USR SICILIA
www.usr.sicilia.it

UFFICIO SCOLASTICO REGIONALE PER LA SICILIA
DIREZIONE GENERALE
Via Fattori, 60 - 90146 Palermo - Tel. 091/6909111
pec drsi@postacert.istruzione.it mail direzione-sicilia@istruzione.it C.F. 80018500829

Ministero Istruzione Università Ricerca

Il DIRIGENTE DELL'UFFICIO I

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 Ministero dell'Istruzione, dell'Università e della Ricerca;
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";
VISTA la nota n. 979 del 25/06/2019 del Capo Dipartimento con la quale si autorizza il Dirigente dell'Ufficio I, nelle more dell'insediamento del nuovo Direttore Generale e con riserva di ratifica da parte dello stesso, a nominare i dirigenti dell'U.S.R. come designati ai sensi del punto 4 della Direttiva;
VISTO il proprio decreto prot. 26320 del 01.10.2019, con cui si nominano i suddetti dirigenti dell'U.S.R. e, in considerazione della vacanza del posto di Dirigente degli Ambiti Territoriali di Messina e Ragusa, ci si riserva con successivo provvedimento di procedere all'individuazione dei soggetti Designati per tali Uffici, ai sensi della predetta Direttiva;
VISTO il Decreto dipartimentale prot. n. 1167 del 26.07.2019, notificato il 10.10.2019, con cui è attribuito alla Dott.ssa Viviana Assenza, dirigente di seconda fascia con funzione ispettiva tecnica, l'incarico di reggenza dell'Ufficio IX - Ambito territoriale di Ragusa (pos. retr. D) dell'Ufficio Scolastico Regionale per la Sicilia del Ministero dell'Istruzione, dell'Università e della Ricerca;
VISTO il Decreto dipartimentale prot. n. 1168 del 26.07.2019, notificato il 18.10.2019, con cui è attribuito d'ufficio al Dott. Filippo Ciancio, dirigente di seconda fascia con funzione ispettiva tecnica, l'incarico di reggenza dell'Ufficio VIII - Ambito territoriale di Messina (pos. retr. C) dell'Ufficio Scolastico Regionale per la Sicilia del Ministero dell'Istruzione, dell'Università e della Ricerca;
RITENUTO, in ragione della complessità organizzativa e gestionale dell'Amministrazione, di affidare specifici compiti e funzioni, connessi al trattamento dei dati dando apposite istruzioni ai *Dirigenti degli uffici di livello dirigenziale non generale* della struttura organizzativa di riferimento;

Dirigente: Marco Anello ☎ ✉ marco.anello@istruzione.it
Responsabile del procedimento: ☎ ✉ drsi.ufficio1@istruzione.it

USR SICILIA
www.usr.sicilia.it

UFFICIO SCOLASTICO REGIONALE PER LA SICILIA
DIREZIONE GENERALE
Via Fattori, 60 - 90146 Palermo - Tel. 091/6909111
pec drsi@postacert.istruzione.it mail direzione-sicilia@istruzione.it C.F. 80018500829

Ministero Istruzione Università Ricerca

DECRETA

1. Ad integrazione di quanto stabilito con decreto prot. 26320 del 01.10.2019 di cui alla premessa, sono nominati come Designati, con riserva di ratifica da parte del nuovo Direttore Generale, i seguenti Dirigenti di livello dirigenziale non generale sulla base di quanto previsto dal punto 4 della Direttiva n. 239 del 25 marzo 2019:

a) Dott.ssa Viviana ASSENZA, Dirigente in reggenza dell'Ufficio IX - Ambito territoriale di Ragusa;
b) Dott. Filippo CIANCIO, Dirigente in reggenza dell'Ufficio VIII - Ambito territoriale di Messina.

