Vademecum sicurezza dati

Regole di condotta ed obblighi dei responsabili ed incaricati del trattamento dei dati personali, in relazione all’uso degli strumenti informatici, di Internet e della Posta Elettronica, redatto ai sensi del provvedimento del Garante della Privacy (Deliberazione n. 13 del 1/3/2007 - pubblicata in GU n. 58 del 10 marzo 2007) comprensivo di alcune note per la gestione dei dati cartacei ed adeguato al Regolamento Europeo 679/2016.

Ente/organizzazione/Istituto: FONDAZIONE ENAC PUGLI A Ente Canossiano di formazione e lavoro “C.Figliolia” ETS

Autorizzazione: il provvedimento adottato dal Garante con cui il titolare del trattamento (ente pubblico, impresa, libero professionista) viene autorizzato a trattare determinati dati “sensibili” o giudiziari, ovvero a trasferire dati personali all’estero.

Comunicazione:far conoscere dati personali a uno o più soggetti determinati (che non siano l’interessato, il responsabile o l’incaricato), in qualunque forma, anche attraverso la loro messa a disposizione o consultazione (vedi anche diffusione)

Consenso:la libera manifestazione di volontà dell’interessato con cui questi accetta espressamente un determinato trattamento dei suoi dati personali, del quale è stato preventivamente informato da chi ha un potere decisionale sul trattamento (vedi titolare).

D.Lgs. 196/2003:Decreto Legislativo 196 del 30 giugno 2003 e sue successive modifiche ed integrazioni (101/2018)

Dato personale : qualsiasi informazione che riguardi persone fisiche identificate o che possono essere identificate anche attraverso altre informazioni, ad esempio, attraverso un numero o un codice identificativo. Sono, ad esempio, dati personali: il nome e cognome o denominazione; l’indirizzo, il codice fiscale; ma ancheun’immagine, la registrazione della voce di una persona, la sua impronta digitale, i dati sanitari, i dati bancari, ecc.

Dato particolare :un dato personale che, per la sua natura, richiede particolari cautele: sono dati sensibili quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'adesione a partiti, sindacati o associazioni, lo stato di salute e la vita sessuale delle persone.

Dato giudiziario :i dati personali che rivelano l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (quali, ad es., i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione). Rientrano in questa categoria anche la qualità di imputato o di indagato.

Diffusione: divulgare dati personali al pubblico o, comunque, ad un numero indeterminato di soggetti (ad esempio, è diffusione la pubblicazione di dati personali su un quotidiano o su una pagina web).

Dipendente: personale dell'Istituto assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio.

GDPR General Data Protection Regulation – Regolamento Generale sulla Protezione dei Dati UE2016/679:è un Regolamento con il quale la Commissione europea intende rafforzare e rendere più omogenea la protezione dei dati personali di cittadini dell'Unione Europea e dei residenti nell'Unione Europea, siaall'interno che all'esterno dei confini dell'Unione europea (UE). Il testo, pubblicato su Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno, inizierà ad avere efficacia il 25 maggio 2018.

Incaricato: ogni dipendente, come sopra identificato, ed ogni consulente esterno che, nell'ambito dell'attività assegnatagli, tratta dati (nell'accezione del capitolo seguente) riferiti all'Istituto. Il regolamento europeo non prevede espressamente la figura dell'incaricato, ma non ne esclude la nomina, facendo riferimento a persone autorizzate al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile (art. 4). In sede europea, alla nostra DPA è stato concesso di poter utilizzare ancora i termini titolare, responsabile e incaricato; traducendo così, nella versione italiana del GDPR, la figura del "controller" (Art. 4.7) con "titolare del trattamento"; "processor" (Art. 4.8) con "responsabile del trattamento"; "third party" (Art.4.10) con "terzo", e di poter continuare ad utilizzare il termine "incaricato" per qualificare "le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile".

