CARTA INTESTATA DELLA SOCIETA'

Parte A – NOMINA DELLE PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI PERSONALI DI (inserire denominazione società)

Ai sensi e per gli effetti del
Regolamento UE 2016/679 "sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati"

Le persone che nello svolgimento della propria attività all'interno di (inserire denominazione società) trattano dati personali degli interessati sono autorizzate al trattamento dei dati personali, ai sensi e per gli effetti degli artt. 28 e 29 del Regolamento UE n. 679/2016. In base a tale incarico, ciascuna persona autorizzata al trattamento dei dati è tenuta a rispettare le specifiche istruzioni impartite da (inserire denominazione società).

In particolare, in base agli obblighi di riservatezza e sicurezza imposti dalla normativa citata, sarà cura di ciascuna persona autorizzata di non diffondere o comunicare a terzi i dati trattati, se non nei casi consentiti dalle specifiche disposizioni di Legge e, comunque, in conformità alle norme e procedure interne, emanate dal Titolare e/o dal Responsabile del Trattamento dei dati di (inserire denominazione società).

I dati a cui le persone autorizzate possono accedere per effettuare i trattamenti (sia informatici che cartacei), sempre strettamente pertinenti alle mansioni svolte e per le finalità previste da (inserire denominazione società), rispettando i principi fondamentali sanciti dal Regolamento, sono relativi alle seguenti categorie di Interessati:

- Personale di terra e personale di bordo (se applicabile) relativamente alle seguenti finalità di trattamento:
  - Gestione interna del personale.
- Candidati relativamente alle seguenti finalità di trattamento:
  - Selezione e valutazione del personale.
- Clienti relativamente alle seguenti finalità di trattamento:
  - Gestione amministrativa dei contratti.
- Fornitori relativamente alle seguenti finalità di trattamento:
  - Selezione e valutazione dei fornitori.
  - Gestione amministrativa dei contratti.

- Membri degli Organi ed organismi interni relativamente alle seguenti finalità di trattamento:
    - Valutazione dei profili professionali.
    - Gestione amministrativa dei contratti in essere.
- Visitatori relativamente alle seguenti finalità di trattamento:
    - Espletamento delle procedure di ingresso.
    - Accesso ai servizi Internet per gli ospiti.
    - Sicurezza.

In particolare, ogni persona autorizzata dovrà avere cura che:

- i metodi di trattamento siano conformi alle regole stabilite dal Regolamento;
- siano mantenute tutte le misure necessarie per evitare l'aumento dei rischi di distruzione o perdita di dati, di accesso non autorizzato o di elaborazione non consentita o di trattamento diverso dagli scopi della raccolta;
- la comunicazione di dati personali sia evitata al di fuori delle ipotesi e modalità consentite dal Regolamento; in particolare, i dati personali non devono essere comunicati a terzi o, in ogni caso, a soggetti che non possono essere identificati con certezza come aventi diritto;
- categorie speciali di dati, come definito dall'art. 9 del Regolamento, siano soggetti a trattamento solo con il consenso esplicito dell'interessato e nel rispetto rigoroso e tempestivo del Regolamento;
- qualsiasi altra disposizione legislativa o regolamentare in materia sia comunque rispettata.

Ciascuna persona autorizzata è inoltre tenuta a rispettare le procedure relative alle misure di sicurezza prescritte dalla Società, incluse le istruzioni riportate nella Parte B di questo documento.

Il TITOLARE DEL TRATTAMENTO
(inserire denominazione società)

_____

Firma per ricevuta e accettazione
La persona autorizzata al trattamento dei dati personali

_____

Data _____

Parte B – ISTRUZIONI OPERATIVE ALLA PERSONA AUTORIZZATA AL TRATTAMENTO DEI DATI PERSONALI

1. PREMESSA

Il Regolamento UE 2016/679 sulla "*Protezione delle persone fisiche con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati*" al fine di garantire che il trattamento sia effettuato nel rispetto dei diritti degli interessati, prevede che il Titolare e i Responsabili del trattamento dei dati debbano impartire istruzioni operative specifiche alle persone che, nell'esercizio delle loro mansioni, sono autorizzate a trattare dati personali, sia mediante sistemi informatici sia mediante documenti cartacei (art.28).

