ISISS "TEODOSIO ROSSI"
Via Montanino - 04015 PRIVERNO (LT)
Cod. Fiscale: 02000800595

Progetto della sicurezza dei dati personali (Regolamento Europeo 679/2016 – GDPR)

REDATTO IL 20/10/2018

INDICE

1. Progetto della protezione dei dati personali

1.1. Revisione

Indice delle revisioni

Rev	Data	Descrizione	Redatto	Verificato	Approvato

1.2. Scopo

Con l'entrata in vigore del **Regolamento Europeo 679/2016 (GDPR)** il Titolare del Trattamento viene responsabilizzato circa l'adozione di misure di sicurezza adeguate e idonee per la protezione dei dati personali in possesso dell'azienda e/o della propria attività.

E' quindi necessaria una completa e radicale revisione del flusso informativo nella struttura funzionale in relazione a quanto previsto dalla norma al fine di porre in essere procedure operative e tecnologie informatiche che permettano la maggiore protezione possibile ai dati presenti in azienda.

Nonostante il Decreto Legge 9 Febbraio 2012 ha di fatto, abrogato l'obbligo di redazione del Documento Programmatico sulla Sicurezza dei dati personali si ritiene utile redigere un documento che attesti la precisa volontà del Titolare circa la corretta applicazione delle misure di sicurezza che costituiscono la parte centrale della norma.
Pertanto lo scopo del presente **Progetto della protezione dei dati personali** è quello descrivere le attività poste in essere per ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, intendendosi per misure di sicurezza il complesso degli accorgimenti tecnici, informatici, organizzativi, logistici e procedurali di sicurezza.

1.3. Campo di applicazione

Il Documento sulla protezione dei dati personali definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.

Il Documento sulla protezione dei dati personali riguarda il trattamento di tutti i dati personali:

- Sensibili
- Giudiziari
- Comuni

Il Documento sulla protezione dei dati personali si applica al trattamento di tutti i dati personali effettuato per mezzo di:

- Strumenti elettronici di elaborazione anche esterni all'azienda (cloud, hosting, ecc)
- Altri strumenti di elaborazione (ed esempio: Cartacei, Audio, Visivi e Audiovisivi, ecc..)

Si dispone con apposito **Regolamento Interno** che Il Documento sulla protezione dei dati personali sia fatto conoscere ed applicato da tutte le funzioni che fanno parte dell'organizzazione.

1.4. Definizioni

Questo documento adotta le definizioni previste dall'Art 4. del R.E. 679/2016 per cui nel prosieguo i seguenti termini si intendono adottati nel medesimo significato espresso dalla norma.

Trattamento

Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

Dato personale

Qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale, l'ubicazione, elementi caratteristici della persona, dell'identità fisica, fisiologica, genetica psichica, economica, sociale o culturale.

Dati sensibili

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 o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

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.

Titolare
La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile
La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

Incaricati
Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

Interessato
La persona fisica o il soggetto giuridico cui si riferiscono i dati personali.

Comunicazione
Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, 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.

Dato anonimo
Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

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

Banca dati
Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Comunicazione elettronica
Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico.
Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.

Misure idonee e adeguate
Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

Strumenti elettronici
Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento. In questa categoria generale vengono inclusi anche strumenti esterni quali spazi in Cloud, server o computer in hosting o housing presso provider di servizi, utilizzo di repository esterni quali la posta elettronica, servizi di interscambio dati, portali personalizzati o web application. Tali strutture se utilizzate sono esplicitate nel **Registro dei Trattamenti**.

Autenticazione informatica
L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

Credenziali di autenticazione
I dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica.

Parola chiave (password)
Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

Profilo di autorizzazione
L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.
Sistema di autorizzazione
L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

2. Ruoli, compiti e nomina delle figure previste per la sicurezza dei dati personali

Così come espresso dalla norma il Titolare del trattamento, previa un'analisi dei flussi informativi, delinea un organigramma di funzioni individuando le seguenti figure se necessarie:

- Responsabile della Protezione dei Dati (DPO)
- Responsabile dell'Amministrazione della rete
- Responsabile dell'Amministratore dei sistemi
- Responsabile dell'Amministrazione delle basi dati
- Responsabili di specifici trattamenti dati
- Incaricati del Trattamento dei Dati Personali

In relazione alla complessità ed alla organizzazione il Titolare può nominare più soggetti con il medesimo profilo. Ogni figura è soggetta agli obblighi ed ai compiti previsti dalla norma (**Art. 28 del R.E. 679/2016**) che vengono riassunti in apposita Lettera di Nomina a firma del Titolare del Trattamento e controfirmata per accettazione dal Responsabile.

