NORME COMPORTAMENTALI PER GLI INCARICATI
DEL TRATTAMENTO DEI DATI PERSONALI

ITI F. Severi
Via Luigi Pettinati, 46
35129 Padova (PD)
Tel. 049 8658111 - Fax 049 8658120
eM.: pdtf04000q@istruzione.it

PREMESSA

Scopo della presente procedura è illustrare le norme comportamentali/tecniche cui gli Incaricati devono attenersi nello svolgimento delle operazioni di trattamento di dati personali.

In particolare la procedura descrive:

- i riferimenti normativi per la gestione delle nomine degli incaricati.
- le regole di ordinaria diligenza che gli Incaricati del trattamento sono tenuti ad osservare nel corso della loro prestazione lavorativa
- le misure di sicurezza per gli archivi elettronici/cartacei da adottare per la protezione dei dati personali.

In particolare sono messi in risalto gli aspetti relativi alle misure di sicurezza previste dall'art. 32 GDPR 2016/679, che ciascun Incaricato è chiamato ad adottare per dare piena applicazione a quanto disposto dalla normativa in materia.

Tale procedura si applica, indistintamente, agli Incaricati interni ed esterni che si trovano ad operare su dati personali, particolari e la cui Titolarità è dell'Istituto ITI F. Severi .

Si precisa comunque che possono essere eseguite attività in autonomia purché non comportino una diminuzione del livello generale e specifico di sicurezza.

L'Istituto ITI F. Severi , tramite verifiche periodiche, direttamente o con l'ausilio di altre Istituto, effettuerà i controlli che riterrà opportuni per vigilare sulla puntuale osservanza delle disposizioni della Normativa vigente e delle presenti Istruzioni Operative.

INDICE DEGLI ARGOMENTI

I RIFERIMENTI NORMATIVI

Il presente documento si inquadra nell'ambito delle Misure di Sicurezza, previste dal GDPR 2016/679 e dalla normativa nazionale vigente in materia di trattamento e protezione dei dati, applicabili all'Istituto ITI F. Severi .

Gli Incaricati del trattamento sono i soggetti, nominati dal Titolare e/o dal Delegato Privacy, che elaborano i dati personali cui hanno accesso attenendosi alle istruzioni loro impartite dal Titolare e/o dal Delegato.

Il GDPR 2016/679 conferma che la conoscenza dei dati personali da parte delle persone incaricate per iscritto di compiere operazioni di trattamento non può considerarsi alla stregua di una comunicazione a terzi come a suo tempo indicato dall'art. 20 della Legge 675/96.

E' necessario, quindi, che il Titolare o i Delegati Privacy nominino con puntuale indicazione dell'ambito di trattamento consentito, quale Incaricato, tutto il personale dell'Istituto ITI F. Severi che tratta dati personali

Allo stesso modo coloro che, trovandosi **temporaneamente** a lavorare per l'Istituto ITI F. Severi (ad es. praticanti, tirocinanti, stagisti, personale in prova ed altri), utilizzano/trattano dati che la legge qualifica come personali, particolari o giudiziari, dovranno essere nominati dai Delegati Privacy "Incaricati", e dovranno operare adottando le medesime modalità stabilite per l'Incaricato interno.

LA LETTERA D'INCARICO E LE ISTRUZIONI OPERATIVE PER GLI INCARICATI

Gli Incaricati ricevono una formale lettera di incarico da parte del Titolare / Delegato Privacy.
In tale lettera sono presenti alcuni elementi che impegnano l'Incaricato a:

1. collaborare con il Delegato Privacy;
2. utilizzare i dati solo per gli scopi istituzionali, nello spirito della legge e secondo le istruzioni scritte che ha ricevuto dal Delegato Privacy;
3. rispettare il segreto di ufficio e professionale, oltre che i requisiti di riservatezza e sicurezza durante l'uso dei dati personali.

E' opportuno ribadire che la formalizzazione scritta dell'incarico è obbligatoria in quanto il GDPR 2016/679 e la normativa nazionale vigente impongono, a coloro che compiono direttamente le operazioni di trattamento, di assumere il ruolo di Incaricati.

IL TRATTAMENTO DEI DATI PERSONALI DA PARTE DELL'INCARICATO

Una volta ricevuta la lettera di nomina e la conseguente autorizzazione, l'Incaricato può svolgere materialmente il trattamento attenendosi alle istruzioni operative dettate dal Delegato Privacy.