Queste istruzioni, così come altre misure di sicurezza, mirano a minimizzare i seguenti rischi:

- distruzione o perdita di dati personali, anche se accidentale;
- accesso non autorizzato;
- elaborazione non consentita o non conforme alle finalità di raccolta.

Di seguito sono riportate le principali regole che tutte le persone autorizzate al trattamento devono seguire nelle loro attività quotidiane e, soprattutto, quando riguardano la gestione dei dati personali.

2. DEFINIZIONI

Trattamento: qualsiasi operazione o insieme di operazioni eseguite su dati personali o su serie di dati personali, anche con strumenti automatizzati, quali raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o alterazione, reperimento, consultazione, uso, divulgazione mediante trasmissione, diffusione o altrimenti messa a disposizione, allineamento o combinazione, restrizione, cancellazione o distruzione.

Dato personale: qualsiasi informazione relativa a una persona fisica identificata o identificabile ("interessato"); una persona fisica identificabile è colui che può essere identificato, direttamente o indirettamente, in particolare facendo riferimento a un identificatore come un nome, un numero di identificazione, dati relativi all'ubicazione, un identificatore online o uno o più fattori specifici per l'aspetto fisico, fisiologico, identità genetica, mentale, economica, culturale o sociale di quella persona naturale.

Dato genetico: dato personale relativo alle caratteristiche genetiche ereditarie o acquisite di una persona fisica, che forniscono informazioni uniche sulla fisiologia o sulla salute di tale persona fisica e che risultano, in particolare, dall'analisi di un campione biologico dalla persona fisica in questione.

Dato biometrico: dato personale risultante da elaborazioni tecniche specifiche relative alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica, che consentono o confermano l'identificazione univoca di tale persona fisica, quali immagini facciali o dati dattiloscopici.

Dato relativo alla salute: dato personale relativo alla salute fisica o mentale di una persona fisica, compresa la fornitura di servizi di assistenza sanitaria, che rivelano informazioni sul suo stato di salute.

Titolare del trattamento dei dati: la persona fisica o giuridica, l'autorità pubblica, l'agenzia o altro organismo che, da solo o congiuntamente con altri, determina le finalità e i mezzi del trattamento di dati personali; se le finalità e i mezzi di tale trattamento sono determinati dalla legge dell'Unione o dello Stato membro, il responsabile del trattamento o i criteri specifici per la sua nomina possono essere previsti dalla legislazione dell'Unione o dello Stato membro.

Responsabile del trattamento dei dati: indica una persona fisica o giuridica, un'autorità pubblica, un'agenzia o altro ente che elabora i dati personali per conto del Titolare del trattamento.

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile.

Interessato: la persona fisica o giuridica, gli enti o le associazioni a cui si riferiscono i dati personali.

Comunicazione: dare conoscenza dei dati personali a uno o più soggetti specifici diversi dagli interessati, dal rappresentante del Titolare nel territorio dello Stato e dai responsabili del trattamento dei dati, in qualsiasi forma, anche mettendo a disposizione i dati o attraverso la consultazione degli stessi.

Dato anonimo: dato che originariamente o a causa dell'elaborazione non può essere associata a una persona identificata o identificabile.

Blocco: conservazione dei dati personali con sospensione temporanea di qualsiasi altra operazione di elaborazione.

3. TRATTAMENTO DEI DATI PERSONALI

3.1 CREAZIONE DI ARCHIVI INERENTI NUOVE CATEGORIE DI INCARICATI

Le persone autorizzate al trattamento dei dati possono gestire esclusivamente gli archivi di dati personali individuati nei rispettivi documenti di nomina. Ogni eventuale creazione o utilizzo di archivi riguardanti nuove categorie di interessati, nonché l'effettuazione di ulteriori trattamenti oltre a quelli già esistenti, dovrà essere preventivamente autorizzata dal *Responsabile del trattamento*.

