Istruzioni operative contenenti le modalità per il trattamento dei dati personali e gli obblighi inerenti alle misure di sicurezza da adottare da parte dei soggetti Autorizzati ai sensi del punto 4 della Direttiva del Ministro dell'Istruzione n. 194/2020

1. Tipologie di dati trattati

a) Dati personali identificativi (art. 4, punto 1 del Regolamento) riferiti a:

- personale della scuola, familiari e conviventi, inclusi i minori, del personale della scuola;
- studenti;
- dipendenti in organico presso la struttura di competenza;
- familiari e conviventi, inclusi i minori, dei dipendenti in organico presso l'Ufficio di competenza;
- fornitori e collaboratori del Ministero;
- referenti, dipendenti e legali rappresentanti di altri enti e istituzioni operanti in ambito nazionale e internazionale;
- stagisti;
- parti, controparti e soggetti terzi, coinvolti nei procedimenti amministrativi di competenza.

b) Dati personali di natura particolare (art. 9 Regolamento) riferiti a:

- personale della scuola;
- studenti;
- dipendenti in organico;
- familiari e conviventi, inclusi i minori, dei dipendenti in organico.

c) Dati personali giudiziari (di cui all'art. 10 Regolamento) riferiti a soggetti coinvolti nei procedimenti amministrativi o giudiziari di competenza:

- dipendenti;
- parti, controparti;
- soggetti terzi.

2. Principi

Il soggetto Autorizzato al trattamento dei dati personali deve:

- assicurare la riservatezza, nonché la protezione dei dati personali dei quali venga a conoscenza durante l'esecuzione delle attività svolte;
- utilizzare i dati personali solo per le finalità connesse allo svolgimento delle attività di competenza, con divieto di qualsiasi altra diversa utilizzazione;
- porre in essere tutte le azioni idonee a garantire il rispetto delle vigenti disposizioni in materia di protezione dei dati personali, segnalando tempestivamente al soggetto che esercita le funzioni di Designato ogni eventuale problema applicativo;

- garantire il rispetto della normativa nelle attività di consultazione e gestione della documentazione contenente dati personali, con riguardo anche alla custodia ed archiviazione della stessa;
- salvaguardare la conformità delle riproduzioni dei documenti agli originali ed evitare ogni azione diretta a manipolare, dissimulare o deformare fatti, testimonianze, documenti e dati;
- controllare e custodire fino alla restituzione gli atti e i documenti contenenti dati personali affidatigli per lo svolgimento dei propri compiti in maniera che ad essi non accedano persone prive di autorizzazione, restituendoli al termine delle operazioni affidate;
- rispettare le misure di sicurezza volte a prevenire l'eventuale distruzione, dispersione o accesso non autorizzato ai documenti, adottando, in presenza di specifici rischi, particolari cautele quali la consultazione in copia di alcuni documenti e la conservazione degli originali in cassaforte o armadi blindati, ove presenti;
- non fare alcun uso improprio e mantenere riservate le notizie e le informazioni concernenti i dati personali non resi pubblici, appresi nell'esercizio delle proprie attività, osservando tali doveri di riserbo anche dopo la cessazione dell'attività lavorativa.

I dati personali devono essere trattati nel rispetto dei seguenti principi:

- **liceità:** ogni trattamento deve essere conforme alle disposizioni in materia di protezione dei dati personali e, in particolare, nella misura in cui ricorra almeno una delle condizioni di cui all'art. 6, par. 1, del Regolamento;
- **correttezza e trasparenza:** il trattamento deve essere esplicitamente chiarito agli interessati, fornendo loro le informazioni necessarie a far comprendere in modo adeguato non solo le modalità del trattamento, ma anche le eventuali conseguenze;
- **sicurezza e riservatezza:** devono essere realizzate misure tecniche e organizzative di sicurezza appropriate ai rischi presentati dal trattamento, secondo le indicazioni ricevute.

I dati devono essere trattati esclusivamente per finalità (principio della limitazione della finalità):

- **determinate** e **direttamente correlate allo svolgimento delle proprie funzioni**, non essendo consentita la raccolta fine a sé stessa;
- **esplicite**, in quanto il soggetto interessato va informato sulle finalità del trattamento;
- **legittime**, nel senso che il fine della raccolta dei dati, oltre al trattamento, deve essere lecito;
- **compatibili** con il presupposto per il quale sono inizialmente trattati, in precipuo riferimento alle finalità esplicite e determinate, specialmente per le operazioni di comunicazione e diffusione degli stessi.

I dati devono essere:

- **esatti,** ossia precisi e rispondenti al vero e, se necessario, aggiornati;
- **adeguati, pertinenti e strettamente limitati** a quanto necessario rispetto alle finalità esplicite e determinate per le quali sono trattati, in quanto devono essere raccolti solo i dati che sono al contempo

strettamente necessari, sufficienti e non esuberanti in relazione ai fini, la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso (principio di minimizzazione dei dati);
- **conservati** per tutto il periodo strettamente necessario.