Informativa: le informazioni che il titolare del trattamento deve fornire ad ogni interessato, verbalmente o

per iscritto quando i dati sono raccolti presso l'interessato stesso, oppure presso terzi. L'informativa deve precisare sinteticamente e in modo colloquiale quali sono gli scopi e le modalità del trattamento; se l'interessato è obbligato o no a fornire i dati; quali sono le conseguenze se i dati non vengono forniti; a chi possono essere comunicati o diffusi i dati; quali sono i diritti riconosciuti all'interessato; chi sono il titolare e l'eventuale responsabile del trattamento e dove sono raggiungibili (indirizzo, telefono, fax, ecc.).

Interessato : la persona fisica cui si riferiscono i dati personali.

Misure di sicurezza: sono tutti gli accorgimenti tecnici ed organizzativi, i dispositivi elettronici o i programmi informatici utilizzati per garantire che i anche in modo accidentale, che solo le persone autorizzate possano avere accesso ai dati e che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti.

NDA: non-disclosure agreement, ovvero accordo di non divulgazione, è un negozio giuridico di natura sinallagmatica che designa informazioni confidenziali e con il quale le parti si impegnano a mantenerle segrete, pena la violazione dell'accordo stesso e il decorso di specifiche clausole penali in esso contenute.

Responsabile del trattamento :la persona, la società, l'ente, l'associazione o l'organismo cui il titolare affida, anche all'esterno, per la particolare esperienza o capacità, compiti di gestione e controllo del trattamento dei dati.

Titolare del trattamento :la persona fisica, l'impresa, l'ente, l'associazione, ecc. cui fa capo effettivamente il trattamento di dati personali e spetta assumere le decisioni fondamentali sugli scopi e sulle modalità del trattamento medesimo (comprese le misure di sicurezza).Nei casi in cui il trattamento sia svolto da una società o da una pubblica amministrazione per titolare va intesa l'entità nel suo complesso e non l'individuo o l'organo che l'amministra o la rappresenta (presidente, amministratore delegato, sindaco, ministro, direttore generale, ecc.).

Trattamento di dati personali: un'operazione o un complesso di operazioni che hanno per oggetto dati personali.

INDICE

SEZIONE 1

Normativa di riferimento

• Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio Europeo del 27 Aprile 2016 (protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE), entrato in vigore il 25 maggio 2018;

• Decreto legislativo 196/2003 così come modificato dal decreto legislativo 101/2018 entrato in vigore il 19.09.2018 (disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento europeo 2016/679) e le ss.mm.ii.

SOGGETTI PREDISPOSTI AL TRATTAMENTO DEI DATI

TITOLARE DEL TRATTAMENTO DEI DATI : Titolare del trattamento è Enac Puglia ente di formazione Canossiano “C.Figliolia”.Il titolare è colui che tratta i dati senza ricevere istruzioni da altri, decide "perché" "come" devono essere trattati i dati. Il titolare del trattamento non è, quindi, chi gestisce materialmente i dati, ma chi decide il motivo e le modalità del trattamento.

RESPONSABILI DEL TRATTAMENTO Responsabile del trattamento è una persona fisica o giuridica distinta dal titolare che elabora dati per conto di questo, è quindi un soggetto esterno. Il responsabile deve trattare dati attenendosi alle istruzioni del titolare, assume responsabilità proprie e ne risponde alle autorità di controllo e alla magistratura

PERSONE AUTORIZZATE AL TRATTAMENTO DEI DATI :assistenti amministrativi, docenti e personale collaboratore Sono le persone fisiche che effettuano materialmente le operazioni di trattamento sui dati personali. Gli autorizzati possono operare alle dipendenze del titolare o collaborare con il medesimo. Ovviamente gli autorizzati possono essere organizzati con diversi livelli di delega. L'autorizzato è un mero esecutore di compiti e deve strettamente attenersi alle istruzioni ricevute dal titolare. Ai sensi dell’art. 2-quaterdecies del Codice della privacy il titolare del trattamento deve individuare le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la loro autorità diretta.

INTERESSATO AL TRATTAMENTO :L’interessato è persona fisica a cui si riferiscono i dati personali.