3.2 AMBITO DI TRATTAMENTO CONSENTITO

Uno dei principali punti del Regolamento è quello che prevede che il trattamento dei dati personali sia reso noto all'interessato nei suoi elementi essenziali, e si svolga entro gli stessi limiti. In altri termini, una volta che l'interessato viene informato delle modalità del trattamento dei suoi dati personali, detta informativa costituisce il limite del trattamento stesso.

Ciascuna persona autorizzata al trattamento dei dati pertanto, oltre a individuare le operazioni di trattamento nella propria lettera di designazione, troverà ulteriori altre informazioni sui trattamenti a lui consentiti, conoscendo le informative che oralmente o per iscritto sono somministrate agli interessati. È chiaro che ogni persona autorizzata avrà cura di valutare con maggiore attenzione le informative che più direttamente riguardano la sua attività.

Una specifica attenzione va dedicata alle ipotesi di comunicazione o diffusione dei dati. In altri termini, ogni qual volta si prospetti l'eventualità di divulgare (in qualsiasi forma o modo) dati personali, è necessario procedere alle seguenti verifiche:

- verifica della legittimità della divulgazione alla luce della informativa fornita all'interessato;
- verifica di eventuali normative che consentano/rendano obbligatoria la divulgazione.

In relazione alle categorie di interessati per le quali è autorizzato il trattamento, è prevista la comunicazione dei dati stessi esclusivamente ai soggetti esterni indicati da (inserire denominazione società).

Ogni ipotesi diversa di comunicazione o, addirittura, di diffusione dei dati dovrà essere preventivamente autorizzata di volta in volta dal Titolare e/o dal Responsabile.

3.3 AGGIORNAMENTO ED ESATTEZZA DEI DATI

La persona autorizzata al trattamento dei dati deve prestare particolare attenzione all'esattezza dei dati trattati e provvedere, inoltre, all'aggiornamento degli stessi.

4. ISTRUZIONI PER IL TRATTAMENTO DI DATI CON L'AUSILIO DI STRUMENTI ELETTRONICI

Le persone autorizzate al trattamento dei dati, che a qualunque titolo accedono al sistema informativo della (inserire denominazione società), collegato o meno alla rete, o che custodisce qualsiasi dato personale di competenza di (inserire denominazione società) e non destinato alla diffusione, dovranno attenersi a quanto riportato di seguito. In particolare si evidenzia che:

- L'accesso a un qualunque tipo di trattamento di dati personali con strumenti elettronici è sempre subordinato al superamento di una procedura di autenticazione informatica che prevede l'inserimento da parte della persona autorizzata al trattamento dei dati personali di un proprio codice di identificazione (user name) e di una parola chiave (password) riservata e conosciuta solamente dalla medesima.
- Il successivo accesso a strumenti informatici necessari per il trattamento di dati personali per una corretta esecuzione del proprio incarico è garantito dalla configurazione sul proprio profilo di ulteriori livelli di credenziali di autenticazione.
- La parola chiave rappresenta la prima barriera in una strategia di accesso selettivo a dati personali, e pertanto una parola chiave selezionata con criteri non soddisfacenti può portare alla compromissione dell'intera rete informativa della (inserire denominazione società).

Per questa ragione ciascuna persona autorizzata al trattamento dei dati personali è responsabile della segretezza della parola chiave associata al proprio codice di identificazione e, pertanto, è tenuta ad assumere tutte le iniziative appropriate per garantire la sicurezza della stessa.

4.1 LINEE GUIDA PER LA COSTRUZIONE DELLE PAROLE CHIAVE

Per garantire il rispetto delle disposizioni di legge (inserire denominazione società) ha previsto password di accesso ai sistemi con lunghezza minima di 8 caratteri. E' stata inoltre impostata una scadenza delle password delle persone autorizzate al trattamento dei dati personali ogni 6 mesi per i dati personali comuni ed ogni 3 mesi per quelli sensibili.

