Privacy System
Consulenze e servizi integrati

Regolamento Europeo 2016/679

Istruzioni operative
e note comportamentali

Anno 2024

Indice degli argomenti:

Premessa

Il presente manuale è redatto ai sensi di quanto previsto dal Regolamento Europeo 2016/679.

Ai sensi di legge, si definisce "persona autorizzata al trattamento" la persona fisica - dipendente, collaboratore, professionista, ecc. - preposta a compiere operazioni di trattamento di dati personali di rilevanza aziendale (anche detta di seguito "incaricato" o "addetto").

Le presenti istruzioni devono considerarsi vincolanti ed inderogabili per tutti coloro che trattano dati personali.

Si evidenzia fin d'ora che il loro mancato rispetto potrà comportare in capo al singolo soggetto, l'insorgere di:

- responsabilità penale in caso di mancata adozione delle adeguate misure di sicurezza;
- responsabilità civile nei confronti dei terzi che venissero danneggiati per effetto di un non corretto trattamento dei dati;
- responsabilità contrattuale nei confronti del datore di lavoro.

Aggiornamenti periodici delle istruzioni

Le presenti istruzioni verranno aggiornate periodicamente per far fronte all'evoluzione normativa ed in particolare alle modifiche che saranno apportate dal legislatore europeo ed italiano, ai chiarimenti del Garante per la Privacy ed allo sviluppo tecnologico dei sistemi ed apparati informatici.

Sarà preciso dovere delle persone autorizzate al trattamento, fare sempre riferimento all'ultima versione delle istruzioni distribuite dall'azienda.

Referenti aziendali Privacy

Per qualunque esigenza pratica ed operativa, per richieste di chiarimenti sulle presenti istruzioni, per delucidazioni normative, per supporto tecnico hardware e software, per supporto a livello comportamentale, ecc., l'incaricato potrà e dovrà fare sempre riferimento ai referenti aziendali Privacy, individuabili nelle figure del Titolare e del Responsabile Protezione Dati (per brevità RPD).

Società di consulenza esterna

Al fine di garantire il massimo supporto giuridico, operativo e tecnico a tutte le persone autorizzate, l'azienda, oltre a fornire assistenza tramite il Titolare ed il Responsabile Protezione Dati, ha provveduto anche a stilare idoneo contratto di consulenza continuativa con apposita società specializzata, a cui ogni addetto potrà e dovrà rivolgersi in caso di dubbi nell'applicazione e/o interpretazione delle leggi in materia di protezione dei dati personali.
Quanto sopra a dimostrazione della volontà del Titolare di addivenire al massimo rispetto e corretta applicazione del Regolamento Europeo e per arrivare, al più presto, all'applicazione in azienda di misure di sicurezza "adeguate", così come da definizione normativa.

Ambito e limiti del trattamento di dati

Il trattamento di dati aziendali è consentito solo ed esclusivamente al fine di svolgere le mansioni per le quali ogni singola persona è stata appositamente autorizzata dal Titolare.

Non è quindi, in nessun caso e per nessun motivo, consentito trattare dati eccedenti rispetto a quanto richiesto dalle reali esigenze lavorative.
In generale la persona autorizzata ha l'obbligo di trattare i dati di cui viene a conoscenza in azienda, secondo principi di correttezza, liceità, necessità e riservatezza.

■ Definizioni normative derivanti dal nuovo Regolamento Europeo 2016/679

Ai fini del presente documenti s'intende per:
1) **dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2) **categorie "particolari" di dati personali:** dati personali che rivelino l'origine razziale od etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
3) **trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

4) **archivio:** qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

5) **titolare del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

6) **responsabile protezione dati:** soggetto designato dal Titolare in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa, delle prassi in materia di protezione dei dati e della capacità di assolvere ai compiti di cui all'art. 39 del Regolamento Europeo 2016/679;

7) **responsabile del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

8) **autorità di controllo:** l'autorità pubblica indipendente istituita da uno Stato membro.