2. I suddetti Dirigenti sono designati per lo svolgimento delle seguenti attività connesse ai trattamenti di dati personali, rientranti nell'ambito delle competenze assegnate nell'atto di incarico dirigenziale. Gli atti di esercizio della presente designazione, che dovranno essere portati a conoscenza del soggetto che esercita le funzioni di Titolare, sono i seguenti:

a) porre in essere misure tecniche e organizzative adeguate per garantire che il trattamento dei dati personali sia effettuato conformemente alle disposizioni del Regolamento;
b) adottare soluzioni di privacy by design e by default;
c) tenere costantemente aggiornato il Registro delle attività di trattamento dei dati personali previsto dall'art. 30 del Regolamento;
d) predisporre le informative relative al trattamento dei dati personali nel rispetto degli artt. 13 e 14 del Regolamento;
e) fornire ai soggetti autorizzati istruzioni specifiche e puntuali per il corretto trattamento dei dati;
f) predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti previsti dalla normativa;
g) disporre l'adozione dei provvedimenti richiesti dal Garante per la protezione dei dati personali (di seguito anche Garante);
h) collaborare con il Responsabile per la protezione dei dati al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
i) assicurare il pieno supporto al soggetto che esercita le funzioni di Titolare nella gestione delle violazioni di dati, ponendo in essere tutti gli adempimenti di competenza previsti nel processo di gestione del data breach;
j) effettuare la preventiva valutazione d'impatto nei casi in cui essa è richiesta a norma dell'articolo 35 del Regolamento;
k) consultare il Garante, nei casi previsti dall'art. 36 del Regolamento, quando la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenta un rischio elevato;
l) richiedere obbligatoriamente nelle richieste di sviluppo di software e di piattaforme l'applicazione della policy in materia di sicurezza di sviluppo delle applicazioni;
m) designare i Responsabili del trattamento ai sensi dell'articolo 28 del Regolamento e gestire le segnalazioni dei Dirigenti degli uffici di livello dirigenziale non generale in relazione a eventuali inadempimenti dei suddetti Responsabili;
n) definire con accordi interni un rapporto di contitolarità, nel caso di determinazione congiunta con altro Titolare di finalità e mezzi ai sensi dell'art. 26 del Regolamento ;
o) definire i ruoli in ambito protezione dei dati personali del MIUR e delle scuole in relazione ai vari processi gestiti, avendo particolare riguardo a quelli gestiti attraverso piattaforme informatiche;
p) autorizzare i soggetti esterni che prestano la loro attività in favore della rispettiva struttura, dando loro specifiche istruzioni in relazione alle attività di trattamento dati assegnate.

Dirigente: Marco Anello ☎ ✉ marco.anello@istruzione.it
Responsabile del procedimento: ☎ ✉ drsi.ufficio1@istruzione.it

3. I soggetti Designati vigilano sui trattamenti posti in essere nelle strutture di cui sono responsabili in relazione alle attività di cui al comma 2 e nel rispetto delle istruzioni di cui all'Allegato A al presente provvedimento.
Il presente decreto viene notificato ai diretti interessati.

IL DIRIGENTE dell'UFFICIO I
Marco Anello

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

ANELLO MARCO
31.10.2019 11:03:01 UTC

Allegato A

Istruzioni al soggetto designato per il trattamento dei dati personali di cui al punto 4 della Direttiva n. 239 del 25 marzo 2019

1. Principi generali

Il soggetto designato 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 e gli interventi idonei a garantire il rispetto delle vigenti disposizioni in materia di protezione dei dati personali, risolvendo tempestivamente 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;
- implementare misure idonee a prevenire l'eventuale distruzione, dispersione o accesso non autorizzato ai documenti;
- non fare alcun uso improprio e mantenere riservate le notizie e le informazioni concernenti i dati personali apprese nell'esercizio delle proprie attività, osservando tali doveri di riserbo anche dopo la cessazione dalla propria attività.

I dati personali devono essere trattati nel rispetto dei principi posti dall'articolo 5 del Regolamento.
Il trattamento dei dati deve avvenire secondo:

- **liceità**: ogni trattamento deve essere conforme alle disposizioni in materia di protezione dei dati personali ed in particolare nella misura in cui ricorra almeno una delle condizioni di cui all'art. 6, par. 1 del Regolamento, in correlazione alle condizioni di cui alle premesse;
- **correttezza e trasparenza**: il trattamento deve essere esplicitamente illustrato 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 adottati, con l'ausilio dell'eventuale Responsabile del trattamento, provvedimenti tecnici ed organizzativi di sicurezza appropriati ai rischi presentati dal trattamento.