3. Sicurezza dei dati

3.1 Norme logistiche per l'accesso fisico ai locali

È necessario evitare che i dati personali trattati possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Pertanto, si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato.

Laddove si esegue il trattamento di dati personali, deve essere possibile riporre in luogo sicuro i documenti cartacei e i supporti rimovibili contenenti tali dati. Pertanto, le porte degli uffici e almeno un armadio per ufficio devono essere dotati di serratura con chiave.

3.2 Istruzioni per l'uso degli strumenti informatici

Si fa presente che sia i dispositivi di memorizzazione del proprio PC sia le unità di rete devono contenere informazioni e dati esclusivamente collegati allo svolgimento della propria attività lavorativa e non possono essere utilizzati per scopi diversi.

3.2.1 Gestione strumenti elettronici (PC fissi e portatili)

Ciascun soggetto autorizzato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). È tenuto a rispettare le misure di sicurezza per la tutela della riservatezza, al fine di evitare l'accesso ai dati da parte di soggetti non autorizzati.

Per la gestione della sessione di lavoro sul PC (fisso), si precisa che:
- al termine dell'orario di lavoro, il PC deve essere spento;
- se il soggetto autorizzato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto, deve chiudere la sessione di lavoro sul PC facendo Logout oppure deve attivare il blocco del PC (usando, ad esempio, la combinazione di tasti Win+L);
- relativamente all'utilizzo della funzione di blocco del PC, dopo un determinato periodo di inattività del PC, essa si attiva automaticamente;
- quando si esegue la stampa di un documento contenente dati personali su una stampante in rete, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non autorizzati. In alternativa, è possibile attivare la funzione "stampa trattenuta" nelle proprietà "base" della stampante alla voce "lav. di stampa" che permette di non stampare il documento fino a quando l'utente non inserisca le credenziali di autenticazione.

Per l'utilizzo dei PC portatili dati in dotazione valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:

- non lasciare mai incustodito il PC portatile e tenerlo assicurato alla scrivania o ad elementi "sicuri" dell'arredamento (maniglie, intelaiature…) utilizzando gli appositi cavi in acciaio forniti dall'Amministrazione;
- per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno (es. armadio chiuso a chiave, cassaforte);
- in caso di furto di un PC portatile è necessario, dopo aver presentato denuncia alle Forze dell'ordine, darne comunicazione tempestiva all'ufficio competente dalla Direzione generale per i sistemi informativi e la statistica, onde prevenire possibili intrusioni nei sistemi informatici;
- in caso di viaggio aereo trasportare tassativamente il portatile come bagaglio a mano;
- eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile; il backup può essere effettuato facendo una copia della cartella presente nel percorso D:\Users\MIxxxxx, relativa al proprio nome utente.

3.2.2 Gestione username e password

L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede al soggetto autorizzato di inserire un nome utente (username) e una parola chiave (password). L'utilizzo della combinazione username/password è fondamentale in quanto:

- tutela da accessi illeciti alla rete, ai dati e, in generale, da violazioni e danneggiamenti del patrimonio informativo;
- tutela il soggetto autorizzato da false imputazioni, garantendo che nessuno possa operare a suo nome con il suo profilo (furto identità digitale);
- è necessario per gestire correttamente gli accessi a risorse condivise.

Ciascun soggetto autorizzato deve scegliere la password in base ai criteri standard di sicurezza quali: combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole; diversificare dalle precedenti; effettuare un cambio frequente; conservare in luogo sicuro; non rivelare o condividere la password con i colleghi di lavoro, familiari e amici, soprattutto attraverso il telefono; non attivare la funzione che permette di salvarla e richiamarla automaticamente da alcune applicazioni.
Si raccomanda, inoltre, di non scegliere password già utilizzate per l'accesso ad altri sistemi esterni a quelli dell'Amministrazione.

3.2.3 Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione è vietata. Solo in casi particolari e motivati è possibile fare richiesta di installazione hardware e software aggiuntivo tramite i referenti informatici che inoltreranno la richiesta alla Direzione generale per i sistemi informativi e la statistica che ne valuterà l'opportunità.
In generale è vietato l'uso di programmi portabili (eseguibili senza installazione) e, in generale, di tutti i software non autorizzati dalla Direzione generale per i sistemi informativi e la statistica.

Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Nel caso in cui si renda indispensabile l'utilizzo di una o più cartelle condivise in rete tra i dipendenti di un ufficio, è necessario inoltrare richiesta alla Direzione generale per i sistemi informativi e la statistica attraverso il referente informatico e specificare nella stessa i soggetti che possono avere accesso al contenuto delle singole cartelle. Si precisa che non possono essere salvati file contenenti dati personali su cartelle condivise, salvo che non siano previsti accessi limitati ai soli soggetti autorizzati al trattamento di tali dati personali.