■ Trattamenti di dati con strumenti elettronici: istruzioni operative

In riferimento ai trattamenti effettuati mediante l'utilizzo di strumenti elettronici (Pc fissi o portatili, tablet, smartphone, ecc.), la persona autorizzata, anche detta "incaricato", ha l'obbligo di attenersi alle seguenti istruzioni:

- **Codice utente (user name):** per accedere allo strumento elettronico l'incaricato dovrà necessariamente utilizzare il codice utente attribuitogli dal Titolare.

Il codice utente potrà essere costituito da un numero, da delle lettere o dalla combinazione di tali elementi anche con altri simboli.

Il codice utente è pubblico ed identifica inequivocabilmente il singolo incaricato.

L'incaricato non potrà cambiare per nessun motivo il suo il codice utente salvo autorizzazione scritta del Titolare o del Responsabile.

- **Parola chiave (password)**: il suddetto codice utente dovrà essere utilizzato in costante abbinamento con la parola chiave, la quale deve avere almeno le seguenti caratteristiche **tassative ed inderogabili**:

- deve essere costituita da almeno **8 caratteri alfanumerici**;
- deve essere **segreta e personale** e non può essere conosciuta da alcuno all'infuori dell'incaricato;
- deve essere digitata in condizioni di **massima riservatezza**;
- non deve contenere **riferimenti facilmente riconducibili alla persona** dell'incaricato (es. proprio nome e data di nascita);
- non deve essere **banale** (es. mese ed anno in corso);
- deve essere cambiata **almeno ogni 2 mesi;**
- deve essere completamente **differente da quelle che l'hanno preceduta**.

Si evidenziano di seguito alcune modalità operative per una corretta selezione della password: la sua scelta rappresenta infatti un momento cruciale per garantire la sicurezza dei sistemi informatici aziendali.

E' fondamentale individuare, da parte di tutti gli incaricati, delle così dette password "forti" e tutelarle nel modo più opportuno.

In pratica, nella creazione della password, si dovrà necessariamente utilizzare una vasta gamma di lettere e numeri ed, eventualmente, anche simboli presenti sulla tastiera.

Si veda a titolo esemplificativo quanto segue:

Password conforme e forte: **82W4ZC&21E**

Tale password risulta:

- ridondante di caratteri (10),
- composta da numeri, lettere e simboli,
- non banale e senza riferimenti personali,
- non contenuta in nessun vocabolario.

Password non valida o debole: **Lorenzo70**

Tale password, seppur costituita da almeno 8 caratteri, risulta:

- banale ed intuibile,
- contenente riferimenti quasi certamente riconducibili all'incaricato,
- carente di simboli.

Si evidenziano di seguito, comportamenti tassativamente da evitare nella gestione della password:

- è assolutamente vietato comunicare ad alcuno la propria password;
- è assolutamente vietato scrivere la password su un supporto cartaceo conservato nelle vicinanze del Pc o comunque in un luogo facilmente rintracciabile;
- è assolutamente vietato digitare la password in presenza di altre persone;
- è assolutamente vietato usare come password il proprio codice utente;
- è assolutamente vietato usare passwords che possano in qualche modo essere legate alla sfera personale dell'incaricato come, ad esempio, il nome proprio e dei famigliari, date di nascita, età, numeri di telefono, ecc.

- **Dispositivi di autenticazione informatica (smart card e similari):** in alternativa all'utilizzo del codice utente e della parola chiave, il Titolare può consegnare agli incaricati degli appositi dispositivi che consentono l'accesso agli strumenti elettronici (ad esempio smart card, penne usb e similari).

  Tali dispositivi sono da considerarsi strettamente personali e potranno essere utilizzati solo ed esclusivamente dall'incaricato che li ha legittimamente ricevuti.

  E' assolutamente vietato consentire l'utilizzo del proprio dispositivo di accesso ad altri soggetti o scambiarsi i dispositivi medesimi.