Con il termine trattamento ci si riferisce ad una qualunque operazione effettuata sui dati svolta con o senza l'ausilio di mezzi automatizzati e che abbia come oggetto una delle operazioni indicate dall'art. 4, p. 2 del GDPR 2016/679[1].
Il trattamento comprende **l'intera vita** del dato personale, dal momento della raccolta a quello della distruzione, abbracciando operazioni di utilizzo interno (organizzazione, conservazione, raffronto, ecc.) ed esterno (comunicazione, diffusione, interconnessione ad altre banche dati), e prescindendo sia dall'eventuale uso di strumenti informatici, sia dalla circostanza che il dato venga divulgato o elaborato nel senso stretto del termine.
Di conseguenza, si parla di trattamento sia nel caso in cui vengano utilizzati mezzi elettronici o comunque automatizzati, sia altri mezzi che richiedono l'esclusivo apporto umano.

1 **Art. 4, 2)**, per "trattamento", si intende 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;

I DATI PERSONALI OGGETTO DEL TRATTAMENTO

Il concetto di "dato personale" (art. 4, p. 1) fa riferimento a qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
I dati personali oggetto di trattamento che vengono presi in considerazione dalla legge possono essere suddivisi in:

- dati identificativi;
- dati particolari idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati personali idonei a rivelare lo stato di salute dell'interessato;
- dati giudiziari, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

La distinzione tra le varie tipologie di dati personali assume notevole rilevanza in quanto i trattamenti vengono disciplinati in maniera differenziata in ragione della diversa natura del dato personale oggetto di trattamento riflettendosi anche sulle misure di sicurezza che dovranno essere adottate e previste dalla Legge.

LE REGOLE DI ORDINARIA DILIGENZA PER L'INCARICATO

Nell'esecuzione dei compiti assegnati, l'Incaricato deve attenersi ad alcune regole di ordinaria diligenza al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento.
Per queste ragioni l'Incaricato, nello svolgimento delle proprie mansioni deve prestare particolare attenzione nel:

- non divulgare a terzi estranei le informazioni di cui viene a conoscenza
- adoperarsi affinché terzi fraudolentemente non entrino in possesso di dati deliberatamente comunicati
- non fare copie, per uso personale, dei dati su cui svolgono operazioni d'ufficio
- la riproduzione di documenti contenenti Dati Personali Particolari e/o Giudiziari su supporti non informatici (ad esempio fotocopie) è vietata se non espressamente autorizzata preventivamente specificatamente dalla Direzione o dal Responsabile competente. La riproduzione deve essere sottoposta alla medesima disciplina dei documenti originali;
- attenersi scrupolosamente alle istruzioni scritte impartite dal Titolare, Delegato Privacy e/o dai singoli Delegati Privacy;
- osservare i dei criteri di riservatezza;
- trattare i dati in modo lecito e secondo correttezza;
- trattare i dati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
- comportarsi nel pieno rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta
- qualora l'Incaricato **abbandoni temporaneamente** la propria postazione di lavoro deve provvedere a :
    a) Fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali.
    b) riporre nei cassetti o negli armadi la documentazione cartacea contenente dati personali.
    c) Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre I documenti e attivare il salva schermo del PC con password
    d) Non rivelare o fare digitare le password dal personale di assistenza tecnica.
    e) Non rivelare le password al telefono né inviarla via fax - nessuno è autorizzato a chiederle.
    f) Segnalare qualsiasi anomalia o stranezza all'eventuale Delegato Privacy o al Responsabile IT.

MISURE PER LA PROTEZIONE DEI DATI PERSONALI PER L'INCARICATO

I principi stabiliti all'articolo 32 del GDPR 2016/679 stabiliscono che i dati debbano essere custoditi e controllati in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
A tal fine, la Legge richiede l'adozione di una serie di misure di sicurezza, individuate dal Titolare del trattamento.
La mancata adozione di tali misure potrebbe comportare anche una responsabilità penale, che potrebbe essere ripartita tra tutti i soggetti coinvolti nel trattamento dei dati, in base al grado di responsabilità ad essi riconosciuto.
E' necessario, quindi, che gli Incaricati osservino le norme comportamentali che discendono dalle misure di protezione secondo quanto indicato nella normativa vigente in materia di trattamento e protezione dei dati, in esame, e descritte nei successivi paragrafi attenendosi scrupolosamente alle presenti istruzioni scritte ed ad ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal "Delegato Privacy".

