ISTRUZIONI GENERALI AI SOGGETTI AUTORIZZATI PER ATTIVITÀ DI TRATTAMENTO DATI

1. Regole generali

I Soggetti Autorizzati (cioè gli utenti) sono chiamati ad attenersi alle seguenti regole di ordinaria diligenza, che costituiscono il regolamento (Regolamento), nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto previsto in materia di tutela dei dati personali. In particolare:

- devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento delle finalità stabilite dall'Azienda, evitando di compiere operazioni non autorizzate;
- tutte le operazioni di trattamento dovranno essere svolte garantendo il rispetto di misure di sicurezza e massima riservatezza;
- in caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro si devono porre in essere tutte le misure necessarie (es. blocco del pc, chiusura del fascicolo cartaceo) affinché soggetti terzi, anche se dipendenti, non possano accedere ai dati personali sia per trattamenti automatizzati che cartacei;
- deve essere costantemente verificata esattezza e pertinenza dei dati, rispetto alle finalità previste;

Si richiede il massimo scrupolo nelle varie fasi di trattamento (raccolta, aggiornamento, conservazione e distruzione), soprattutto quando vengono trattate categorie particolari di dati personali (ad esempio: dati sensibili), dati giudiziari (ad esempio: fedina penale) o altri dati che possono avere un impatto negativo sulle libertà o i diritti delle persone. Tali dati devono essere trattati secondo il principio della minimizzazione del trattamento: riducendone all'essenziale il loro utilizzo (evitare di salvare/stampare documenti non necessari all'attività lavorativa). I Soggetti Autorizzati a trattare categorie particolari di dati riceveranno specifiche istruzioni operative su come gestire i dati trattati con mezzi automatizzati (ad esempio: file) e non automatizzati (ad esempio: archivi cartacei).

Nei successivi paragrafi si riportano le norme che gli Soggetti Autorizzati devono adottare nel caso di trattamenti effettuati in formato elettronico e cartaceo.

2. Postazioni

La postazione di lavoro deve essere:

- Utilizzata solo per scopi legati alla propria attività lavorativa;
- Utilizzata in modo esclusivo da un solo Soggetto Autorizzato, salvo non sia predisposta per la multiutenza (con apposite password);
- Protetta, evitando che soggetti non autorizzati possano avere visibilità dei dati trattati.

Il Soggetto Autorizzato deve attenersi alle seguenti procedure:

- Non utilizzare in Azienda risorse informatiche private (ad esempio: elaboratore, periferiche, token);
- Non installare alcun software sugli strumenti Aziendali;
- Non lasciare sulla scrivania informazioni riservate o dati personali su qualunque supporto esse siano archiviate (per esempio, carta, CD, dispositivi USB);
- In caso di assenza momentanea bloccare il sistema operativo del proprio elaboratore o, in alternativa, e, in ogni caso, impostare lo screen saver con password in modo che si attivi dopo 5 minuti di inattività;
- Non lasciare elaboratore, cellulare, tablet ed altri device incustoditi;
- Non utilizzare fax e/o telefono per trasmettere dati personali se non si è assolutamente certi dell'identità del destinatario.

3. Password

Ogni Soggetto Autorizzato deve gestire la propria password come segue, fatte salve diverse prassi aziendali:

- modificare, alla prima connessione, quella che è stata attribuita di default;
- modificarla almeno ogni 90 giorni, o immediatamente nei casi in cui sia compromessa;
- comporla utilizzando almeno 8 caratteri o, nel caso in cui lo strumento elettronico non lo consenta, con un numero di caratteri pari al massimo consentito;
- usare sia lettere che numeri e almeno un carattere maiuscolo;
- non basare la scelta su informazioni facilmente ricollegabili alla propria persona, ad esempio, il nome proprio o quello dei familiari, date di nascita, indirizzi;
- mantenerla strettamente riservata e non divulgarla a terzi;
- non permettere ad altri utenti (ad esempio: colleghi, collaboratori, fornitori) di operare con le proprie credenziali;
- non trascriverla in posti facilmente accessibili a terzi (ad esempio: post-it, scrivania), né lasciarla memorizzata sul proprio elaboratore;
- non comunicarla mai per telefono o via e-mail in chiaro, salvo gravi necessità.

4. Antivirus

Gli strumenti assegnati agli utenti sono protetti da antivirus ma rimangono potenzialmente esposti ad aggressioni di software non conosciuti o di comportamenti inavveduti degli utenti.