  L'incaricato dovrà conservare con la massima cura il dispositivo non lasciandolo mai incustodito.

  In caso di furto o smarrimento del dispositivo, l'incaricato dovrà immediatamente darne notizia al Titolare o Responsabile tramite nota scritta.

- **Caratteristiche biometriche:** in alternativa all'utilizzo del codice utente e della parola chiave, il Titolare può anche introdurre riconoscitori di caratteristiche biometriche (ad esempio impronte digitali, timbro della voce, retina, ecc.), che consentono l'accesso agli strumenti elettronici da parte degli incaricati, solo dopo l'identificazione.

  E' assolutamente vietato utilizzare la propria caratteristica biometrica per far accedere agli strumenti elettronici altri soggetti.

- **Profilo di autorizzazione:** ogni incaricato, una volta che abbia avuto accesso allo strumento elettronico e quindi ai dati da trattare, dovrà tassativamente rispettare il proprio profilo di autorizzazione assegnatogli dal Titolare in forma scritta con idonea lettera d'incarico.

  All'infuori di tale profilo, l'incaricato non può accedere e trattare alcun dato, se non appositamente e preventivamente autorizzato per iscritto dal Titolare.

Il profilo di autorizzazione sarà verificato periodicamente dal Titolare al fine di accertare che l'incaricato non tratti dati ridondanti rispetto alle sue reali necessità lavorative.

- **Firewall:** ogni qual volta l'incaricato utilizzi un Pc (es. Pc portatile) non connesso alla rete aziendale ed acceda ad una rete informatica esterna, ad esempio internet, dovrà accertarsi, sotto la sua responsabilità, che lo strumento elettronico in sua dotazione sia idoneamente protetto con apposito firewall hardware o software debitamente impostato ed aggiornato; se così non fosse, l'incaricato dovrà rinunciare ad accedere alla rete esterna ed informare senza indugio e con nota scritta il Titolare.

- **Antivirus:** ogni qual volta l'incaricato utilizzi un Pc (es. Pc portatile) non connesso alla rete aziendale, dovrà accertarsi, sotto la sua responsabilità, che lo strumento elettronico in sua dotazione sia costantemente ed idoneamente protetto con apposito programma antivirus debitamente attivato, impostato e costantemente aggiornato; se così non fosse, l'incaricato dovrà immediatamente interrompere la sessione di lavoro ed informare senza indugio e con nota scritta il Titolare.

- **Salvataggi:** l'incaricato dovrà effettuare, sotto la sua responsabilità, il salvataggio dei dati eventualmente residenti solo sul supporto di memorizzazione dello strumento elettronico in sua dotazione e non memorizzati sul "server" centrale dell'azienda. Il salvataggio di tali dati ad opera dell'incaricato dovrà avvenire con cadenza almeno settimanale e con gli strumenti ritenuti da lui più idonei. I supporti di salvataggio utilizzati dovranno essere tassativamente custoditi in apposito sito chiuso a chiave (es. armadio, cassetto, cassaforte, cassetta di sicurezza esterna, ecc.), al fine di prevenirne il furto o semplicemente l'utilizzo temporaneo da parte di terzi non autorizzati. I supporti di salvataggio non più necessari all'azienda (esempio cd non riscrivibili

e ridondanti), poiché, ad esempio, superati da successive versioni di back up, dovranno essere sistematicamente sovrascritti e/o distrutti e non semplicemente cestinati. Nel caso in cui l'incaricato non avesse a disposizione le necessarie risorse hardware e software per effettuare in modo efficace i salvataggi, dovrà informare senza indugio e con nota scritta il Titolare del trattamento. Non è in generale consentito portare i dati salvati al di fuori dell'azienda, se non a seguito di apposita autorizzazione del Titolare e nel rispetto di un rigido protocollo di trasporto, che tuteli al meglio i supporti contenenti i dati stessi, da rischi di furto, dispersione, distruzione, ecc.