Le misure di sicurezza sono obbligatorie e sono distinte in funzione delle seguenti modalità di trattamento dei dati:

1. **senza l'ausilio di strumenti elettronici** (es. dati in archivi cartacei o su supporto magnetico/ottico);
2. **con l'ausilio di strumenti elettronici** (PC ed elaboratori).

1. TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

I dati personali archiviati su supporti di tipo magnetico e/o ottico devono essere protetti con le stesse misure di sicurezza previste per i supporti cartacei.
Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.

1.1 Consegna e consultazione della documentazione cartacea

- La consultazione dei documenti, contenenti Dati Personali, deve avvenire esclusivamente da parte degli Incaricati al trattamento, solo quando operativamente necessario e, quando possibile, in loco.
- L'Incaricato al trattamento può effettuare la consultazione di tali documenti fuori orario di lavoro, solo se preventivamente autorizzato dal Delegato Privacy, identificato e registrato sull'apposito registro dal personale addetto alla vigilanza.
- La consegna dei documenti contenenti Dati Personali deve essere effettuata, in modo da garantirne la riservatezza, in busta chiusa indirizzata nominativamente al destinatario (Delegato, Incaricato e/o Interessato).

1.2 Custodia

- I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (es. armadi o cassetti chiusi a chiave).
- I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

1.3 Comunicazione

- L'utilizzo dei dati personali deve avvenire in base al principio del *"need to know*" e cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento). I dati non devono essere comunicati all'esterno dell'Istituto ITI F. Severi e comunque a soggetti terzi se non previa autorizzazione.

1.4 Distruzione

- Tutti i documenti che non devono essere conservati per legge, devono essere distrutti al termine della loro utilizzazione.
- La distruzione dei documenti cartacei, nei limiti consentiti dalla legge, deve essere effettuata quando comunicato dal Delegato Privacy, all'interno della propria area di competenza.
- I documenti dovranno essere distrutti, sotto la supervisione del Delegato Privacy, all'interno della propria unità.
- Qualora sia necessario distruggere i documenti contenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.
- I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti.

1.5 Ulteriori istruzioni in caso di trattamento di dati riservati, Particolari e/o giudiziari

- I documenti contenenti dati riservati, Particolari e/o giudiziari devono essere controllati e custoditi dagli Incaricati in modo che non vi accedano persone prive di autorizzazione. Ad esempio, la consultazione di documenti/certificati per l'inserimento in procedure informatiche di gestione/amministrazione del personale di dati relativi ai loro emolumenti, a permessi sindacali, assenze per malattie ecc., deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati in base alle presenti istruzioni.
- L'archiviazione dei documenti cartacei contenenti dati Particolari e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.
- Per accedere agli archivi contenenti dati Particolari e/o giudiziari fuori orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Delegato Privacy oppure farsi identificare e registrare su appositi registri.
- Qualora si acceda ad un locale/archivio contenente dati Particolari al di fuori dell'orario di lavoro, è necessario identificarsi e registrarsi sull'apposito registro previsto nella propria funzione di riferimento in modo da mantenere traccia delle attività svolte.

2. TRATTAMENTI CON L'AUSILIO STRUMENTI ELETTRONICI

2.1 Gestione delle credenziali di autenticazione

La legge prevede che l'accesso alle procedure informatiche che trattano dati personali sia consentito agli Incaricati in possesso di "credenziali di autenticazione" che permettano il superamento di una procedura di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato (user-id) associato ad una parola chiave riservata (password), oppure in un dispositivo di autenticazione (es. smart card) o in una caratteristica biometrica. Gli Incaricati devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni:

- Le user-id individuali per l'accesso alle applicazioni non devono mai essere condivise tra più utenti (anche se Incaricati del trattamento). Nel caso altri utenti debbano poter accedere ai dati è necessario richiedere l'autorizzazione al Delegato Privacy e/o al Responsabile IT.
- Gli strumenti di autenticazione (ad esempio le password) che consentono l'accesso alle applicazioni devono essere mantenute riservate. Essi non vanno mai condivisi con altri utenti (anche se Incaricati del trattamento).
- Le password devono essere sostituite, a cura del singolo Incaricato, **almeno ogni 90 giorni**

