessi dati, solo se le informazioni precedentemente in essi contenute non sono intellegibili e tecnicamente in alcun modo ricostruibili.

6.5. Backup dei dati

Il backup dei dati, ovvero il loro salvataggio periodico, è importante misura di protezione delle informazioni, a completa cura del SIA. In quest'ottica è di fondamentale importanza che il Responsabile e l'Incaricato posizionino i dati aziendalmente rilevanti ed a maggior ragione quelli personali degli Interessati, sulle cartelle di rete indicate dal SIA all'atto della consegna delle credenziali di accesso al proprio PC.

6.6. Comunicazione Elettronica (E-mail, Instant Messaging, Live Meeting, ecc.)

Nel precisare che anche la posta elettronica e tutti gli altri strumenti di comunicazione elettronica sono strumento di lavoro, si segnala che:

a) che Le è stato assegnato un account di posta elettronica con dominio dalla scrivente Società;
b) di non utilizzare sistemi di posta elettronica al di fuori di quelli dalla scrivente Società dei quali non può conoscere il livello di protezione;
c) di utilizzare l'indirizzo di posta elettronica aziendale solo per scopi lavorativi.

Pertanto:

a) non è consentito inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
b) non è consentito partecipare a newsgroup, forum o mailing list non attinenti all'attività lavorativa;
c) è bene sapere che i messaggi di posta elettronica sono intercettabili e possono essere utilizzati a favore di una delle parti in caso di diverbio.
d) l'uso della mail o dei messaggi vocali di un altro utente è proibito a meno che sia necessario e giustificato ma richiede l'avvertimento, e l'autorizzazione da parte dell'utente interessato;
e) non inviare, ove possibile, per posta elettronica documenti od informazioni "Strettamente riservati o confidenziali" dal momento che la posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da terzi;
f) nel caso in cui debbano essere inviati per posta elettronica documenti/informazioni contenenti dati sensibili (ai sensi del Reg. UE 2016/679) occorre contattare il SIA in maniera che tali dati possano preventivamente essere criptati e/o protetti da password;
g) si eviti, quando si risponde ad una e-mail, di replicare in copia a tutti i destinatari in origine indicati, ove ciò non sia indispensabile.

6.7. Internet

Nel precisare che anche l'uso di Internet deve avvenire nell'ambito e per lo svolgimento delle mansioni lavorative, secondo i principi di correttezza, diligenza, buona fede, è vietato l'uso di Internet a fini personali ed in particolare l'accesso a qualsiasi sito osceno o pornografico.

Per queste ragioni è vietato inoltre:

a) ogni forma di registrazione a siti i cui contenuti non siano pertinenti all'attività lavorativa;

b) la partecipazione, per motivi non professionali, a newsgroup, forum, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);

c) la memorizzazione e la trasmissione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

d) l'utilizzo di sistemi aziendali per scaricare o distribuire software pirata;

e) imputare dati su pagine WEB (c.d. "form") se non per fine strettamente lavorativi;

f) fare uso di cloud storage (es. "Dropbox", "Google Drive", "Microsoft OneDrive") senza una specifica autorizzazione del SIA.

Lo scarico di software gratuiti (freeware) e shareware prelevati da siti Internet è riservato al personale del SIA. Pertanto nel caso fosse necessario l'utilizzo di tali programmi occorre chiedere l'autorizzazione preventiva al suindicato Servizio.

6.8. Protezione dei dispositivi portatili (notebook, smartphone, tablet)

I Responsabili e gli Incaricati che hanno in dotazione dispositivi portatili devono osservare le seguenti regole:

a) non lasciarli mai incustoditi;

b) durante la guida assicurarsi che le porte dell'auto siano chiuse e comunque non lasciarli mai in vista;

c) limitarne l'utilizzo alle attività strettamente necessarie alle mansioni lavorative attribuite;

d) operare in locali, o in condizioni tali da garantire sempre la riservatezza delle informazioni visibili sul display;

e) effettuare il backup dei dati almeno una volta la settimana secondo le specifiche istruzioni date dal SIA alla consegna del dispositivo;

f) effettuare il download degli aggiornamenti del programma antivirus secondo le istruzioni ricevute dal SIA alla consegna del dispositivo;

g) verificare con frequenza giornaliera la versione e la data dell'ultimo aggiornamento del software antivirus.