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**, nel senso che 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, nel senso che 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.

2. Istruzioni su conformità giuridica del trattamento dei dati

a) mettere in atto, sulla base di quanto previsto dell'art. 25, par. 1 del Regolamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento, misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie previste dal Regolamento, nonché a tutelare i diritti degli interessati (c.d. *protection by design)*;
b) porre in essere, sulla base di quanto previsto dell'art. 25, par. 2 del Regolamento, le misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento nel rispetto del principio della minimizzazione del dato, assicurando la liceità del trattamento (c.d. *protection by default)* ;
c) assicurare, qualora necessario, un riesame e aggiornamento delle misure tecniche e organizzative,;
d) garantire la compilazione del Registro dell'attività di trattamento di dati personali di cui all'articolo 30 del Regolamento attraverso l'aggiornamento costante con l'indicazione verificabile della data della prima adozione e delle date delle successive versioni del Registro stesso;
e) conservare tutte le versioni del Registro delle attività di trattamento anche al fine di metterlo a disposizione dell'autorità di controllo (di seguito anche "Garante"), tenendo conto delle istruzioni sul Registro messe a disposizione del Garante pubblicate nell'area riservata del sito istituzionale del MIUR dedicata alla privacy;
f) garantire, ai sensi dell'art. 32 del Regolamento, che la protezione dei dati personali all'interno degli Uffici di propria competenza sia realizzata sulla base delle misure che garantiscono un livello di sicurezza adeguato al rischio a cui possono essere esposti i trattamenti e porre in atto le misure tecniche e organizzative adeguate a garantire tale livello di sicurezza;
g) assicurare che il trattamento di dati personali per finalità di gestione del rapporto di lavoro sia in linea con la normativa vigente e nel rispetto delle linee guida del Garante (Deliberazione n. 23 del 14 giugno 2007, nei limiti della sua compatibilità con la normativa vigente);
h) rilasciare e impartire apposite e specifiche istruzioni al personale dipendente o agli eventuali soggetti esterni autorizzati ai trattamenti di competenza *dell'Ufficio/Direzione Generale* in base a quanto previsto dall'articolo 29 del Regolamento;
i) aggiornare/modificare, quando necessario, i provvedimenti di autorizzazione e le relative istruzioni impartite ai soggetti autorizzati;
j) assicurare che il personale autorizzato riceva la formazione prevista e le istruzioni che nel tempo dovessero rendersi necessarie, anche in caso di novità normative e/o organizzative significative;
k) consentire ai singoli autorizzati l'accesso ai sistemi informativi attraverso idonei profili in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento assegnate;
l) verificare che le misure di sicurezza, tecniche e organizzative predisposte, siano rispettate dalle persone autorizzate in osservanza delle istruzioni ricevute;
m) adottare misure appropriate per fornire all'interessato tutte le informazioni di cui agli artt. 13 e 14 del Regolamento utilizzando una forma concisa, trasparente, intellegibile e facilmente accessibile, con un linguaggio semplice e chiaro;
n) rendere conoscibile agli interessati le modalità (ad esempio, attraverso l'istituzione di apposita casella di posta elettronica) con le quali possono essere esercitati i diritti di cui agli artt. da 15 a 22 del Regolamento e assicurare che gli stessi ricevano riscontro alle proprie istanze, tenendo conto delle limitazioni ai diritti dell'interessato poste dagli artt. 2-*undecies e 2-duodecies* del Codice privacy;
o) porre in essere le misure necessarie a dare piena attuazione ai provvedimenti richiesti dal Garante;
p) comunicare al soggetto che esercita le funzioni di Titolare tempestivamente ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità giudiziaria in relazione alla protezione dei dati personali;
q) in caso di accertamenti o controlli, fornire al Garante tutte le informazioni e i documenti richiesti anche con riferimento al contenuto di banche di dati così come previsto dall'articolo 157 del Codice privacy;