❖ **Più espressamente va osservata la seguente gestione delle password**

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

- impostare la password con una lunghezza di almeno 8 caratteri, salvo diverse istruzioni
- può essere alfanumerica (può contenere lettere, numeri e caratteri speciali)
- deve essere diversa dal "Nome Utente" o "User ID"
- non basarla su informazioni facilmente deducibili, quali:
  - nomi propri di persona
  - sigle di funzioni organizzative o aree e/o progetti interni all'Istituto
  - nomi di personaggi della politica, sport, cinema e fumetti
  - nomi di riferimento geografici
  - nomi di giorni della settimana, mesi dell'anno o stagioni
  - riferimenti al corrispettivo identificativo utente
  - il proprio nome e/o cognome
  - il nome e/o cognome dei famigliari
  - la data di nascita e/o il proprio codice fiscale
  - esclusivamente date in qualsiasi formato e con qualsiasi separatore di uso comune
- comunicare la password secondo le istruzioni ricevute
- mantenere la password riservata e non divulgarla a terzi
- non trascriverla su fogli, agendine, post-it facilmente accessibili a terzi
- sostituirla, qualora non indicato diversamente, almeno una volta ogni 90 giorni, salvo il caso di perdita della sicurezza della stessa
- non includere la password in alcun processo di connessione automatica.

Nel caso in cui una password perda di segretezza, l'Incaricato deve provvedere alla sua immediata sostituzione. Quando questo non risulti possibile, l'Incaricato deve comunicare tale circostanza al Responsabile IT che provvederà alla sostituzione della stessa.

E' opportuno che l'Incaricato sappia che:

- è imposto il divieto di collegamento da due o più postazioni contemporanee con le medesime credenziali
- in caso di mancato utilizzo, per un periodo superiore a **30 giorni** l'account è disabilitato automaticamente;
- in caso di revoca/esclusione dall'incarico che consentiva l'accesso all'elaboratore o all'applicazione, la user-id viene a decadere con decorrenza immediata.

2.2 CONDOTTA A PROTEZIONE DEI DATI E DEL PC

- Tutti i PC devono essere dotati di password rispondenti a quanto stabilito dall'Istituto ITI F. Severi (vedi Modello DTEC_S allegato al DRSP: Documento Riepilogativo del Sistema Privacy) e, ove non diversamente possibile, va impostata anche la password di BIOS.

- Tutti i PC devono essere dotati di **SOFTWARE ANTIVIRUS** aggiornato costantemente e con la **funzione "Monitor" attiva**.
- Sui PC devono essere installati esclusivamente software necessari all'attività lavorativa, dotati di licenza e forniti dalle strutture di appartenenza. Sono vietati i software scaricati da Internet o acquisiti autonomamente.

La postazione di lavoro deve essere:

- utilizzata solo per scopi legati alla propria attività di lavoro
- utilizzata, da utenti con nome utente e password personali
- configurata in modo che sia presente esclusivamente software fornito/approvato dall'Istituto ITI F. Severi .
  Sulla base di quanto sopra detto, gli Incaricati che accedano a dati personali conservati in formato elettronico devono impostare lo screen saver con password in modo che si attivi dopo pochi minuti di inattività e chiudere le applicazioni in uso prima di allontanarsi dalla postazione di lavoro.
  Al fine di proteggere la sessione di lavoro da utilizzi non autorizzati in sua assenza l'incaricato non deve lasciare incustodito e accessibile lo strumento elettronico. Quindi nel caso in cui ci si allontani dalla postazione si dovrà attivare lo screensaver o idonei mezzi di protezione messi a disposizione dall'Istituto ITI F. Severi che impediscano l'accesso ai dati presenti nel PC. Quando vi è necessità di assentarsi in modo prolungato dalla propria postazione di lavoro, oltre che attivare gli idonei mezzi di protezione sopra citati, si consiglia, ove possibile, di chiudere a chiave la porta quando si esce dalla stanza.
- Sui PC devono essere installati, appena vengono resi disponibili (e comunque almeno annualmente), tutti gli aggiornamenti software necessari a prevenirne vulnerabilità e correggerne i difetti dei sistemi operativi.