In relazione alla disponibilità di risorse umane e finanziare il Titolare può avocare a se stesso una o più funzioni, o assegnare più funzioni al medesimo soggetto; può altresì avvalersi di soggetti esterni all'azienda espressamente contrattualizzati ed incaricati con esplicita e controfirmata Lettera di Nomina.

I compiti di ciascuna figura così individuata sono sanciti dalla norma ed integrata dal Titolare del Trattamento secondo le necessità operative e funzionali dell'azienda.

Modalità e forme di applicazione delle disposizioni previste dal Titolare e dai Responsabili saranno comunicate agli Incaricati del Trattamento tramite una Lettera di Nomina a firma del Responsabile e controfirmata per accettazione da ogni Incaricato del Trattamento: quest'ultimo, inoltre, sarà tenuto all'osservanza di ogni e qualsiasi disposizione del Titolare del Trattamento o del Responsabile che lo ha incaricato e a seguire le disposizioni impartite attraverso il Regolamento Interno.

Il mancato rispetto delle direttive emanate dal Titolare del Trattamento e dal Responsabile o di una disposizione del Regolamento Interno saranno considerate violazioni compiute dall'Incaricato passibili di reprimenda, ammenda e quant'altro previsto dalla norma, ivi comprese le sanzioni e la responsabilità civile e penale di qualsiasi genere a natura direttamente ascrivibili all'Incaricato.

Procedure generali si sicurezza

Il Titolare del Trattamento individua alcune operazioni essenziali per la protezione dei dati e si riserva di assegnare i compiti relativi all'applicazione e alla verifica di tali procedure ad uno o più soggetti Responsabili o Incaricati scelti per competenza e disponibilità.

- Controllo periodico dell'integrità dei sistemi informativi e di eventuali aggiornamenti di sicurezza
- Verifica ed aggiornamento dei sistemi di protezione (antivirus, firewall, ecc)
- Verifica costante e periodica
- Controllo periodico della validità delle credenziali di ogni sistema sia interno che esterno
- Copie di sicurezza (backup) automatico e programmato della banche dati e loro conservazione
- Integrità delle chiusure dei locali, degli armadi

- Controllo degli accessi
- Verifica del corretto e costante utilizzo dell'eventuale modulistica adottata

Le attività periodiche dovranno essere rendicontate al Titolare del Trattamento attraverso i mezzi stabiliti (report cartacei o digitali) nelle forme e nei modi concordati. Il Titolare del Trattamento si riserva il diritto di verificare, controllare ed ispezionare le attività dei Responsabili e degli Incaricati.

3. Trattamenti con l'ausilio di strumenti elettronici

3.1. Sistema di autenticazione informatica

Procedura di identificazione
In conformità a quanto disposto dalla norma nel caso in cui il trattamento di dati personali è effettuato con strumenti elettronici, il **Responsabile dello specifico trattamento** deve assicurarsi che il trattamento sia consentito solamente agli **Incaricati del trattamento dei dati personali** dotati di **Credenziali di autenticazione** che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Identificazione dell'incaricato
Il trattamento di dati personali, effettuato con strumenti elettronici, è consentito solamente agli **Incaricati del trattamento** dotati di una o più **Credenziali di autenticazione** tra le seguenti:

- Un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo
- Un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave
- Una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

Cautele per assicurare la segretezza della componente riservata della credenziale
Gli incaricati devono adottare le necessarie cautele per assicurare la segretezza della **parola chiave** e custodire diligentemente ogni altro dispositivo che gli è stato affidato per i sistemi di autenticazione informatica (badge magnetici, tessere magnetiche, ecc..).
Inoltre ogni **Incaricato del trattamento** deve essere informato e reso edotto che le **Credenziali di autenticazione**:

- Sono personali
- Devono essere memorizzate
- Non devono essere comunicate a nessuno
- Non devono essere trascritte

Caratteristiche della parola chiave
Il Titolare del Trattamento dispone che ogni credenziale di accesso (parola chiave o password) deve rispettare i seguenti criteri:

- Non deve contenere nomi comuni
- Non deve contenere nomi di persona
- Deve contenere sia lettere che numeri
- Deve contenere almeno 1 carattere speciale
- Deve essere diversa dallo User-Id
- Deve essere lunga 8 caratteri o massimo consentito dal sistema di autenticazione
- Non deve essere riconducibile in modo evidente all'utente

Profilo utente e Permessi utente
Il Titolare del Trattamento, d'intesa con Responsabili di specifici trattamenti, stabilisce per ciascun incaricato o categoria di incaricati un profilo utente che comprende, limita o delimita i permessi operativi e gli accessi ad uno o più trattamenti, procedure informatiche, locali, servizi, uffici, mezzi e strumenti secondo le necessità aziendali.
Il profilo utente si riferisce sia alle componenti informatiche (password, applicazioni disponibili sull'elaboratore elettronico, ecc) che a quelle logistiche (chiavi, badge, ecc).

3.2. Sistema di autorizzazione
Il **Responsabile di uno specifico trattamento di dati personali** nomina gli **Incaricati del trattamento** per ogni tipologia di banca di dati personali trattata.
In particolare il **Responsabile di uno specifico trattamento di dati personali** può decidere quali operazioni di trattamento siano consentite ad ogni **Incaricato del trattamento** tra le seguenti:

- Inserire nuove informazioni nella banca di dati personali
- Accedere alle informazioni in visualizzazione e stampa
- Modificare le informazioni esistenti nella banca di dati personali
- Cancellare le informazioni esistenti nella banca di dati personali

3.3. Altre misure di sicurezza
In considerazione di quanto disposto dalla norma è fatto divieto a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dall'**Amministratore di base di dati** oggetto del trattamento.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal **Responsabile dello specifico trattamento**, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del **Responsabile dello specifico trattamento**, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal **Responsabile dello specifico trattamento**, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

Periodicità di revisione del Documento sulla protezione dei dati personali
Non è definita per legge una priorità di revisione del presente documento, mentre le misure di sicurezza compresi i profili di autorizzazione assegnati agli incaricati, devono essere revisionate con cadenza almeno annuale, si ritiene che sia importante per una corretta Compliance Privacy effettuarne un aggiornamento ogni qualvolta vengano introdotte variazioni significative nella logica di trattamento dei dati personali.

Elenco dei trattamenti di dati personali
L'elenco dei trattamenti è oggetto dell'apposito Registro dei Trattamenti introdotto dal Regolamento Europeo 679/2016 e che è parte integrante del presente documento. Il Responsabile della Protezione dei Dati ha il compito di tenere aggiornato tale registro.

Elenco degli archivi dei dati oggetto del trattamento
Sono stati individuate tre tipologie di banche dati così definite:
Dati amministrativi contabili
Dati dei Dipendenti
Dati degli Alunni e delle Famiglie

Elenco dei sistemi di elaborazione per il trattamento
Al **Titolare del trattamento** attraverso i suoi collaboratori è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione con cui viene effettuato il trattamento dei dati.
Per ogni sistema deve essere specificato:

- Il nome dell'**Incaricato della gestione e della manutenzione**
- Il nome dell'incaricato o degli incaricati che lo utilizzano

- Il nome di uno o più **Incaricati della custodia delle copie delle credenziali**

4. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

Elenco dei soggetti autorizzati al trattamento dei dati
Ogni Responsabile di uno specifico trattamento di dati personali ha il compito di:
- Nominare gli Incaricati del trattamento dei dati personali limitatamente alle Banche di dati di cui sono responsabili
- Assegnare le Credenziali di autenticazione
- Informare l'Amministratore di sistema delle variazioni intervenute nell'assegnazione delle Credenziali di autorizzazione.