Le Politiche della (inserire denominazione società) consigliate in merito alla scelta delle parole chiave prevedono:

- Password contenenti caratteri appartenenti a 3 delle 4 categorie seguenti: caratteri maiuscoli (A – Z), caratteri minuscoli (a – z), cifre in base 10 (0 – 9), caratteri non alfabetici (ad esempio !, $, #, o %) ;
- Non uguaglianza con il profilo utente;
- Password non facilmente riconducibili alla persona autorizzata al trattamento dei dati personali;
- Password note SOLO alla persona autorizzata al trattamento dei dati personali, scelte da quest'ultima al primo accesso al sistema.

Si riportano alcune indicazioni per aiutare nella scelta di password che possono considerarsi sicure:

<u>Parole chiave sicure</u>

Sono da ritenere parole chiave di soddisfacente sicurezza quelle che hanno le seguenti caratteristiche:

- Sono composte da caratteri maiuscoli e minuscoli.
- Utilizzano anche caratteri di interpunzione, come ; [,] , * " , ed una combinazione di numeri e lettere.
- Non devono rappresentare una parola in una qualsiasi lingua o dialetto sufficientemente diffuso.
- Non devono essere basate su informazioni personali, come nomi di membri della famiglia, date di nascita, anagrammi o combinazione di nomi e simili.
- Un altro importante accorgimento riguarda la selezione di parole chiave, che possano essere facilmente digitate sulla tastiera, senza doverla guardare, per ridurre al minimo il tempo di digitazione ed evitare che la digitazione possa essere osservata surrettiziamente da terzi nelle vicinanze.

<u>Parole chiave deboli</u>

Si sottolinea che le parole chiave di facile individuazione hanno le seguenti caratteristiche:

- La parola chiave si può trovare in un comune dizionario italiano, in inglese od altra lingua comune.

- La parola chiave è una parola di uso comune, come ad esempio il nome di qualche membro della famiglia, di animali da salotto, di amici, di collaboratori o di caratteri di fantasia.
- La parola chiave legata a espressioni informatiche, hardware e software, come pure quelle legate a date di nascita od altre informazioni personali, come l'indirizzo, il numero telefonico e simili.
- Le sequenze numeriche del tipo aaaaaaaa, bbbb, 121212, 123456 sono da scartare parole come sopra, digitate alla rovescia.
- Una qualsiasi delle parole chiave precedentemente indicata come debole, preceduta o seguita da una cifra come ad esempio giovanni1, oppure 1giovanni.

Raccomandazioni per la protezione della parola chiave

- Non utilizzare la stessa parola chiave per sistemi di autenticazione interni a (inserire denominazione società) e per sistemi di autenticazione esterni, come ad esempio l'accesso al proprio conto corrente bancario ed altre attività, non legate all'attività istituzionale della (inserire denominazione società).
- Non condividere la parola chiave con alcun soggetto, interno o esterno a (inserire denominazione società), ivi inclusi i superiori, a qualsiasi livello.

Tutte le parole chiave che sono state generate dalla persona autorizzata al trattamento dei dati personali devono essere trattate come informazione strettamente riservata.

In particolare, ecco un elenco degli accorgimenti da adottare:

- Non rivelare una parola chiave attraverso il telefono a chicchessia.
- Non scrivere la parola chiave su un qualsiasi documento e non nasconderlo in alcuna parte dell'ufficio.
- Non archiviare la parola chiave in un qualsiasi tipo di sistema di elaborazione, incluso un telefono cellulare, un computer palmare e simile.
- Non scrivere una parola chiave in un messaggio di posta elettronica.
- Non parlare di parole chiave di fronte a terzi.
- Non dare alcuna indicazione in merito al formato e alla lunghezza della parola chiave utilizzata.
- Non rivelare la parola chiave a colleghi di lavoro, mentre si è in vacanza;
- Non utilizzare mai la caratteristica, offerta da parecchie applicazioni, di memorizzare la parola chiave.

Nel caso di operazioni sistemistiche che richiedano la vostra password (es: cambio del PC o installazione di programmi), i sistemisti o le persone autorizzate al trattamento dei dati personali dal Titolare/Responsabile del trattamento la cambieranno temporaneamente, dandovene comunicazione. Al primo utilizzo del PC è obbligatorio che modifichiate subito la password.