Ulteriori disposizioni sono riportate nel "Disciplinare Informatico Scolastico".

❖ **più espressamente va osservata la seguente gestione antivirus**

Al fine di evitare possibili danneggiamenti prodotti dall'ingresso nel sistema informativo di programmi contenenti virus è necessaria l'adozione di alcuni accorgimenti e misure di sicurezza. Per questi motivi l'Incaricato deve:

- evitare di introdurre applicazioni/software che non siano state preventivamente approvate dall'Istituto ITI F. Severi o la cui provenienza sia dubbia;
- controllare che il programma antivirus installato sia aggiornato periodicamente e costantemente attivo;
- verificare, con l'ausilio del programma antivirus in dotazione, ogni supporto magnetico contenente dati (cd/ dvd-rom, pendrive usb, schede SSD, ecc.), prima dell'esecuzione dei file in esso contenuti;
- prestare sempre debita attenzione agli eventuali messaggi di segnalazione di virus e, in caso di anomalie, contattare immediatamente l'Amministratore di Sistema Interno;
- Salvo nei casi espressamente autorizzati, non accedere via modem/router/chiavetta privati ad internet;
- Ogni ulteriore e più specifica misura di sicurezza sarà reperibile nel "Disciplinare Informatico Scolastico".

❖ **Come gestire la posta elettronica**

- Non aprire messaggi con allegati di cui non si conoscono l'origine, possono contenere virus in grado di cancellare i dati sul PC.
- Evitare di aprire filmati e presentazioni non attinenti l'attività lavorativa per evitare situazioni di pericolo per i dati contenuti sul vostro PC.

❖ **Salvataggio dei dati**

- Per quanto riguarda il salvataggio dei dati personali, alla fine di ogni sessione di lavoro, l'Incaricato deve salvare i files contenenti i dati solo sul proprio computer sempre a condizione che sia protetto da password.
- I salvataggi o backup periodici (almeno settimanali) su supporti esterni dovranno essere eseguiti su supporti opportunamente conservati e non accessibili da persone non autorizzate.

❖ **Supporti di memorizzazione dei dati**

Nel caso in cui siano utilizzati supporti informatici quali pendrive usb, schede SSD, Cd/Dvd-rom o nastri per la memorizzazione di dati personali particolari, gli Incaricati devono osservare alcune misure di sicurezza al fine di salvaguardare la riservatezza dei dati:

- i supporti informatici già contenenti dati personali particolari possono essere riutilizzati solo dopo aver provveduto a cancellare i dati e le informazioni in essi contenuti, in modo che non siano tecnicamente ed in alcun modo recuperabili;
- qualora si riscontrassero delle difficoltà nello svolgimento di tali operazioni, si può richiedere l'intervento dell'Amministratore di Sistema Interno;
- qualora la procedura di cancellazione dei dati risulti inapplicabile, al termine delle operazioni di trattamento i

supporti di memoria utilizzati devono essere distrutti;

- fra i supporti di memorizzazione sono ricompresi a pieno titolo i dischi equipaggiati nei computer dimessi e/o sostituiti dai dipendenti.
- l'Istituto ITI F. Severi non risponderà della perdita dei dati strettamente personali, eventualmente archiviati nella propria postazione di lavoro, il cui trattamento in ogni caso non deve interferire con la normale attività lavorativa. In particolare tali dati non potranno essere salvati nei server istituzionali.

L'incaricato del trattamento dei dati ha la responsabilità di:

- segnalare la necessità di un'eventuale riparazione degli hard disk;
- segnalare la necessità di un'eventuale dismissione dei CD-ROM, dei nastri magnetici, drgli hard disk, delle pendrive usb e delle schede SSD;
- eseguire la reinizializzazione delle pendrive usb e delle schede SSD per poterli successivamente riutilizzare;
- effettuare il test sulla reinizializzazione delle pendrive usb e delle schede SSD eseguita precedentemente.

Le attività d'uso e riuso sono possibili solo se disposte ed autorizzate specificatamente dal proprio Delegato e ogni caso non devono in alcun modo pregiudicare I livelli di sicurezza richiesti dall'attività specifica dall'Istituto ITI F. Severi .