- **Screen saver con parola chiave e procedure di logout:** ogni incaricato dovrà mantenere sullo strumento elettronico in sua dotazione, idoneo screen saver con richiesta di parola chiave alla ripresa della sessione di lavoro e con tempo di entrata in funzione non superiore a minuti 5 o comunque in base a quanto indicato di volta in volta dal Titolare. Sarà in ogni caso cura dell'incaricato, chiudere la sessione di lavoro con idoneo logout, ogni qual volta si dovesse assentare dalla stanza in cui è collocato lo strumento elettronico.
- **Aggiornamenti dei sistemi operativi e programmi utilizzati (patch e similari):** l'incaricato dovrà effettuare, sotto la sua responsabilità, l'aggiornamento periodico dei sistemi operativi e programmi utilizzati sullo strumento elettronico in sua dotazione, che per ragioni tecniche o per qual si voglia altra ragione, non sia possibile effettuare a livello di server aziendale. Nel caso in cui l'incaricato non avesse a disposizione le necessarie conoscenze informatiche o le tecnologie hardware e software per effettuare tali aggiornamenti, dovrà informare senza indugio e con nota scritta il Titolare del trattamento.

Si veda, in riferimento a quanto sopra, anche la seguente tabella:

Tabella di sintesi

Trattamenti con strumenti elettronici

OBBLIGO	DESTINATARI DELL'OBBLIGO	SUPPORTO NORMATIVO ED OPERATIVO
Utilizzo di codici utente conformi	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Utilizzo di parole chiave conformi	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Cambiamento periodico della parola chiave	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Analisi dei criteri di selezione della parola chiave nel tempo	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Eventuale adozione di dispositivi alternativi alla parola chiave (es. badge, smart card, dati biometrici)	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Adozione di idonei profili di autorizzazione	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Installazione ed aggiornamento di antivirus	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Installazione ed aggiornamento firewall hardware	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Installazione e aggiornamento firewall software (alternativo al precedente)	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Salvataggio periodico dei dati	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Mantenimento di screensaver con richiesta di parola chiave	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Procedura di log out in caso di assenza dalla stanza di lavoro	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Aggiornamento periodico dei sistemi operativi e programmi utilizzati (patch e similari)	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.

■ Internet e posta elettronica: istruzioni operative

Si premette che il personal computer, sia fisso che mobile, ed i relativi software e/o apparati hardware affidati al dipendente, costituiscono strumenti di lavoro e pertanto tali beni vanno utilizzati in modo consono e conforme alle finalità aziendali e mai per scopi personali.

Essendo, in caso di violazioni normative, sia l'impresa che il singolo lavoratore potenzialmente punibili con sanzioni anche di natura penale, l'azienda, nel pieno rispetto e per il rispetto della normativa sulla Privacy, si riserva di verificare la preservazione del proprio sistema informatico e la correttezza delle sue configurazioni e delle sue banche dati con le finalità e gli scopi lavorativi.

L'azienda, per esigenze di controllo della sicurezza della gestione dei dati e del regolare svolgimento dell'attività lavorativa, potrà quindi accedere, a campione e nel rispetto della massima riservatezza di ognuno, agli archivi di posta elettronica od ai file che evidenzino gli episodi di collegamento alla rete.

➧ **Utilizzo di internet:** le presenti indicazioni di massima, possono essere integrate e modificate dalla specifica "Privacy & Internet Policy" aziendale eventualmente già adottata dalla società.