L'Amministratore di sistema deve tenere aggiornato ad ogni variazione l'Elenco del personale autorizzato al trattamento dei dati.
L'Elenco del personale autorizzato al trattamento dei dati deve essere redatto dal Responsabile della sicurezza dei dati personali, che deve essere allegato al presente Documento sulla protezione dei dati personali, e deve essere conservato a cura dell'Amministratore di sistema, in luogo sicuro.
Una copia dell'Elenco del personale autorizzato al trattamento dei dati deve essere consegnata all'Incaricato della custodia delle copie delle credenziali.

Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni
L'Amministratore di sistema eventualmente in collaborazione con i Responsabili degli specifici trattamenti di dati personali ha il compito di verificare ogni anno, le Credenziali di autenticazione.
L'Amministratore di sistema deve tenere aggiornato ad ogni variazione l'Elenco del personale autorizzato al trattamento dei dati.
L'Elenco del personale autorizzato al trattamento dei dati deve essere redatto dall'Amministratore di sistema, utilizzando il modulo DTEC_F, che deve essere allegato al presente Documento sulla protezione dei dati personali, e deve essere conservato a cura del Amministratore di sistema, in luogo sicuro.
Una copia dell'Elenco del personale autorizzato al trattamento dei dati deve essere consegnata all'Incaricato della custodia delle copie delle credenziali.

5. Analisi dei rischi

Analisi dei rischi hardware
L'**Amministratore di sistema** in collaborazione con gli **Incaricati della gestione e della manutenzione degli strumenti elettronici**, anche avvalendosi di consulenti interni o esterni, deve verificare ogni anno:
- La situazione delle apparecchiature hardware installate con cui vengono trattati i dati
- La situazione delle apparecchiature periferiche
- La situazione dei dispositivi di collegamento con le reti pubbliche

La verifica ha lo scopo di controllare l'affidabilità del sistema tenendo conto anche dell'evoluzione tecnologica, per quanto riguarda:
- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito

Gli **Incaricati della gestione e della manutenzione degli strumenti elettronici** devono aggiornare il **Report annuale dei rischi hardware** conformemente al modulo DTEC_T.

Gli **Incaricati della gestione e della manutenzione degli strumenti elettronici** nel caso in cui esistano rischi evidenti devono informare tempestivamente l'**Amministratore di sistema** affinché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

Analisi dei rischi sui sistemi operativi e sui software installati
All'**Amministratore di sistema** in collaborazione con gli **Incaricati della gestione e della manutenzione degli strumenti elettronici**, è affidato il compito di verificare ogni anno, la situazione dei Sistemi Operativi e delle applicazioni software installate sulle apparecchiature con cui vengono trattati i dati.
La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi e delle applicazioni software, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito.

Tenendo conto in particolare di:

- Disponibilità di nuove versioni migliorative dei software utilizzati.
- Segnalazioni di Patch, Fix o System-Pack per la rimozione di errori o malfunzionamenti.
- Segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

L'**Amministratore di sistema** in collaborazione con gli **Incaricati della gestione e della manutenzione degli strumenti elettronici**, deve aggiornare il **Report annuale dei rischi sui software installati**.
Gli **Incaricati della gestione e della manutenzione degli strumenti elettronici**, nel caso in cui esistano rischi evidenti, devono informare tempestivamente l'**Amministratore di sistema** affinché siano presi gli opportuni provvedimenti per assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

Analisi degli altri rischi nel trattamento dei dati
Al **Titolare del trattamento** in collaborazione con i **Responsabili degli specifici trattamenti di dati personali**, è affidato il compito di analizzare eventuali altri rischi connessi al trattamento dei dati tenendo conto in particolare di:

- Rischi connessi al comportamento degli operatori
- Rischi connessi al contesto fisico ed ambientale

Il **Titolare del trattamento** in collaborazione con i **Responsabili degli specifici trattamenti di dati personali** deve aggiornare il **Report annuale degli altri rischi** conformemente al modulo DTEC_Z.
I **Responsabili degli specifici trattamenti di dati personali**, nel caso in cui esistano rischi evidenti, devono informare tempestivamente il **Titolare del trattamento** affinché siano presi gli opportuni provvedimenti per assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

Misure da adottare per garantire l'integrità e la disponibilità dei dati
L'**Amministratore di base di dati** in collaborazione con gli **Incaricati della gestione e della manutenzione degli strumenti elettronici**, al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce la periodicità con cui devono essere effettuate le copie di sicurezza delle banca di dati trattati.
I criteri devono essere definiti in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

Gli **Incaricati della gestione e della manutenzione degli strumenti elettronici**, per ogni banca di dati devono predisporre le istruzioni di copia, verifica e ripristino dei dati.