3.2.4 Gestione posta elettronica istituzionale

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti interni ed esterni per le finalità del Ministero dell'Istruzione (di seguito MI).
Al fine di non compromettere la sicurezza del Sistema Informativo del MI, occorre adottare le seguenti norme comportamentali:

- se si ricevono e-mail da destinatari sconosciuti contenenti tipi di file sospetti, procedere alla loro immediata eliminazione;
- è fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list che esulano dalla propria attività lavorativa.

Nell'ipotesi in cui la e-mail debba essere utilizzata per la trasmissione di categorie particolari di dati, si raccomanda di prestare attenzione a che:

- il destinatario sia effettivamente competente e autorizzato a ricevere i dati inviati;
- l'indirizzo del destinatario sia stato correttamente digitato;
- l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
- nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio.

3.2.5 Gestione del salvataggio dei dati

Per i dati e i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle condivise di rete e database, sono eseguiti i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali file distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.
Per i dati ed i documenti che risiedono esclusivamente sul PC, è opportuno effettuare copie di backup.

3.2.6 Gestione dei supporti rimovibili

I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri soggetti non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati opportunamente formattati al fine di non consentire il recupero dei dati rimossi. Il trasferimento di file contenenti dati personali su supporti rimovibili è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. Si raccomanda di proteggere con password i supporti rimovibili contenenti dati personali.

3.2.7 Protezione dai virus informatici

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni PC del MI è stato installato un software antivirus che si aggiorna automaticamente all'ultima versione disponibile.

L'antivirus non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.

Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus oppure si sospetti la presenza di un virus non rilevato dal programma antivirus, è necessario segnalarlo all'assistenza tecnica.

Si raccomanda di non scaricare e né tantomeno aprire file sospetti provenienti via e-mail da mittenti sconosciuti. Tali file possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in esso contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

3.2.8 Richieste di pubblicazioni sul sito istituzionale

Per le richieste di pubblicazione on line di contenuti, informazioni e documenti che contengono dati personali sui siti istituzionali dell'Amministrazione, devono essere opportunamente contemperate le esigenze di pubblicità e trasparenza con i diritti e le libertà fondamentali, nonché la dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali previste dalla normativa vigente. A tal fine, le richieste di pubblicazione di contenuti in cui sono presenti dati personali, dovranno essere preventivamente autorizzate dal soggetto che esercita le funzioni di Titolare/Designato che valuterà l'esistenza di idonei presupposti normativi. Si raccomanda di far riferimento, per le parti ancora vigenti, alle Linee guida del Garante per la protezione dei dati personali in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati"(Pubblicato sulla Gazzetta Ufficiale n. 134 del 12 giugno 2014 e rinvenibili sul sito web del Garante).

3.3 Istruzioni per l'uso degli strumenti "non elettronici"

Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio microfilm, microfiches e lucidi. I documenti contenenti dati personali devono essere custoditi in appositi armadi o cassettiere dotate di chiavi. Tali documenti, quando si ritiene debbano essere eliminati, devono essere distrutti.

Per proteggere i dati personali è obbligatorio evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), nonché in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro e al termine dell'orario di lavoro.

In particolare, si richiede in ogni ufficio la presenza e l'uso tassativo di armadi e/o cassettiere dotati di serratura adeguata.

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzano strumenti per la riproduzione cartacea di documenti digitali sono tenuti a procedere alla relativa distruzione del supporto qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie.

Il soggetto autorizzato deve attenersi alle seguenti prescrizioni:

- in nessun caso è concesso l'accesso a documentazione contenente dati personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti autorizzati;
- è severamente vietato utilizzare documenti contenenti dati personali, come carta da riciclo o da appunti;
- l'accesso ai documenti deve essere limitato al tempo necessario a svolgere i trattamenti previsti;
- il numero di copie di documenti contenenti dati personali deve essere strettamente funzionale alle esigenze di lavoro;
- ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale autorizzato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
- l'accesso agli archivi deve essere controllato permettendo l'accesso ai soli soggetti autorizzati.

Il sottoscritto ……. in servizio presso l'Ufficio VI Ambito territoriale per la provincia di Sassari della Direzione Generale dell'USR Sardegna, dichiara di aver ricevuto le suddette istruzioni operative contenenti le modalità per il trattamento dei dati personali e gli obblighi inerenti alle misure di sicurezza, che si impegna a seguire e a rispettare, avendole attentamente esaminate e comprese.

(data)_____ (firma dell'autorizzato) _____

IL DIRIGENTE
ANNA MARIA MASSENTI
Firmato digitalmente ai sensi
del c.d. Codice dell'Amministrazione
digitale e norme ad esso connesse

Firmato digitalmente da
MASSENTI ANNA MARIA
C=IT
O=MINISTERO
DELL'ISTRUZIONE