-DATI PERSONALI-

Ai sensi dell’art. 4 del GDPR, i dati personali sono qualsiasi informazione concernente una persona fisica identificata (es. il nome) o identificabile anche indirettamente e perciò anche un’informazione riguardante una persona, la cui identità può comunque essere accertata mediante informazioni supplementari (es. il codice fiscale, l’impronta digitale, l’immagine).

Tutti i dati che riguardano un individuo godono della tutela del GDPR, ma non tutti i dati sono uguali. Esistono dati comuni, categorie particolari di dati e dati giudiziari.

Categorie particolari di dati (art. 9 GDPR)

- Dati di origine razziale o etnica
- Dati riguardanti le opinioni politiche
- Dati relativi alle convinzioni religiose o filosofiche
- Dati di appartenenza sindacale
- Dati genetici
- Dati biometrici intesi a identificare in modo univoco una persona fisica
- Dati inerenti la salute o l’orientamento sessuale della persona

-DATI GIUDIZIARI-(art. 10 GDPR)

1. Dati relativi a condanne penali
2. Dati riguardanti i reati
3. Dati inerenti all’applicazione di misure di sicurezza

TRATTAMENTO DEI DATI

Per “trattamento dei dati” si intende qualsiasi attività effettuata sui dati personali: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, raffronto o interconnessione, limitazione, cancellazione o distruzione (art. 4 GDPR).
Elemento identificativo del trattamento è la finalità, che costituisce lo scopo effettivo per il quale i dati vengono raccolti e gestiti.
A ciascuna finalità deve necessariamente corrispondere uno specifico trattamento.

-Indicazioni operative da rispettare per il trattamento dei dati personali-

Il legislatore europeo all’articolo 5 del GDPR fissa i principi applicabili al trattamento dei dati personali. Il titolare del trattamento e tutti i soggetti che trattano dati in suo nome e conto devono pertanto rispettare e applicare i seguenti principi:

• Liceità, correttezza e trasparenza del trattamento. Liceità: il trattamento dei dati deve essere rispettoso delle disposizioni del Regolamento e delle Carte sovranazionali e nazionali dei diritti dell’uomo e del cittadino e delle altre norme di legge. Correttezza: il titolare non deve violare norme di legge o commettere abusi nel trattamento dei dati. Trasparenza: chiarezza negli obblighi informativi nei confronti dell’interessato.

• Limitazione delle finalità. I dati devono essere raccolti per finalità determinate, esplicite e legittime (pertanto il titolare dovrà assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati)

• Minimizzazione dei dati. I dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati.

• Esattezza. I dati trattati devono essere esatti e se necessario aggiornati (compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento).

• Limitazione della conservazione. I dati devono essere conservati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento (una volta conseguite le finalità di trattamento i dati vanno eliminati o anonimizzati).

• Integrità e riservatezza. I dati devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

• Responsabilizzazione. Il titolare del trattamento dei dati è competente per il rispetto di tutti i principi sopra descritti e deve essere in grado di comprovarlo.

-Modalità relative al trattamento dei dati-

Ogni dipendente deve trattare i dati personali in modo lecito, corretto e trasparente rispettando le seguenti indicazioni:

• raccogliere e registrare i dati personali per finalità determinate, esplicite e legittime, ed i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati;

• verificare che siano esatti e, se necessario, aggiornarli;

• verificare che siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;

• conservarli in modo sicuro e per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;

• non trasferire a un paese terzo o a un'organizzazione internazionali i dati personali;

• verificare che per ogni trattamento sia stata previamente presentata l'informativa agli interessati, ai sensi degli artt. 13 e 14 del Regolamento UE 2016/679;

• non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale;

• informare prontamente il Titolare del trattamento di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata dei dati stessi;

• informare prontamente il Titolare del trattamento qualora si verificasse la necessità di porre in essere operazioni di trattamento di dati personali per finalità o con modalità diverse da

quelle risultanti dalle istruzioni ricevute, nonché di ogni istanza di accesso ai dati personali da parte di soggetti interessati e di ogni circostanza che esuli dalle istruzioni impartite;