Se possibile per ogni banca di dati si deriniscano le seguenti specifiche:

- Il Tipo di supporto da utilizzare per le Copie di sicurezza dei dati.
- Il numero di Copie di sicurezza dei dati effettuate ogni volta
- Se i supporti utilizzati per le Copie di sicurezza dei dati sono riutilizzati e in questo caso con quale periodicità .
- Se per effettuare le Copie di sicurezza dei dati si utilizzano procedure automatizzate e programmate.
- Le modalità di controllo delle Copie di sicurezza dei dati.

- La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
- Il nome dell'incaricato a cui è stato assegnato il compito di effettuare le Copie di sicurezza dei dati.
- Le istruzioni e i comandi necessari per effettuare le Copie di sicurezza dei dati.
- Le istruzioni e i comandi necessari per effettuare il ripristino delle Copie di sicurezza dei dati.

Istruzioni di Backup
Le operazioni di backup vanno condotte seguendo le procedure previste dal Sistema Operativo in uso e dal software in dotazione.
All'**Amministratore di sistema** e all'**Amministratore di base di dati,** in collaborazione con gli **Incaricati della gestione e della manutenzione degli strumenti elettronici**, e con gli **Incaricati delle copie di sicurezza delle banche dati** è affidato il compito di verificare ogni anno periodicamente le necessità di formazione del personale incaricato di effettuare le Copie di sicurezza delle banca di dati trattate, in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica.
Se necessario sarà disposta un'apposita sessione formativa per gli incaricati del backup.

6. Misure da adottare per la protezione di dati personali, rilevanti ai fini della loro custodia e accessibilità

Misure generali
In considerazione di quanto disposto dalla norma, è fatto divieto a chiunque di:
- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dall'**Amministratore di sistema** o dal **Responsabile dello specifico trattamento di dati personali** oggetto del trattamento.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal **Responsabile dello specifico trattamento di dati personali**, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del **Responsabile dello specifico trattamento di dati personali**, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal **Responsabile dello specifico trattamento di dati personali**, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

Formazione degli incaricati del trattamento

Piano di formazione
Il **Titolare del trattamento**, in collaborazione con i **Responsabili degli specifici trattamenti di dati personali**, valuta per ogni incaricato a cui è stato affidato il trattamento, sulla base dell'esperienza, delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, la necessità di pianificare interventi di formazione.
La formazione è programmata già al momento dell'ingresso in servizio di nuovi incaricati del trattamento, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.
Il Piano di formazione del personale può essere composto anche di sessioni plenarie su argomenti comuni in materia di sicurezza dei dati.

Criteri da adottare per garantire l'adozione delle misure di sicurezza adeguate in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare

Il **Titolare del trattamento**, può decidere di affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.
Il **Titolare del trattamento**, deve redigere e aggiornare ad ogni variazione l'elenco dei soggetti che effettuano il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, ed indicare per ognuno di essi il tipo di trattamento effettuato specificando:
- I soggetti interessati

- I luoghi dove fisicamente avviene il trattamento dei dati stessi
- I responsabili del trattamento di dati personali

Per l'inventario dei soggetti a cui affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, deve essere utilizzato il modulo DTEC_E, che deve essere allegato al presente Documento sulla protezione dei dati personali, e deve essere conservato a cura del **Responsabile della sicurezza dei dati personali**, in luogo sicuro.

Nel caso in cui, per i trattamenti dei dati affidati in tutto o in parte all'esterno della struttura del titolare, sia possibile nominare responsabili del trattamento soggetti controllabili dal **Titolare del trattamento** stesso (relativamente alle modalità e alle misure minime di sicurezza da adottare nel trattamento stesso), è possibile indicare gli stessi **Responsabili del trattamento in Out-sourcing**,
In questo caso, il **Titolare del Trattamento** ha la facoltà di verificare che il Responsabile del trattamento in Out-sourcing, applichi correttamente le misure minime di sicurezza, nel trattamento dei dati che gli viene affidato.

