Ministero dell'Istruzione
Ufficio Scolastico Regionale per la Lombardia
Ufficio X Ambito Territoriale di Milano
Via Soderini 24– 20146 Milano - Codice Ipa: m_pi

IL DIRIGENTE

VISTO il Decreto legislativo 30 marzo 2001, n. 165 e successive modificazioni, recante «Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche»;

VISTO il Regolamento (UE) del 27 aprile 2016 n. 2016/679 del Parlamento Europeo e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito Regolamento);

VISTO il Decreto legislativo 30 giugno 2003, n. 196, modificato dal Decreto legislativo 10 agosto 2018, n. 101 (di seguito anche D. Lgs. 101/2018), contenente le disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento;

VISTI il Regolamento di organizzazione del Ministero dell'Istruzione, dell'Università e della Ricerca (di seguito, MIUR) approvato il Decreto del Presidente del Consiglio dei Ministri 11 febbraio 2014, n. 98;

VISTI il Decreto Ministeriale 26 settembre 2014, n. 753, così come modificato dal Decreto Ministeriale 5 febbraio 2018, n. 100, recante l'individuazione degli uffici di livello dirigenziale non generale dell'Amministrazione centrale del MIUR, nonché i Decreti 18 dicembre 2014 (dal numero 908 al numero 925), relativi all'organizzazione e ai compiti degli Uffici di livello dirigenziale non generale in cui si articolano gli Uffici Scolastici regionali;

VISTA la Direttiva del Ministro dell'Istruzione, dell'Università e della Ricerca 25 marzo 2019, n. 239 (di seguito, "Direttiva"), che individua le modalità organizzative di gestione delle attività di trattamento dei dati personali nell'ambito del MIUR in linea con la normativa europea e nazionale di riferimento;

VISTE le Linee guida relative al processo di gestione della *privacy* del MIUR;

VISTO il punto 2 della Direttiva, che individua nel Capo di Gabinetto, nei Capi dei Dipartimenti e nei Dirigenti generali o nei Dirigenti preposti agli Uffici scolastici regionali i soggetti mediante i quali il Ministero esercita le funzioni di Titolare del trattamento dei dati personali;

VISTO il punto 4 della Direttiva, ai sensi del quale "i soggetti che esercitano le funzioni di Titolare possono affidare specifici compiti e funzioni, connessi al trattamento dei dati, a dirigenti, che da essi dipendono, designandoli espressamente ed impartendo apposite istruzioni. I soggetti designati svolgono i compiti e le funzioni ad essi affidati nell'ambito delle proprie competenze per i trattamenti connessi ai processi di cui sono responsabili";

VISTO il decreto del D.G. n.16798 del 07/10/2019 con il quale il soggetto che esercita le funzioni Titolare del trattamento di dati personali ha designato il Dirigente dell'Ufficio Scolastico territoriale di Milano, dott. Marco Bussetti a svolgere specifici compiti e funzioni ad esso affidate*;*

CONSIDERATO che i soggetti autorizzati al trattamento dei dati personali, di cui al punto 5 della Direttiva, sono i Dirigenti generali e non generali in relazione alle competenze degli Uffici cui sono

preposti e il personale non dirigente in servizio e il personale della scuola comandato e/o assegnato nei limiti delle competenze attribuite all'ufficio o alla struttura di appartenenza;

CONSIDERATO che, con riferimento al personale non dirigente in servizio e al personale della scuola comandato, per specifiche attività è opportuno individuare nominativamente i dipendenti autorizzati al trattamento dei dati personali nell'ambito dell'Ufficio diretto, fornendo loro le relative istruzioni;

CONSIDERATO che i dipendenti indicati nel successivo art. 1, *prestano attualmente la loro attività* all'interno dell'Ufficio X- Ufficio scolastico territoriale di Milano- della Direzione generale dell'USR Lombardia*;*

CONSIDERATO che le mansioni assegnate comportano lo svolgimento di attività di trattamento di dati personali;