Per ridurre le probabilità del verificarsi di tali attacchi è necessario che vengano osservate le seguenti regole:

- controllare che il programma antivirus installato sia aggiornato periodicamente e sia attivo;
- chiudere correttamente i programmi in uso;
- non aprire file provenienti da fonti sospette ed analizzare gli allegati e-mail con attenzione prima di procedere alla loro apertura;
- non scaricare o installare applicazioni/software in assenza di preventiva autorizzazione;
- verificare tramite appositi applicativi in dotazione ogni supporto magnetico contenente dati (ad esempio, dispositivi USB, CD), prima dell'esecuzione dei file in esso contenuti;
- non utilizzare supporti di dubbia provenienza;
- porre attenzione ai messaggi di errore del proprio elaboratore;
- usare correttamente e solo per esigenze di lavoro i servizi di posta elettronica e Internet;
- non modificare le impostazioni del proprio elaboratore;
- spegnere il proprio elaboratore al termine della prestazione, prima di lasciare l'Azienda.

Se viene segnalato o si verifica un malfunzionamento dell'elaboratore, che possa far sorgere il sospetto della presenza di un virus, il Soggetto Autorizzato, senza ritardo, deve:

1. sospendere ogni operazione sull'elaboratore e prendere velocemente nota dell'eventuale messaggio di errore;

2. spegnere l'elaboratore;
3. contattare immediatamente l'Amministratore di Sistema.

5. Salvataggio dati

Tutti i dati al termine della giornata lavorativa vanno salvati conformemente alle prassi aziendali.

6. Dispositivi portatili

Un dispositivo portatile (ad esempio: elaboratore portatile, tablet, cellulare) è estremamente vulnerabile. Fermo quanto sopra, il Soggetto Autorizzato è tenuto a:

- conservare lo strumento in un luogo sicuro;
- non lasciare il dispositivo incustodito;
- avvertire tempestivamente l'Amministratore di Sistema in caso di furto o compromissione del dispositivo;
- fare attenzione all'uso del dispositivo in pubblico (dati password potrebbero essere carpiti da terzi).

7. Internet e posta

Internet, posta elettronica e gli altri sistemi di messaggistica devono essere utilizzati esclusivamente per finalità lavorative.

In particolare, il Soggetto Autorizzato è obbligato ad osservare le seguenti regole:

1. la navigazione in internet è possibile solo per l'esecuzione dei compiti assegnati, altrimenti è espressamente vietata;
2. non è consentito scaricare software, anche se ne è nota la fonte;
3. salvo ciò non rientri nei compiti assegnati, non è consentita l'interazione con social network, gruppi di discussione, chat, sistemi di messaging o assimilati;
4. è vietato aprire e-mail e file allegati anomali o di origine sconosciuta (ad esempio: spam o simili).

Si consideri che posta elettronica, sistemi di instant messaging, navigazione internet veicolano anche software malevoli (virus), che possono creare gravi danni in Azienda;

5. è vietato l'utilizzo della posta elettronica per comunicare informazioni riservate, dati personali,

senza garantirne l'opportuna protezione;

6. fare attenzione ai destinatari della comunicazione inviando dati personali solo a chi ha titolo per trattarli. In caso di errore avvertire immediatamente il soggetto che ha ricevuto la comunicazione richiedendo di cancellare il messaggio e relativi allegati;
7. è vietato modificare le impostazioni del proprio dispositivo od installare dispositivi di memorizzazione, comunicazione o dispositivi non autorizzati preventivamente dall'Amministratore di Sistema;
8. per migliorare l'efficienza dei sistemi è necessario cancellare messaggi e documenti inutili o al-

legati pesanti, se non necessari (o non collegati con l'attività lavorativa), verificando se la propria casella ha superato i limiti di capienza;

9. In caso di assenza programmata il Soggetto Autorizzato deve attivare la procedura che consente

di avvertire i mittenti di messaggi di posta elettronica della sua assenza e di comunicare i recapiti di un collega presente ("Out of Office").

8. Archivi cartacei

I fascicoli ed i documenti che contengono dati personali non deve essere lasciato incustodito nella postazione di lavoro e, terminata la prestazione, devono essere conservati in un luogo sicuro. Inoltre, il Soggetto Autorizzato non deve consentirne l'accesso a terzi (colleghi compresi, se non coinvolti in tale attività) anche quando il fascicolo o documento è in lavorazione.
In caso di trattamento categorie particolari di dati (stati di salute, iscrizione a sindacati), dati giudiziari, etc., tutta la documentazione cartacea deve essere conservata in armadi/cassetti chiusi a chiave o stanze chiuse a chiave in caso di allontanamento, anche temporaneo, dalla postazione di lavoro.
L'accesso a tutti i locali Aziendali deve essere consentito solo a personale preventivamente autorizzato dall'Azienda.
I documenti contenenti dati personali, se duplicati per errore, devono essere eliminati mediante apposita macchina "distruggi documenti" o con qualunque altro mezzo che ne renda impossibile la ricostruzione.