❖ **Incidenti informatici e/o violazioni dei dati personali (Data Breach)**

Qualsiasi situazione a rischio e qualsiasi sospetto di carenza nella sicurezza, in special modo se esse riguardano i dati, devono essere segnalati tempestivamente al proprio "Responsabile" diretto, senza ingiustificato ritardo dopo essere venuto a conoscenza. Nei casi particolari di incidenti fisici o informatici, oppure in particolari situazioni di rischio che possono essere considerate "confidenziali", la notizia va mantenuta riservata, altrimenti una eventuale indagine interna relativa alla valutazione di tali rischi e/o violazioni, rischia di essere fuorviata. Il "Responsabile" diretto, a sua volta, dovrà avvisare l'Area IT e il Delegato Privacy.

In caso di violazione dei dati personali, soprattutto se questa ha comportato una violazione dei dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche, la Direzione in concorso con il Responsabile IT valuterà l'opportunità di comunicare l'accaduto, secondo quanto previsto dall'art. 33 del GDPR 2016/679, all'Autorità Garante, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

2.3 MEZZI DI TRASMISSIONE E RIPRODUZIONE DEI DOCUMENTI

E' importante adottare delle cautele nella trasmissione e riproduzione dei documenti contenenti dati personali, al fine di prevenire eventuali rischi di accesso ai dati da parte di soggetti non autorizzati.

A tal fine ciascun Incaricato deve:

- non lasciare incustoditi presso il fax, la stampante di rete o la macchina fotocopiatrice documenti contenenti dati personali;
- nel caso di trasmissione via fax di documenti contenenti dati personali accertarsi telefonicamente dell'avvenuta ricezione del fax e, una volta inviati, ritirarli immediatamente;
- nel caso di invio di dati personali a mezzo del servizio di posta elettronica, proteggere il documento con una password.

Nel caso di utilizzo di strumenti di interscambio di file, utilizzare le directory accessibili ai soli soggetti che hanno i requisiti previsti dalla Legge per effettuare a loro volta il trattamento dei dati.

❖ **Ulteriori istruzioni in caso di trattamento di dati particolari e/o giudiziari**

- Le password di accesso alle procedure informatiche che trattano dati Particolari e/o giudiziari devono essere sostituite, da parte del singolo incaricato, **almeno ogni 90 giorni.**
- L'installazione degli aggiornamenti software necessari a prevenire vulnerabilità e correggerne i difetti dei programmi per elaboratori deve essere effettuato almeno semestralmente.

GLOSSARIO

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.

Dato sensibile
I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico, sindacale, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale. Tali dati possono essere oggetto di trattamento solo con il consenso scritto dell'Interessato e previa autorizzazione del Garante.

Dato giudiziario
"dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale

Dato anonimo o dato non personale
Il dato che in origine, o a seguito di *trattamento*, non può essere associato ad un interessato identificato o identificabile, oppure, nel secondo caso, il dato non riconducibile ad una persona fisica (es.: ragione sociale di un'azienda).

Banca dati
Qualsiasi complesso di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo una pluralità di criteri determinati tali da facilitarne il *trattamento*.

Trattamento
Per "trattamento" s'intende 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;

Blocco
La conservazione di dati personali con sospensione temporanea di ogni altra operazione del *trattamento*.

Comunicazione
Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Diffusione
Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Violazione dei dati personali
La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Garante per la protezione dei dati personali
L'Autorità di Controllo istituita ai sensi dell'art. 51 del GDPR 2016/679. E' un organo collegiale costituito da quattro membri, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato.
Essi eleggono al loro interno un Presidente il cui voto prevale in caso di parità. I membri sono scelti tra persone che assicurino indipendenza e che siano esperti di riconosciuta competenza nelle materie del diritto o dell'informatica, garantendo la presenza di entrambe le qualificazioni.

Titolare
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.

Responsabile
La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Delegato Privacy
Le persone delegate per iscritto di compiere le operazioni di *trattamento* dal Titolare che operano sotto la loro diretta

autorità, che gestiscono uno o più incaricati a livello direzionale e/o organizzativo e che coordinano le attività di trattamento relativamente alla propria area di competenza.

Incaricato al trattamento
Le persone incaricate per iscritto di compiere le operazioni di *trattamento* dal Titolare o dal Responsabile o dai propri Delegati Privacy e che operano sotto la loro diretta autorità.

Interessato
La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.