Enti terzi cui è affidato li trattamento dei dati in out-sourcing
Al fine di consentire la corretta e completa gestione delle attività e finalità, il Titolare avendo analizzato esigenze operative e strutture tecniche che offrono le necessarie garanzie di sicurezza, adotta supporti e servizi esterni esterni (out-sourcing) limitatamente ad al alcuni specifici trattamenti.
La lista dei trattamenti in outsorcing deve essere aggiornata a cura del Responsabili dei Trattamenti: qualsiasi modifica o variazione deve essere concordata e autorizzata dail Titolare.
Il **Titolare del trattamento**, può affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare a quei soggetti terzi che abbiano i requisiti di esperienza, capacità ed affidabilità.
Il Titolare a cui è stato affidato il trattamento dei dati all'esterno deve rilasciare una dichiarazione scritta da cui risulti che sono state adottate le di sicurezza per il trattamento ai sensi del GDPR.
Per ogni trattamento affidato ad un soggetto esterno alla struttura del titolare, il **Titolare del trattamento** deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.
Il **Responsabile del trattamento in Out-sourcing** deve accettare la nomina, secondo il modello a meno che non se ne assume la diretta responsabilità il Titolare stesso ed è tenuto al rispetto delle indicazioni fornitegli nella lettera di incarico..
La nomina del **Responsabile del trattamento in Out-sourcing** deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del **Titolare del trattamento** in luogo sicuro.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari
In conformità a quanto disposto dalla norma al fine di garantire la sicurezza dei dati sensibili o giudiziari contro l'accesso abusivo, l'**Amministratore di sistema in collaborazione** con l'**Amministratore di rete**, deve stabilire, con il supporto tecnico degli **Incaricati della gestione e della manutenzione degli strumenti elettronici**, le misure tecniche da adottare in rapporto ad eventuali rischi.
I criteri devono essere definiti dall' **Amministratore di rete** in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.
In particolare per ogni Sistema interessato devono essere definite le seguenti specifiche:

- individuare gli idonei strumenti per la protezione degli strumenti elettronici contro il rischio di intrusione e dell'azione di programmi informatici aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.
- stabilire la frequenza con cui aggiornare i programmi per elaboratore per prevenire la vulnerabilità degli strumenti elettronici e correggerne difetti.
- individuare come proteggere, mediante l'utilizzo di idonei strumenti elettronici, i dati sensibili o giudiziari contro l'accesso abusivo da parte di chiunque abusivamente si introduce nel sistema informatico o telematico.

Per ogni sistema deve essere redatta una scheda periodica comprovante l'avvenuta manutenzione e verifica dello stato complessivo del sistema e dell'efficacia delle misure di sicurezza.

Per ogni **supporto utilizzato per le operazioni di copia** deve essere individuato il luogo di conservazione in modo che sia convenientemente protetto dai potenziali rischi di:

- Agenti chimici
- Fonti di calore
- Campi magnetici
- Intrusioni e atti vandalici
- Incendio
- Allagamento
- Furto
- Accesso non autorizzato
- Trattamento non consentito

L'accesso ai supporti utilizzati per le copie dei dati è limitato per ogni banca di dati a:

- Incaricati delle copie di sicurezza delle banche dati
- Amministratore di sistema
- Amministratore di base di dati

L'**Amministratore di base di dati** è responsabile della custodia e della conservazione dei supporti utilizzati per le copie dei dati.
Se l'**Amministratore di base di dati** decide che i supporti magnetici contenenti dati sensibili o giudiziari non siano più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto annullando e rendendo intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso contenute.
E' compito dell'**Amministratore di base di dati** controllare e assicurarsi che in nessun caso vengano lasciate copie di **Banche di dati** contenenti dati sensibili o giudiziari, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso registrate.
La decisione di ripristinare la funzionalità degli elaboratori elettronici guasti, è compito esclusivo dell'**Amministratore di sistema** che si può avvalere del parere dell'**Incaricato della gestione e della manutenzione degli strumenti elettronici**.