r) fornire riscontro alle richieste del Responsabile per la protezione dei dati;
s) indicare, nell'atto di costituzione di gruppi di lavoro che prevedono il trattamento di dati personali, i soggetti autorizzati e le relative istruzioni;
t) porre in essere tutte le attività per mettere a disposizione del Computer Emergency Response Team (CERT) del MIUR o dell'Unità di presidio regionale i dati/le banche dati/le informazioni necessarie per la gestione degli incidenti di sicurezza nei tempi e nelle modalità previste dalla procedura di gestione del *data breach*;
u) porre in essere tutte le attività per mettere a disposizione del soggetto che esercita le funzioni del Titolare le informazioni necessarie per la gestione degli incidenti di sicurezza nei tempi e nelle modalità previste dalla procedura di gestione del *data breach*;
v) vigilare affinché i dati oggetto di trattamento siano conservati per il periodo di tempo strettamente necessario all'esecuzione delle attività per i quali sono stati raccolti e trattati e, comunque, non oltre i termini di legge;
w) adottare adeguate cautele per assicurare la riservatezza dei dati personali destinati ad essere comunicati o altrimenti trasmessi agli altri uffici interni o esterni al Ministero, anche attraverso l'utilizzo di mezzi adeguati, nel rispetto di specifici obblighi e garanzie posti dagli artt. 28 e 32 del Regolamento;
x) vigilare affinché i dati personali trattati non vengano diffusi al di fuori dei casi e oltre il termine previsti in adempimento di specifici obblighi normativi anche nel rispetto delle linee guida del Garante definite in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul *web* pubblicate sulla Gazzetta Ufficiale n. 134 del 12 giugno 2014, nei limiti della loro attuale applicabilità;
y) Individuare e designare, con contratto o altro atto giuridico secondo quanto previsto dall'art. 28, comma 3 del Regolamento, quali Responsabili del trattamento, unicamente soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato;
z) stipulare, nel caso di rapporto di contitolarità secondo quanto previsto dall'articolo 26 del Regolamento, accordi interni che rappresentino in modo trasparente le rispettive responsabilità, con particolare riguardo all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14;
aa) garantire all'interessato la disponibilità del contenuto essenziale degli accordi interni di cui all'articolo 26 del Regolamento;
bb) informare prontamente il soggetto che esercita le funzioni del Titolare di ogni questione rilevante ai fini della corretta applicazione della normativa vigente sulla protezione dei dati personali;
cc) assicurarsi, fin dall'analisi della richiesta di sviluppo di *software* e di piattaforme, che vengano previste e rispettate, anche da parte del Responsabile del trattamento, le disposizioni definite dalla *policy* del Ministero in materia di sicurezza di sviluppo delle applicazioni;
dd) effettuare la valutazione di impatto sulla protezione dei dati in presenza di trattamenti che comportino un rischio elevato ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, sulla base anche di quanto previsto dal Garante nell'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018;
ee) consultare, prima di procedere al trattamento, l'autorità di controllo qualora la valutazione di impatto sulla protezione dei dati indichi che il trattamento presenti un rischio elevato in assenza di misure adottate dal Titolare per attenuare il rischio secondo quanto previsto dall'art. 36 del Regolamento;
ff) verificare, ai sensi dell'art. 2 *ter*, comma 2, del Codice privacy, che, in caso di comunicazione tra titolari o designati che effettuano il trattamento di dati personali di dati diversi da quelli ricompresi nelle particolari categorie di dati personali di cui all'art. 9 del Regolamento e di quelli relativi a

condanne penali e reati di cui all'art. 10 del Regolamento, esista esclusivamente una norma di legge o, nei casi previsti dalla legge, di Regolamento;

gg) verificare che, in mancanza della base giuridica di cui all'art. 2 *ter*, comma 1, del Codice privacy, la comunicazione di dati tra titolari che effettuano il relativo trattamento sia necessaria per lo svolgimento di compiti di interesse e lo svolgimento di funzioni istituzionali e assicurarsi che sia decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati;