• accedere solo ai dati strettamente necessari all’esercizio delle proprie funzioni;

• accertarsi dell’identità degli interessati e della loro autorizzazione al trattamento e dell’eventuale autorizzazione scritta a terzi, al momento del ritiro di documentazione in uscita;

• non fornire telefonicamente o a mezzo fax dati e informazioni ai diretti interessati, senza avere la certezza della loro identità;

• non effettuare fotografie e diffonderle, a documenti interni dell’istituzione scolastica che devono rimanere riservati;

• non effettuare fotografie, registrazioni vocali e video agli alunni e diffonderle, anche ai genitori degli alunni, senza il consenso degli interessati e l’autorizzazione scritta del titolare del trattamento;

• seguire le attività di formazione organizzate dalla istituzione scolastica;

• partecipare alla attività di verifica affinché le misure di sicurezza vengano applicate nell’Istituto.

L’eventuale trasferimento avverrà in ogni caso nel rispetto delle garanzie appropriate e opportune ai fini del trasferimento ai sensi della normativa applicabile. Istruzioni specifiche:

• non trattare nessun documento al di fuori delle autorizzazioni ricevute;

• una volta presi in carico, gli atti e i documenti, contenenti dati personali, non lasciarli liberi di vagare senza controllo ed a tempo indefinito per gli uffici, ma provvedere in qualche modo a controllarli e custodirli, possibilmente all’interno di armadi blindati, o dotati di serratura, soprattutto se contenenti dati particolari o giudiziari;

• in caso di affidamento di atti e documenti contenenti dati di categorie particolari, il controllo e la custodia devono avvenire in modo tale, che ai dati non accedano persone prive di autorizzazione. A tale fine, è quindi necessario dotarsi di cassetti con serratura, o di altri accorgimenti aventi funzione equivalente, nei quali riporre i documenti contenenti dati sensibili o giudiziari prima di assentarsi dal posto di lavoro, anche temporaneamente.

Assicurare l'accesso a tali archivi alle sole persone autorizzate da specifico e scritto profilo di autorizzazione da parte del titolare;

• custodire i dati cartacei in modo da renderli non facilmente accessibili a terzi;

• non lasciare incustoditi sulla propria scrivania o cattedra i documenti cartacei;

• se collocati sulla scrivania per esigenze di maggiore praticità, riporre i documenti cartacei contenenti dati personali di qualsiasi natura al termine della giornata lavorativa all’interno dei cassetti, o armadi;

• per evitare il pericolo di illecita divulgazione dei dati personali, è vietato far accedere all’interno dei locali della segreteria persone non espressamente autorizzate ad entrarvi;

• i cassetti e/o gli armadi contenenti documenti riservati dovranno essere chiusi a chiave all’orario di chiusura della scuola;

• è severamente vietato utilizzare documenti contenti dati personali, di qualsiasi natura, come carta da riciclo o da appunti;

• una volta raggiunto il loro scopo, i documenti contenti dati personali di qualsiasi natura non dovranno essere buttati nei cestini, ma eliminati attraverso una trita-documenti.

TRATTAMENTO DEI DATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Istruzioni specifiche:

• non trattare nessun documento al di fuori delle autorizzazioni ricevute;

• una volta presi in carico, gli atti e i documenti, contenenti dati personali, non lasciarli liberi di vagare senza controllo ed a tempo indefinito per gli uffici, ma provvedere in qualche modo a controllarli e custodirli, possibilmente all’interno di armadi blindati, o dotati di serratura, soprattutto se contenenti dati particolari o giudiziari;

• in caso di affidamento di atti e documenti contenenti dati di categorie particolari, il controllo e la custodia devono avvenire in modo tale, che ai dati non accedano persone prive di autorizzazione. A tale fine, è quindi necessario dotarsi di cassetti con serratura, o di altri accorgimenti aventi funzione equivalente, nei quali riporre i documenti contenenti dati sensibili o giudiziari prima di assentarsi dal posto di lavoro, anche temporaneamente. Assicurare l'accesso a tali archivi alle sole persone autorizzate da specifico e scritto profilo di autorizzazione da parte del titolare;