In riferimento all'utilizzo della rete internet e per una ottimale sicurezza dei dati aziendali, si segnala in generale all'incaricato che:

- non è permesso visitare siti non inerenti e non necessari allo svolgimento delle mansioni lavorative attribuite;
- non è permesso, a maggior ragione, visitare siti che mostrino contenuti contrari all'etica comune e alle prescrizioni di legge;
- non è permessa alcuna forma di registrazione a siti i cui contenuti non siano strettamente connessi all'attività lavorativa;

- non è permessa l'installazione di programmi anche gratuiti, trial, shareware e similari, prelevabili da siti Internet, se non in casi espressamente autorizzati in via preventiva dal Titolare;
- non è permessa l'effettuazione di qualunque tipo di transazioni economico/finanziarie di natura privata, comprese le operazioni di home banking, acquisti on-line e simili, fatti salvi i casi autorizzati dal Titolare o dal Responsabile e con il rispetto delle procedure indicate volta per volta;
- non è permesso prelevare dalla rete Internet o reti similari, prodotti elettronici ed informatici in violazione delle normative sul diritto d'autore (esempio file audio, film, videogiochi, ecc.);
- non è permessa la conservazione su alcun supporto hardware aziendale, di file o immagini di natura oltraggiosa o che possano indurre a discriminazioni di natura sessuale, religiosa, razziale, politica e similare;
- non è permessa la partecipazione a giochi in rete o gruppi di discussione, l'utilizzo di chat line e servizi similari.

Utilizzo del servizio di posta elettronica: le presenti indicazioni di massima, possono essere integrate e modificate dalla specifica "Privacy & Internet Policy" aziendale eventualmente già adottata dalla società.

In riferimento all'utilizzo della posta elettronica e per una ottimale sicurezza dei dati aziendali, si segnala in generale all'incaricato che:

- non è permesso utilizzare la posta elettronica per motivi non inerenti allo svolgimento delle mansioni assegnate; eventuali messaggi ricevuti da terzi non connessi all'attività lavorativa, devono essere immediatamente "dirottati" verso l'account personale dell'utente; quest'ultimo non deve essere utilizzato durante l'orario di lavoro.

- non è permesso l'accesso alla posta elettronica ed alla navigazione Internet in generale, in orari differenti da quello di lavoro previsto per un determinato utente.
- non è permessa la trasmissione, a mezzo posta elettronica, di dati sensibili, personali e commerciali di alcun genere, salvo preventiva autorizzazione scritta del Titolare.
- non è permesso l'uso di posta elettronica per i contatti interpersonali tra lavoratori non inerenti l'uso d'ufficio.

■ Trattamenti di dati con supporti cartacei: istruzioni operative

In riferimento ai trattamenti effettuati mediante l'utilizzo di supporti cartacei, la persona autorizzata (incaricato) ha l'obbligo di attenersi alle seguenti istruzioni che potranno, caso per caso, essere integrate dal Titolare del trattamento:

- **Profilo di autorizzazione:** ogni incaricato dovrà tassativamente rispettare il proprio profilo di autorizzazione assegnatogli dal Titolare in forma scritta con idonea lettera d'incarico.

  All'infuori di tale profilo, l'incaricato non può accedere e trattare alcun dato contenuto su qualsivoglia tipo di supporto cartaceo, se non appositamente e preventivamente autorizzato per iscritto dal Titolare.

  Il profilo di autorizzazione sarà verificato periodicamente dal Titolare al fine di accertare che l'incaricato non tratti dati ridondanti rispetto alle sue reali necessità lavorative.

- **Gestione del documento cartaceo:** gli atti e i documenti, contenenti dati personali, non devono essere lasciati liberi di circolare senza controllo e non devono essere lasciati al di fuori di idonei raccoglitori per un tempo eccedente le finalità di utilizzo.

Devono quindi essere immediatamente riposti/archiviati o restituiti al termine delle operazioni.

- **Gestione del documento cartaceo contenente dati sensibili/particolari:** in caso di atti e documenti contenenti dati sensibili/particolari, la custodia e la gestione devono avvenire in modo tale che ai dati non possano accedere, in nessun modo e per nessun motivo, persone prive di apposito profilo di autorizzazione. A tale fine, i documenti dovranno essere sempre archiviati in:

- cassetti con serratura,
- armadi con serratura,
- casseforti,
- utilizzando altri dispositivi aventi funzione equivalente.

Prima di assentarsi dalla postazione di lavoro, anche per pochi istanti, i documenti andranno riposti nei siti protetti di cui appena sopra.