Se qualcuno insiste per conoscere la vostra parola chiave, dapprima fate riferimento a questo documento e successivamente informate immediatamente il vostro responsabile di riferimento.

Se avete anche solo il minimo sospetto che la vostra parola chiave sia stata in qualche modo compromessa o venuta a conoscenza di terzi, provvedete immediatamente alla sostituzione della parola chiave e riferite l'accaduto al vostro responsabile di riferimento.

Nel caso la persona autorizzata al trattamento dei dati personali abbia qualsiasi dubbio afferente alle modalità sicure di generazione, utilizzo e conservazione delle parole chiave, deve rivolgersi quanto prima possibile al responsabile dei sistemi informativi per ottenere opportuni chiarimenti ed istruzioni.

4.2 SESSIONI DI TRATTAMENTO INCUSTODITE

Si raccomanda di non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento di dati personali. In particolare, qualora sia necessario allontanarsi temporaneamente dal posto di lavoro, si ricorda che la pressione contemporanea dei tasti Ctrl + Alt + Canc attiva la finestra di "Protezione di Windows" dalla quale è possibile premere il pulsante "Blocca computer" per bloccare la stazione di lavoro senza la necessità di uscire dai programmi in uso. Una volta ritornati davanti alla propria postazione, per riprendere l'operatività è necessario seguire le istruzioni a video delle finestre di Windows premendo nuovamente i tasti Ctrl + Alt + Canc e inserendo la propria password.

Si ricorda che, per maggiore sicurezza, su ciascuna postazione di lavoro può essere configurato uno screen saver con password di sblocco che si attiva dopo n. minuti di inattività.

4.3 RACCOMANDAZIONI PER IL SALVATAGGIO DEI DATI IN RETE

Si ricorda che le uniche aree autorizzate al salvataggio di dati personali elaborati con gli strumenti di Office Automation (word, Excel, ecc), sono gli spazi riservati sul server. Tali spazi sono configurati al fine di garantire la sicurezza e la custodia dei dati, assicurando disponibilità degli stessi in caso di emergenza e sottoposti a backup.

In particolare i dati personali gestiti da ciascuna persona autorizzata al trattamento dei dati personali possono essere salvati nelle seguenti tipologie di cartelle di rete:

- Cartelle personali in cui ciascuna persona autorizzata al trattamento dei dati salva i propri documenti di lavoro.
- Cartelle condivise da tutte le persone autorizzate al trattamento dei dati personali all'interno delle quali vengono memorizzati dati relativi a progetti e/o attività comuni.

Ogni salvataggio in locale è fortemente sconsigliato ed è sotto la totale responsabilità della persona autorizzata al trattamento dei dati personali.

4.4 RACCOMANDAZIONI PER LA CUSTODIA, USO E DISTRUZIONE DI SUPPORTI RIMOVIBILI

In linea generale, non viene raccomandata la copia su supporti rimovibili (cd, chiavette USB, ecc.) di dati personali, per ridurre al minimo il rischio di perdita o distruzione anche accidentale dei dati stessi.

Ciò premesso, ove nello svolgimento della normale attività assegnata alla persona autorizzata al trattamento dei dati personali, nell'ambito del suo profilo di autorizzazione, sia indispensabile effettuare una copia di dati personali su supporti rimovibili, occorre attenersi alle seguenti cautele:

- Accertarsi che il supporto rimovibile sia debitamente formattato e privo di altri file, che potrebbero essere infetti. Nel dubbio, è sempre bene provvedere alla formattazione ex novo del supporto, prima di registrare dati personali.
- Contrassegnare il supporto rimovibile con un'etichetta, riportante l'indicazione in chiaro od in codice, tale da permettere alla persona autorizzata al trattamento dei dati personali di riconoscere immediatamente il contenuto del supporto in questione, ed evitare che egli possa confonderlo con altri supporti in suo possesso.