9. Accesso ai dati del Soggetto Autorizzato

L'Amministratore di Sistema è abilitato ad accedere ai dati trattati dal Soggetto Autorizzato tramite posta elettronica o navigazione in rete esclusivamente per motivi di sicurezza e protezione del sistema informatico in caso di necessità (ad esempio: virus, spyware, malware, intrusioni telematiche, spam, phishing), ovvero per motivi tecnici e/o di regolare svolgimento dell'attività Aziendale (ad esempio: gestione software o hardware). Fatta eccezione per gli interventi urgenti che si rendano necessari per far fronte a situazioni di emergenza, il personale incaricato avrà accesso ai dati su richiesta del Soggetto Autorizzato e/o previo avviso al medesimo, sia fisicamente che da remoto. In quest'ultimo caso, il Soggetto Autorizzato avrà contezza dell'inizio dell'intervento e della sua fine, mediante appositi messaggi.
Lo stesso Amministratore di Sistema può, nei casi suindicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità dei sistemi informatici (ad es. verifica, disinstallazione file e software pericolosi).
L'Amministratore di Sistema, in caso di assenza improvvisa o prolungata del Soggetto Autorizzato o comunque, non programmata e per improrogabili necessità di sicurezza o di operatività del sistema è abilitato ad accedere alla posta elettronica del Soggetto Autorizzato per le strette necessità operative. Il Soggetto Autorizzato sarà avvertito di tale intervento.
L'Amministratore di Sistema può procedere a controlli sulla navigazione finalizzati a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, ad esempio mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta.
L'eventuale controllo sui file di log da parte dell'Amministratore di Sistema non è comunque continuativo ed è limitato ad alcune informazioni per esempio (i) per la posta elettronica: indirizzo del mittente/destinatario, data e ora di invio/ricezione ed oggetto; (ii) per la navigazione Internet: nome del Soggetto Autorizzato, identificativo del device, indirizzo IP, data/ora di navigazione, siti visitati e totale accessi effettuati ed i file stessi vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'Azienda, e comunque non oltre 12 mesi, fatti salvi in ogni caso specifici obblighi di legge.
Il sistema di registrazione dei log è configurato per cancellare periodicamente ed automaticamente (at-

traverso procedure di sovra registrazione) i dati personali degli utenti relativi agli accessi internet e al traffico telematico.
L'Amministratore di Sistema è altresì abilitato ad accedere ai dati contenuti negli strumenti informatici restituiti dal Soggetto Autorizzato all'Azienda per cessazione del rapporto, sostituzione delle apparecchiature, etc.
Sarà cura del Soggetto Autorizzato la cancellazione preventiva di tutti gli eventuali dati personali eventualmente ivi contenuti.
In ogni caso, l'Azienda garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza.

A tale proposito si sottolinea che la strumentazione tecnologica/informatica e quanto con essa creato è di proprietà dell'Azienda in quanto mezzo di lavoro. È vietato l'uso di tutti i sistemi Aziendali per finalità ed interessi diversi da quelli Aziendali.
Le verifiche sugli strumenti informatici saranno realizzati dall'Azienda nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti e del presente Regolamento.
In caso di anomalie, l'Azienda, per quanto possibile, privilegerà preliminari controlli anonimi e quindi riferiti a dati aggregati nell'ambito di intere strutture lavorative o di sue aree nelle quali si è verificata l'anomalia.
In tali casi verrà emesso un avviso generico a tutte le strutture coinvolte.
In caso di successive, perduranti anomalie, ovvero ravvisandone comunque la necessità, l'Azienda si riserva di effettuare verifiche anche su base individuale, comunque finalizzate esclusivamente alla individuazione di eventuali condotte illecite.
In nessun caso verranno realizzate verifiche prolungate, costanti o indiscriminate, fatte salve le verifiche atte a tutelare gli interessi Aziendali.

10. Sanzioni Il Soggetto Autorizzato al fine di non esporre se stesso e l'Azienda al rischio di sanzioni è tenuto ad adottare comportamenti conformi alla normativa vigente es alla regolamentazione aziendale.
Gli utenti sono responsabili del corretto utilizzo degli strumenti e servizi aziendali.

Il Soggetto Autorizzato è responsabile per i danni cagionati all'Azienda ed ai terzi, a causa della sua condotta.
Tutti gli utenti sono pertanto tenuti ad osservare e a far osservare le disposizioni contenute nel presente Regolamento il cui mancato rispetto o la cui violazione, costituendo inadempimento contrattuale potrà comportare:
- per il personale dipendente provvedimenti di natura disciplinare, anche previsti dalla contrattazione collettiva, oltre alle azioni civili e penali stabilite dalla legge;
- per i collaboratori esterni la risoluzione del contratto, oltre alle azioni civili e penali stabilite dalla legge.

Il presente Regolamento è stato predisposto dall'Azienda, Titolare del trattamento, ed è sottoscritto dal Soggetto Autorizzato, al quale ne è consegnata una copia, per presa visione ed accettazione del suo contenuto.

Dello, 11/04/2024