Nel caso in cui l'incaricato non avesse a disposizione le necessarie dotazioni per custodire in modo efficace i documenti contenenti dati sensibili/particolari, dovrà informare senza indugio e con nota scritta il Titolare del trattamento.

Gli uffici ed i locali in genere, contenenti dati sensibili/particolari, dovranno poi essere chiusi a chiave quando l'incaricato dovesse assentarsi, anche per un brevissimo lasso temporale.

La circolazione di un documento contenente dati sensibili/particolari dovrà sempre avvenire in busta chiusa e sigillata; la busta potrà essere aperta solo dall'incaricato preposto dall'azienda.

- **Gestione del curriculum:** si evidenzia che i curricula che arrivano in azienda, tramite e-mail, posta ordinaria, fax, consegna diretta, possono spesso contenere dati particolari (ad esempio l'appartenenza del candidato a categorie protette): tali documenti potranno quindi essere trattati solo ed esclusivamente dagli incaricati preposti dall'azienda, appositamente formati in

base a quanto prescritto dal Garante e dotati di idoneo profilo di autorizzazione. Tutti gli altri incaricati che incidentalmente, dovessero ricevere un curriculum, ad esempio sulla propria casella di posta elettronica, dovranno immediatamente distruggerlo senza visionarne il contenuto.

- **Fax:** l'invio di qualunque fax potrà avvenire, solo ed esclusivamente utilizzando l'idonea copertina messa a disposizione dall'azienda e contenente l'informativa Privacy prevista dall'art. 13 del Regolamento Europeo 2016/679.
  E' assolutamente vietato inoltrare fax senza la copertina di cui appena detto.
  Nel caso in cui l'incaricato non avesse a disposizione la copertina del fax, dovrà informare senza indugio e con nota scritta il Titolare del trattamento.
- **Stampe in stanza non controllata:** se l'incaricato effettua dal proprio Pc, stampe presso un locale adiacente al suo, dovrà immediatamente recuperarle senza lasciarle incustodite.
- **Fotocopie:** le fotocopie di documenti contenenti dati personali, dovranno essere effettuate solo se veramente necessarie e non in modo ridondante.
  Il documento fotocopiato dovrà essere gestito con le stesse identiche procedure previste per l'originale.
- **Carta da riciclo:** è assolutamente vietato utilizzare come carta da riciclo quei documenti cartacei che contengono dati personali.
- **Distruzione documenti:** i documenti non più necessari od inutilizzati, di cui l'incaricato intenda disfarsi, non dovranno essere semplicemente cestinati, ma dovranno essere fisicamente resi inutilizzabili e non intelligibili, ad esempio utilizzando le apposite apparecchiature distruggi documenti.

Nel caso in cui l'incaricato non avesse a disposizione le apparecchiature per distruggere i documenti, dovrà distruggerli manualmente e dovrà informare senza indugio e con nota scritta il Titolare del trattamento.

- **Accesso agli archivi dopo l'orario di chiusura:** l'incaricato che, per motivi di servizio abbia la necessità di accedere agli archivi dopo l'orario di chiusura, dovrà obbligatoriamente identificarsi e registrarsi, seguendo procedure manuali (ad esempio compilazione di apposito registro controfirmato) o procedure elettroniche, che consentano di rintracciare i documenti estratti dagli archivi ed i trattamenti effettuati.
- **Gestione delle richieste scritte di soggetti terzi:** l'incaricato al quale dovesse pervenire un qualunque tipo di documento (lettera raccomandata, lettera ordinaria, e-mail), con richieste di chiarimenti in ambito Privacy, da parte di un soggetto terzo (ad esempio cliente, fornitore, dipendente, ecc.), dovrà darne immediatamente notizia al Titolare.