I supporti rimovibili contenenti dati personali devono essere sempre direttamente e personalmente custoditi della persona autorizzata al trattamento dei dati personali che ha realizzato la copia.

Qualora i dati contenuti su supporti rimovibili non abbiano più ragione di essere, si deve provvedere immediatamente alla loro formattazione.

Poiché i supporti rimovibili sono particolarmente sensibili ai campi magnetici, per evitare la cancellazione o danneggiamento anche accidentale dei dati, essi non devono mai essere avvicinati ad un campo magnetico, come ad esempio il magnete di un altoparlante, oppure lasciati abbandonati nelle vicinanze di un trasformatore, come i trasformatori utilizzati nelle lampade da tavolo, in quanto i campi dispersi potrebbero danneggiarne il contenuto.

Si faccia sempre attenzione a non dimenticare il supporto rimovibile all'interno del computer, quando, al termine della copia, si spegne il computer e ci si allontana.

Il supporto rimovibile contenente dati personali non deve mai essere lasciato abbandonato sul tavolo, ma deve essere immediatamente posto all'interno di una custodia sicura, quando non utilizzato; in funzione della criticità dei dati archiviati, si può andare da un cassetto della scrivania chiuso a chiave, sino ad un armadio blindato od una cassaforte, idonea alla custodia di supporti magnetici.

4.5 RACCOMANDAZIONI PER L'UTILIZZO DI HARDWARE E SOFTWARE

Il software installato in ciascuna macchina nonché la relativa configurazione hardware, rispecchiano la condizione necessaria e sufficiente per il consueto lavoro da svolgersi.

Qualora la persona autorizzata al trattamento dei dati personali ritenga necessario disporre di un nuovo software o di un aggiornamento hardware per le consuete mansioni, è necessario inoltrare una specifica richiesta al Responsabile dei Sistemi informativi il quale valuterà la stessa in accordo con il responsabile di riferimento.

È bene ricordare che ogni software, ad esclusione di quelli denominati freeware, ha una licenza e l'uso improprio di questa può portare a conseguenze civili.

4.6 INTERNET E POSTA ELETTRONICA

L'utilizzo di Internet e della posta elettronica sono resi disponibili dal Titolare del trattamento principalmente a scopo lavorativo, cioè al fine di ottemperare alle mansioni previste dal proprio ruolo. È necessario ricordare che l'utilizzo dell'e-mail può comportare dei rischi derivanti dalla possibile intercettazione della medesima e, quindi, i documenti in essa contenuti potrebbero essere letti e/o utilizzati da persone estranee al carteggio.

Nel momento in cui una e-mail viene stampata, assume tutte le caratteristiche di un documento cartaceo e la persona autorizzata al trattamento dei dati personali deve attenersi alle istruzioni in merito a questa tipologia di trattamento.

Il servizio e-mail è considerato da (inserire denominazione società) uno strumento di lavoro a tutti gli effetti, come il fax, il telefono e pertanto il dipendente deve farne un uso appropriato, che non esuli dal contesto lavorativo in cui opera; spedire e-mail personali non è vietato. Tale uso deve essere però circoscritto ad un numero di e-mail limitato oppure all'orario di pausa.

Relativamente alla connettività Internet, è vietato scaricare file di notevoli dimensioni (solitamente sono file musicali, film, video…) in quanto tale operazione comporta la saturazione della banda, rallentando chi utilizza Internet per la consultazione a scopo lavorativo. È vietato anche scaricare dalla Rete programmi eseguibili se non preventivamente autorizzati dal Responsabile dei Sistemi Informativi.

(inserire denominazione società) considera Internet uno strumento utile e proficuo se utilizzato nell'ambito professionale in cui la persona autorizzata al trattamento dei dati personali opera. Se dovessero emergere abusi nell'utilizzo del medesimo da parte di una persona autorizzata al trattamento dei dati personali, gli sarà negato l'accesso.