hh) verificare la sussistenza della base giuridica di cui all'art. 2 *ter*, comma 1, del Codice privacy nella diffusione e comunicazione di dati personali per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri a soggetti che intendono trattarli per altre finalità;

ii) assicurare il rispetto dei principi posti dal Regolamento negli artt. 44 e seguenti in caso di trasferimento di dati personali verso paesi terzi o organizzazioni internazionali;

jj) assicurarsi che il trattamento di categorie particolari di dati personali necessari per motivi di interesse pubblico rilevante si basino, secondo quanto previsto dall'articolo 2 *sexies* del Codice privacy nell'ordinamento interno da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato, tenendo conto anche delle precisazioni del Garante nella relativa nota presente sul sito istituzionale;

kk) garantire che, fatto salvo quanto previsto dal D.Lgs. 51/2018, il trattamento dei dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza che non avviene sotto il controllo dell'autorità pubblica, è consentito, ai sensi dell'articolo 10 del Regolamento, solo se autorizzato da una norma di legge o nei casi previsti dalla legge, di regolamento che prevedano garanzie appropriate per i diritti e le libertà degli interessati ai sensi dell'articolo 2 *octies* del Codice privacy;

ll) tener conto del divieto di cui all'articolo 13 del decreto del Presidente della Repubblica 22 settembre 1988, n. 448, di pubblicazione e divulgazione con qualsiasi mezzo di notizie o immagini idonee a consentire l'identificazione di un minore si osserva anche in caso di coinvolgimento a qualunque titolo del minore in procedimenti giudiziari in materie diverse da quella penale secondo quanto previsto dall'articolo 50 del Codice privacy;

mm) assicurare la piena osservanza di quanto disposto dall' articolo 52 del Codice privacy in merito alla diffusione anche da parte di terzi di sentenze o di altri provvedimenti o delle relative massime giuridiche, anche con riguardo all'indicazione delle generalità e degli altri dati identificativi dei soggetti coinvolti;

nn) tener conto che, ai sensi dell'articolo 99 del Codice privacy il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici può essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati in linea con le indicazioni del Titolo VII del suddetto Decreto.

3. Istruzioni per la sicurezza dei dati

3.1. Principi

Il soggetto Designato 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, con divieto di qualsiasi altra diversa utilizzazione;

- porre in essere tutte le azioni e gli interventi idonei a garantire il rispetto delle vigenti disposizioni in materia di protezione dei dati personali, segnalando tempestivamente al soggetto che esercita le funzioni di Titolare ogni eventuale problema applicativo;
- definire 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 funzioni, osservando tali doveri di riserbo anche dopo la cessazione dalla propria attività.

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 adottati, con l'ausilio dell'eventuale Responsabile del trattamento, provvedimenti tecnici ed organizzativi di sicurezza appropriati ai rischi presentati dal trattamento.

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.

4. Sicurezza dei dati

4.1 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.

4.1.1 Gestione strumenti elettronici (PC fissi e portatili)

Ciascun soggetto designato 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 e portatile), si precisa che:

- al termine dell'orario di lavoro, il PC deve essere spento;
- se il soggetto designato 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 autentificazione.

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 contratti, gli acquisti e per i sistemi informativi e la statistica (in seguito, DGCASIS), 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.

4.2.2 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 designato 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 designato 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 designato deve scegliere la password in base ai criteri standard di sicurezza quali: combinare 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.

4.2.3 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.

4.2.4 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.

Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di categorie particolari di dati (precedentemente identificati come dati sensibili), 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.

4.2.5 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.

4.2.6 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.

4.2.7 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.

4.3 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.
Il soggetto designato 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;
- l'accesso agli archivi deve essere controllato permettendo l'accesso ai soli soggetti autorizzati.

Per quanto non previsto, si rimanda alle politiche interne e alle linee guida adottate dal Garante e dal Ministero dell'Istruzione, dell'Università e della Ricerca.