CONSIDERATO che il Titolare del Trattamento ha l'obbligo di adottare specifiche misure organizzative e di impartire istruzioni a tutti coloro che sono stati autorizzati al trattamento dei dati personali (artt. 5, 24, 29 e 32 del Regolamento);

DECRETA

Articolo 1

I sotto indicati dipendenti, in servizio presso l'Ufficio Scolastico territoriale di Milano dell'USR Lombardia, in qualità di soggetti Autorizzati ai sensi del punto 5 della Direttiva, possono effettuare il trattamento di tutti i dati personali e tutte le operazioni/tipologie di trattamento, nei limiti di quanto indicato nell'art. 2 e nel rispetto delle istruzioni contenute in allegato. Il rispetto dei medesimi limiti e istruzioni fa parte integrante della prestazione lavorativa e, pertanto, è obbligatorio in base al vigente contratto di lavoro:

Cognome	**Nome**
Aliperti	Claudio
Ambrosetti	Nadia
Amoroso	Ilaria
Antonucci	Pasqua
Basile	Ilaria
Basile	Vincenzina
Basileo	Paolo
Bassi	Luisa
Belluomo	Giovanna
Belvedere	Giuseppe
Bevilacqua	Mariangela
Buscaino	Rosa
Calderari	Monica
Caligiuri	Tommaso
Cassani	Giuliana Maria

Ciccotti	Antonio
Ciriolo	Eros
Comunello	Andrea Maria
Cozzolino	Rossana
Croce	Maria
D'Angelo	Angela
Dall'Anese	Italia
De Cesare	Stefano
De Pari	Angela
Delle Fave	Alberto
Del Vecchio	Paola
Destefano	Daniela Maria
Di Benedetto	Veronica
Di Fabio	Sergio
Di Grado	Miriam
Dicuonzo	Giovanna
Donatelli	Luca
Falivene	Antonio
Favata	Antonio
Fedele	Maria Teresa
Ferraro	Antonio
Fierro	Linda
Fois	Annalisa
Fumagalli	Daniela Maria
Fumante	Mariano
Galdi	Filomena
Gallo	Carmela
Gallo	Carmine
Gamberi	Alessandro
Gigantiello	Cosimo
Goffredo	Antonio
Leopardi	Maria Agnese
Leronni	Anna

Lopis	Caterina
Lovino	Isabella
Luberto	Rosalia
Maestri	Mario
Malara	Antonella
Marino	Giuseppina
Mazzola	Sandro
Meale	Franca Paola Elena
Miele	Gennaro
Miro	Carmela
Molfese	Antonio Lucio
Morelli	Alfredo
Mori	Giulia
Mungiguerra	Pasquale
Nigro	Imperiale Giulia
Passarelli	Antonietta
Passini	Roberto Matteo
Petrucelli	Stefano
Portaluri	Lucrezia Maria
Proietti	Laura
Pugliese	Carmela
Ragozzino	Filomena
Raimondi	Mariangela Damiana
Rappazzo	Patrizia
Rea	Francesco
Recupito	Claudio Severino
Rizzo	Domenica
Robles	Felicia Annamaria
Robles	Pasquale
Romano	Emanuela Lucia
Rossini	Maria Stella
Russano	Michela
Salomone	Silva

Savoja	Alessandro
Schirripa	Teodora
Scotto	Silvia
Scribano	Carmela Concetta
Scribano	Gabriella
Scutiero	Elvira
Serafino	Francesco
Simoneschi	Angela
Sirleto	Maria Luisa
Spanò	Mario
Stampini	Laura
Stroscio	Anna
Tallarico	Tommaso
Turotti	Laura
Varricchio	Antonietta
Varvo	Maria Rosaria
Verzino	Maurizio
Vicenti	Immacolata
Vigo	Annamaria
Vitale	Annamaria
Vitrone	Carmela
Volpe	Rosanna

Articolo 2

Gli stessi sono tenuti a limitare il trattamento dei dati a quanto necessario ed indispensabile all'adempimento delle mansioni assegnate a ciascun dipendente nell'ambito dell'organizzazione dell'Ufficio di appartenenza o delle attività svolte dal personale della scuola impiegato presso l'A.T. di Milano, osservando inderogabilmente le norme di legge, i regolamenti interni, le linee guida di riferimento, le circolari, gli ordini di servizio, le istruzioni comunque impartite dal Titolare del Trattamento e/o dai suoi Designati.