6.9. Installazione di apparecchiature sulla rete

L'installazione di nuovi server, PC, software e materiale di natura informatica in genere deve essere giustificata da una chiara necessità e deve essere preventivamente approvata. Il personale dalla scrivente Società è tenuto a fornire, per via gerarchica, tutte le informazioni relative a questi asset con l'indicazione della tipologia di utilizzo delle apparecchiature e del tipo di informazioni che saranno gestite.

7. TRATTAMENTI DI DATI PERSONALI CONTENUTI IN DOCUMENTI ED ARCHIVI CARTACEI

La scrivente Società ha messo a disposizione degli Incaricati dei luoghi sicuri (armadi/cassetti chiusi a chiave, locali archivio) ove custodire i documenti contenenti dati personali.

Ciascun Responsabile/Incaricato deve quindi adottare le seguenti cautele:

a) asportare i documenti da tali luoghi sicuri solo qualora necessario e per il tempo strettamente indispensabile per effettuare le operazioni di trattamento e, in questo caso controllarli e custodirli con la massima diligenza;

b) ove possibile asportare solo i documenti necessari per le operazioni di trattamento e non le intere pratiche;

c) al termine delle operazioni di trattamento riporre immediatamente i documenti;

d) controllare che i documenti composti da numerose pagine o più raccoglitori siano sempre completi, verificando sia il numero dei fogli che l'integrità del contenuto;

e) riporre i documenti nei luoghi sicuri al termine della giornata lavorativa;

f) qualora si debbano lasciare i documenti in ufficio al termine dell'orario di lavoro, occorre individuare un luogo sicuro ove riporli, che fornisca idonee garanzie di sicurezza;

g) i documenti non devono essere mai lasciati incustoditi sulla scrivania durante il giorno e occorre verificare che, in caso di allontanamento anche temporaneo dalla propria postazione di lavoro, non vi sia possibilità, da parte di colleghi non autorizzati o di terzi, di accedere ai dati personali per i quali sia in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato;

h) assicurarsi che gli atti e i documenti cartacei non siano suscettibili di indebita e non autorizzata visione durante l'accesso agli uffici da parte di terzi estranei alla scrivente Società (es. visitatori, consulenti, dipendenti di società esterne, addetti alle pulizie,

ecc.); in quest'ottica, è importante limitare l'accesso e la permanenza dei suindicati soggetti e, laddove necessario, vigilare sugli stessi;

i) riporre analoga cautela ed attenzione allorquando si trattino i dati in maniera non documentale ovvero durante colloqui orali o durante l'uso dell'apparecchio telefonico (fisso o mobile); a tal proposito s'invita ad assumere un timbro di voce adatto alla criticità del dato personale trattato;

j) occorre limitare al massimo il numero delle stampe o fotocopie effettuate. Una volta effettuate le medesime debbono essere immediatamente prese in carico da chi le ha prodotte evitando che restino incustodite;

k) i documenti sottoposti a scannerizzazione debbono essere immediatamente riposti nei fascicoli di competenza;

l) in caso di spedizione utilizzare modalità che garantiscano la prova dell'avvenuto ricevimento da parte del destinatario e della loro integrità;

m) occorre presidiare quanto spedito o ricevuto via fax, riponendo i correlati documenti negli appositi fascicoli, rispettivamente, di origine o di "distribuzione posta interna" in modo tale che giungano a chi di dovere;

n) eventuali stampe o fotocopie non riuscite, appunti o bozze in genere, devono essere distrutte con le apposte macchine distruggitrici, se disponibili, altrimenti devono essere ridotte in pezzi tali da non permettere di ricostruirne il contenuto;

o) non utilizzare stampe o fotocopie non riuscite come carta per appunti nonché, per lo stesso fine, trasportarle all'esterno dalla scrivente Società;

p) conservare i documenti per il tempo necessario per adempiere ad obblighi di legge e/o alle finalità di trattamento perseguite dalla scrivente Società trascorso il quale essi devono essere distrutti con le modalità decise dal Titolare.

Il Responsabile/l'Incaricato in caso di trasporto dei documenti al di fuori della scrivente Società deve:

a) tenere sempre con sé la cartella o la borsa contenente i documenti e ove possibile, evitare che sia visibile da terzi anche soltanto la prima pagina o la copertina dei documenti;

b) non lasciare mai incustodite la cartella o la borsa durante il trasporto e, se possibile, chiuderle a chiave o azionare le serrature a combinazione.

Infine, è vietato:

a) effettuare copie fotostatiche o di qualsiasi altra natura di documenti, atti, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante dati personali oggetto del trattamento per fini estranei all'attività lavorativa;

b) diffondere dati personali o comunicarli a terzi.

8. ALLEGATI