Trattamenti di dati sanitari o di particolare rilevanza
I dati sanitari e i dati sensibili in generali devono essere sempre sottoposti alle massime misure di sicurezza disponibili.
I documenti cartacei saranno custoditi in cassetti, armadi, casseforti o locali con chiusura idonea e funzionante: la gestione delle chiavi e degli accessi è del Responsabile dello specifico trattamento di dati cui la documentazione si riferisce. Se la documentazione si riferisce a più ambiti di trattamento, la gestione sarà concordata da tutti i Responsabili interessati.
I documenti digitali, di qualunque forma o natura e in qualsivoglia sistema fisico conservati, devono essere soggetti ad accesso con credenziali. Se possibile i dati devono essere crittografati secondo uno standard prestabilito in modo da prevenire il più possibile l'accesso non autorizzato anche in caso di violazione della sicurezza.

Descrizione degli interventi effettuati da soggetti esterni
Nel caso in cui ci si avvalga di soggetti esterni alla propria struttura, per provvedere al controllo del buon funzionamento hardware e/o software degli strumenti elettronici e alla eventuale riparazione, aggiornamento o sostituzione, il **Titolare del trattamento**, deve farsi consegnare puntualmente dal personale che ha effettuato l'intervento tecnico, una dichiarazione scritta (Rapporto di lavoro) con la descrizione dettagliata delle operazioni eseguite che attesti la conformità a quanto stabilito dalla norma e concordato con il Responsabile.
Secondo quanto disposto dal **provvedimento del Garante per la privacy del 27 novembre 2008 pubblicato nella Gazzetta Ufficiale del 24 dicembre 2008**, nel caso di servizi si amministrazione di sistema affidati in outsourcing, il T**itolare del trattamento**, deve conservare direttamente e specificatamente per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali **Amministratori di sistema.**

7 . Ulteriori disposizioni di sicurezza per il trattamento di dati senza l'ausilio di strumenti elettronici

Ulteriori disposizioni di sicurezza in merito al trattamento di documenti cartacei o digitali sono contenuto nel Codice di Condotta e riassunti nella Lettera di Incarico firmata per accettazione da ogni incaricato.
E' fatto divieto a chiunque di:

- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal **Responsabile della sicurezza dei dati personali,** di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del **Responsabile della sicurezza dei dati personali**, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal **Responsabile della sicurezza dei dati personali**, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

8. Controllo degli accessi

L'accesso agli archivi e ai locali di persone e personale esterno e di visitatori deve essere controllato e registrato dagli incaricati del controllo degli accessi che dovranno riportare sull'apposito modulo tutti gli ingressi. L'incaricato del controllo degli accessi deve assicurarsi che la persona sia effettivamente ricevuta da u Responsabile o da un Incaricato seguendo le disposizioni operative ricevute.

9. Diritti dell'interessato

Facendo riferimento comunque alla norma, all'interessato vengono garantiti i diritti sanciti dagli artt. 15-21 del GDPR nei limiti e nei modi previsti dalla norma stessa
L'esercizio dei diritti viene esercitato con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un delegato, alla quale è fornito idoneo riscontro senza ritardo.
L'interessato può esercitare i suoi diritti anche con ricorso formale o con ricorso al Garante della Privacy come previsto dalla norma e dal Codice.
La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. La richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile che la recepisce acquisendo anche la controfirma dell'interessato.
I diritti riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.
La richiesta è formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.

Riscontro all'interessato

All'interessato viene garantito idoneo riscontro in modo intelligibile, chiaro e completo in relazione alla sua richiesta; il riscontro viene inoltrato formalmente e acquisito agli atti. Se il riscontro prevede la comunicazione di informazioni tecniche dovranno essere fornite le opportune e necessarie informazioni per la loro decodifica.
Il Titolare può decidere sull'opportunità di informare i Responsabili o gli incaricati di un ricorso ricevuto al fine di motivare o introdurre modifiche operative o funzionali derivanti dal ricorso stesso.
Quando, a seguito della richiesta di esercizio dei diritti non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico. Il contributo spese deve essere versato tramite circuito bancario o postale e non direttamente a qualsiasi titolo ad un Responsabile o ad un incaricato.