Articolo 3

Sono tenuti altresì a partecipare in via obbligatoria ai corsi di formazione in materia di disciplina della protezione dei dati, dei quali sarà data comunicazione da parte del soggetto che esercita le funzioni di Titolare o del suo Designato.

Articolo 4

Gli obblighi sopra descritti fanno parte integrante della prestazione lavorativa e, pertanto, sono dovuti in base al vigente contratto di lavoro.

Articolo 5

Il presente atto ha efficacia fino alla risoluzione del rapporto di lavoro per qualsiasi causa oppure fino a modifica o revoca da parte del soggetto che esercita le funzioni di Titolare o del suo Designato.

Articolo 6

Le istruzioni in allegato costituiscono parte integrante del presente atto e vengono notificate ai soggetti Autorizzati con pubblicazione sul sito dell'A.T. di Milano.

IL DIRIGENTE DESIGNATO DEL TRATTAMENTO
Marco BUSSETTI

Firmato digitalmente ai sensi del Codice
dell'Amministrazione digitale e norme ad esso connesse

Firmato digitalmente da
BUSSETTI MARCO
C=IT
O=MINISTERO
DELL'ISTRUZIONE

Allegato - Istruzioni

1. Tipologie di dati trattati

Le tipologie dei dati personali trattati dal personale autorizzato in servizio presso l'Ufficio Scolastico di Milano, vengono indicate, a titolo esemplificativo, per settore di riferimento ed in linea con quanto indicato nel Registro delle attività di trattamento dei dati, come di seguito:

Settore I – Legale-:

-Supporto alle Istituzioni scolastiche nella gestione del contenzioso;
-Gestione del contenzioso con il patrocinio dell'Avvocatura dello Stato o su delega della stessa, esecuzione dei relativi provvedimenti e gestione dei ricorsi al Presidente della Repubblica;
-Gestione dei procedimenti cautelari e disciplinari del personale scolastico;
-Procedimenti per responsabilità penale e amministrativo-contabile;
-Interdizione da incarichi, uffici e servizi in scuole, istituti pubblici e privati del personale scolastico;
-Gestione richieste Accesso Civico;

Settore II – organico docenti primo ciclo:

-Autorizzazione al Part-time del personale docente di primo ciclo;
-Operazione di nomina del personale a tempo indeterminato della scuola
-Procedure di riammissione in servizio

Settore III- organico docenti secondo ciclo:

-Autorizzazione al Part-time del personale docente di secondo ciclo;
- Operazione di nomina del personale a tempo indeterminato della scuola
-Procedure di riammissione in servizio

Settore IV- organico ATA:

-Attribuzione delle Posizioni Economiche del Personale ATA;
-Autorizzazione al Part-time del personale ATA
-Utilizzazione del personale docente "inidoneo" ;
-Operazione di nomina del personale ATA a tempo indeterminato;

Settore V – mobilità docenti ed ATA:

-Riconoscimento al personale scolastico di permessi retribuiti per motivi di studio
-Gestione delle domande di mobilità, utilizzazione e assegnazione provvisoria del personale scolastico

Settore VI –graduatorie personale docente:

-Gestione delle graduatorie per il reclutamento del personale docente

Settore VII – risorse finanziarie e strumentali dell'Ufficio:

-Erogazione di contributi statali a scuole paritarie e sezioni primavera;
-Consulenza e supporto alle scuole per le procedure amministrativo-contabili;
-Rilascio e rinnovo tessere di riconoscimento a favore del personale della scuola e amministrativo dell'USR e de Gestione amministrativo contabile delle risorse finanziarie;
-Pagamento di provvidenze a favore del personale scolastico e dipendente dell'USR i loro familiari;
-Acquisizione e gestione di beni e servizi e pagamento delle fatture ai fornitori. Esecuzione delle attività connesse all'incarico di Consegnatario;
-Recupero dei crediti erariali;

settore VIII – comunicazione, risorse umane e funzioni di segreteria:

-Abilitazioni ai profili di accesso alle piattaforme MIUR (a titolo esemplificativo POLIS, SIDI, Plico telematico);
-Gestione, supporto e consulenza alle istituzioni scolastiche e della sicurezza nei luoghi di lavoro;
-Organizzazione e gestione dei servizi di portineria, vigilanza sede e accoglienza;
-Gestione dell'URP ;
-Organo di Garanzia;
-Iscrizione degli alunni posti sotto protezione;
-Gestione delle Relazioni sindacali;
-Rilascio dei certificati di abilitazione/idoneità all'insegnamento nei concorsi riservati e nei concorsi ordinari;
-Gestione giuridico-economica del personale;
-Gestione dei procedimenti di esonero dall'espletamento dei normali obblighi di servizio per il personale scolastico.

Settore IX – pensioni personale della scuola:

-Predisposizione provvedimenti per il trattamento pensionistico del personale scolastico e amministrativo dell'USR ;
-Ricostruzione di carriere del personale scolastico in ruolo ante 1999;

Settore X – ordinamenti , affari generali e archivio:

-Commissioni Esami di Stato I ciclo;
-Esame delle richieste pervenute dai candidati esterni agli Esami di Stato di II grado;
-Nomina dei presidenti di commissione e dei componenti delle commissioni per gli Esami di Stato di II grado ed eventuale gestione delle sostituzioni;
-Nomina dei Presidenti e dei componenti delle Commissioni per gli esami di abilitazione alle libere professioni;
-Predisposizione e rilascio dei duplicati di diplomi e certificazioni sostitutive del diploma;
-Gestione dei dati degli alunni diplomati in annualità passate della Scuola secondaria di I e II grado;
-Riconoscimento di dichiarazioni di equipollenza per titoli di studio e diplomi conseguiti all'estero;
-Riconoscimento dei titoli di formazione professionale conseguiti nella comunità europea;
- Gestione scuole paritarie;
-Rinnovo Convenzioni di parifica delle Scuole primarie paritarie;
-Gestione delle richieste di benemerenze e onorificenze;
-Gestione delle richieste pervenute per l'intitolazione delle Scuole, delle aule scolastiche e dei locali interni alle scuole;
-Concessione di patrocini;
-Gestione segnalazioni e reclami relativi al personale della scuola;
-Inclusione scolastica,
-Organi collegiali Istituzioni scolastiche.

Autonomia:

- Verifica dello stato di avanzamento dei progetti finanziati con fondi Europei
-Gestione dei Campionati studenteschi, tra i quali, a titolo esemplificativo, di progetti nazionali di attività motoria e sportiva, di educazione stradale, di educazione alla legalità, di educazione alimentare e alla salute e corretti stili di vita;
-Predisposizione di protocolli di intesa e di convenzioni;
-Gestione richieste di organico di sostegno per gli studenti in situazione di disabilità e autorizzazione in deroga dei posti di sostegno - Partizione dell'Anagrafe Nazionale degli Studenti dedicata agli alunni con disabilità ;
-Formazione e aggiornamento del personale scolastico;

-Formazione obbligatoria del personale scolastico neo-assunto;
-Consulte degli studenti;
-Inclusione scolastica;
-Collaborazioni e supporto alle associazioni di genitori.

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

- 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 (eventuali);
- fornitori e collaboratori (eventuali);
- 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 (eventuali);

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 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

E' 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). E' 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.

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 DGCASIS 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 DGCASIS.

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 DGCASIS, 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 MIUR.

Al fine di non compromettere la sicurezza del Sistema Informativo MIUR, occorre adottare le seguenti norme comportamentali:

- se si ricevono email 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.
- non è consentito l'utilizzo di posta elettronica privata per invio/ricezione mail contenenti dati personali e/o di natura sensibile o giudiziaria.

Nell'ipotesi in cui la email 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 MIUR 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 email 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.

3.3 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 opportuno 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.