5. TRATTAMENTI NON AUTOMATIZZATI

5.1 GESTIONE QUOTIDIANA PRATICHE

Istruzioni per i dati personali in genere

- Le pratiche contenenti dati personali (di seguito: "le pratiche") devono essere di norma riposte in archivi chiusi. Si considera archivio chiuso anche il locale chiuso a chiave.
- Le pratiche sono prelevate, a cura delle persone autorizzate al trattamento dei dati personali, solo nella misura e per il tempo strettamente necessari per lo svolgimento dei relativi compiti, al termine dei quali - ed in ogni caso al termine della giornata/settimana lavorativa - sono riposte negli archivi. Ciascuna persona autorizzata al trattamento dei dati personali deve aver cura di verificare che le pratiche affidategli non restino incustodite, specie in contesti accessibili a soggetti non autorizzati al trattamento (aree di passaggio, sale d'attesa, sale riunioni, e via dicendo).

- Anche durante la giornata lavorativa, in caso di allontanamento dalla postazione di lavoro per un periodo di tempo significativo, le pratiche sono riposte negli archivi, salvo adeguata garanzia di controllo da parte di altre persone autorizzate ai medesimi trattamenti. In ogni caso le pratiche non devono essere mai lasciate incustodite sul tavolo durante il giorno.
- Lo smarrimento o il furto di informazioni deve essere comunicato immediatamente al proprio responsabile di riferimento.
- È buona regola evitare la proliferazione eccessiva di stampe e fotocopie di documenti contenenti dati personali. Le stampe e le fotocopie malriuscite debbono essere distrutte nell'apposito distruggi-documenti, se disponibile, oppure devono essere strappate in pezzi piccoli.

Istruzioni per i dati personali particolari e giudiziari

Oltre a quanto previsto per i dati personali in genere, le pratiche contenenti dati c.d. particolari o giudiziari sono conservate in archivi ad accesso controllato e sono controllate e custodite dalle persone autorizzate al trattamento dei dati personali fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione (ivi compresi altre persone autorizzate al trattamento dei dati personali che non siano autorizzate ad accedere alle informazioni sensibili), e sono restituite al termine delle operazioni affidate.

5.2 GESTIONE CHIAVI

Le persone autorizzate al trattamento dei dati personali chiamate a gestire le chiavi "fisiche" degli archivi devono:

- all'atto della consegna delle chiavi, verificarne subito il corretto funzionamento;
- verificare che le chiavi non restino inserite negli armadi/archivi di riferimento;
- conservare le chiavi in un luogo e con modalità che ne garantiscano una sicurezza adeguata anche al tipo di archivio;
- non metterle a disposizione né, se possibile, mostrarle ad estranei;
- in caso di smarrimento o sottrazione, farne immediata segnalazione al Referente e richiedere la sollecita sostituzione della serratura, spostando se del caso –per il tempo necessario- i documenti dall'archivio non protetto.

5.3 SCARTI DI ARCHIVIO

Gli scarti di archivio, ossia il periodico smaltimento di materiale cartaceo contenente dati personali, deve essere effettuato evitando che le informazioni personali, specie se sensibili, possano essere utilizzate da soggetti non autorizzati.

In particolare i dati particolari devono essere smaltiti mediante utilizzo degli appositi strumenti per la distruzione dei documenti, ove disponibili, oppure, in assenza di questi ultimi, i fogli contenenti dati particolari devono essere strappati in piccoli pezzi prima di essere cestinati.

5.4 USO DEL FAX

Se occorre inviare un fax contenente dati personali ad una persona autorizzata a visionarli, è necessario assicurarsi che la persona destinataria sia vicina al fax al momento della spedizione/ricevimento. Nel caso in cui l'invio del fax avviene al di fuori l'orario di lavoro è necessario che l'apparecchio del fax sia posto in un locale chiuso e accessibile solo dalla persona autorizzata al trattamento dei dati trasmessi.

5.5 TELEFONATE E COLLOQUI

Si raccomanda vivamente non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando cellulari all'esterno della (inserire denominazione società) o anche all'interno, in presenza di terzi non autorizzati, per evitare che dati personali possano venire a conoscenza di terzi non autorizzati, anche accidentalmente.