Si veda, in riferimento a quanto sopra, anche la seguente tabella:

Tabella di sintesi

Trattamenti con supporti cartacei

OBBLIGO	DESTINATARI DELL'OBBLIGO	SUPPORTO NORMATIVO ED OPERATIVO
Rispetto del profilo di autorizzazione	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Corretta gestione del documento cartaceo: custodia, circolazione, archiviazione, ecc.	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Corretta gestione del documento cartaceo contenente dati sensibili/particolari	Incaricati preposti al trattamento dei dati sensibili/particolari	Titolare, Responsabile, Società di consulenza.
Corretta gestione del curriculum	Incaricati preposti al trattamento dei dati sensibili/particolari	Titolare, Responsabile, Società di consulenza.
Distruzione del curriculum ricevuto	Incaricati non autorizzati al trattamento dei dati sensibili/particolari	Titolare, Responsabile, Società di consulenza.
Utilizzo della copertina per l'invio di fax	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Corretta gestione delle stampe da Pc	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Corretta gestione dei documenti fotocopiati	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Divieto di utilizzo della carta da riciclo	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Corrette modalità di distruzione dei documenti	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.
Corretta procedura di accesso agli archivi dopo l'orario di chiusura	Tutti gli incaricati	Titolare, Responsabile, Società di consulenza.

■ Conversazioni: istruzioni operative

In riferimento ai trattamenti effettuati mediante l'utilizzo di apparecchiature telefoniche o mediante conversazione diretta con l'interlocutore, la persona autorizzata (incaricato) ha l'obbligo di attenersi alle seguenti istruzioni che potranno, caso per caso, essere integrate dal Titolare del trattamento:

- **Telefonate:** le telefonate dovranno avvenire ad un tono di voce moderato, in modo tale che i vicini di scrivania od i colleghi d'ufficio non possano venire a conoscenza di informazioni riservate.
  E' in generale vietato comunicare telefonicamente qualsiasi tipo di informazione riservata per la quale non si sia stati appositamente autorizzati.
- **Distanza di cortesia:** è obbligatorio rispettare e far rispettare idonee distanze di cortesia nel momento in cui si stia dialogando con terzi o si stiano consegnando dei documenti a carattere riservato (ad esempio consegna della busta paga).
- **Gestione delle richieste orali di soggetti terzi:** l'incaricato al quale dovesse pervenire un qualunque tipo di richiesta orale (tramite telefonata o colloquio) in ambito Privacy, da parte di un soggetto terzo (ad esempio cliente, fornitore, dipendente, ecc.), dovrà darne immediatamente notizia al Titolare.

■ Formazione del personale obbligatoria

Il Titolare ed il Responsabile Protezione Dati organizzano periodicamente e con cadenza almeno annuale, corsi di formazione (in aula od on-line) ed informazione in ambito Privacy, con il supporto della società esterna di consulenza Winger S.a.s..

A tali corsi dovranno obbligatoriamente intervenire, per espressa previsione di legge, tutti gli incaricati che trattano, anche solo occasionalmente, dati personali. Ciò al fine di addivenire ad una ottimale conoscenza della normativa e di quelle che sono le misure di sicurezza in ambito Privacy.

■ Integrazioni e chiarimenti alle istruzioni

Le presenti istruzioni potranno essere integrate in ogni momento con ulteriori chiarimenti forniti oralmente o per iscritto dal Titolare.

■ Quesiti degli incaricati: servizio di risposta

Si invitano tutte le persone autorizzate al trattamento, per qualunque dubbio dovesse insorgere nell'operatività quotidiana, ad inoltrare i propri quesiti in forma scritta al Titolare e al Responsabile Protezione Dati, i quali provvederanno a fornire idoneo riscontro, sempre in forma scritta.

Per la competenza e dedizione dimostrate nella stesura del presente manuale, si desidera ringraziare gli stimati professionisti, del cui operato si ha il piacere di avvalersi ogni giorno.

In ordine alfabetico:

- *Dott.ssa Annachiara Grasselli*
- *Avv. Eros Grasselli*
- *Ing. Francesco Manzini*
- *Dott. Juri Torreggiani*