• custodire i dati cartacei in modo da renderli non facilmente accessibili a terzi;

• non lasciare incustoditi sulla propria scrivania o cattedra i documenti cartacei;

• se collocati sulla scrivania per esigenze di maggiore praticità, riporre i documenti cartacei contenenti dati personali di qualsiasi natura al termine della giornata lavorativa all’interno dei cassetti, o armadi;

• per evitare il pericolo di illecita divulgazione dei dati personali, è vietato far accedere all’interno dei locali della segreteria persone non espressamente autorizzate ad entrarvi;

• i cassetti e/o gli armadi contenenti documenti riservati dovranno essere chiusi a chiave all’orario di chiusura della scuola;

• è severamente vietato utilizzare documenti contenti dati personali, di qualsiasi natura, come carta da riciclo o da appunti;

• una volta raggiunto il loro scopo, i documenti contenti dati personali di qualsiasi natura non dovranno essere buttati nei cestini, ma eliminati attraverso una trita-documenti.

TRATTAMENTO DATI CON SISTEMI INFORMATICI

Istruzioni specifiche per l’’utilizzo del pc, di sistemi informatici, gestione password ed email

• Il personal computer (fisso o mobile) ed i relativi programmi e/o applicazioni affidati al dipendente sono, strumenti di lavoro, pertanto: tali strumenti devono essere custoditi in modo appropriato;

• utilizzare il personal computer ed i relativi programmi e/o applicazioni affidati solo per fini professionali (in relazione, ovviamente alle mansioni assegnate) e non per scopi personali, tanto meno per scopi illeciti; debbono essere prontamente segnalati al titolare del trattamento il furto, danneggiamento o smarrimento di tali strumenti;

• non lasciare supporti di memoria informatici (chiavette USB, DVD, ecc.), cartelle o altri documenti contenenti dati personali e/o sensibili a disposizione di estranei;

• non scaricare/installare di propria iniziativa programmi non previamente autorizzati dall’Istituto;

• non lasciare aperta la sessione di lavoro con la propria password inserita, in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l’individuazione dell’autore del trattamento;

• impostare la funzione blocca-schermo per le ipotesi di non utilizzo della propria postazione per più di 10 minuti;

• spegnere correttamente il computer al termine di ogni sessione;

• cambiare periodicamente (almeno una volta ogni 3 mesi in caso di trattamento di dati di categorie particolari o dati relativi a reati e condanne penali, altrimenti ogni 6 mesi) la propria password o qualora si ritenga compromessa, e scegliere una password con le seguenti caratteristiche: originale, composta da almeno otto caratteri, che contenga almeno una lettera maiuscola, un numero ed un carattere speciale (es.: * @ -), che non sia facilmente intuibile (evitando il nome proprio, il nome di congiunti, del proprio animale domestico, numeri di telefono, date di nascita e comunque riferimenti alla propria persona o lavoro facilmente ricostruibili);

• curare la conservazione della propria password ed evitare di comunicarla ad altri;

• non rivelare le credenziali di accesso al sistema informatico, di propria iniziativa, o dietro richiesta, ad alcuno la propria password;

• non scrivere la password in nessun posto in cui che possa essere letta facilmente, soprattutto vicino al computer (es.: post-it attaccati allo schermo del PC);

• utilizzare esclusivamente la posta elettronica con il dominio della scuola per l’invio di comunicazioni e/o documenti inerenti all’attività lavorativa;

• è vietato utilizzare la posta elettronica della scuola per motivi non attinenti allo svolgimento delle mansioni assegnate;

• in caso di utilizzo di posta elettronica, non aprire i documenti di cui non sia certa la provenienza e controllare accuratamente l’indirizzo dei destinatari prima di inviare email contenenti, in allegato e/o nel corpo del messaggio, dati personali;

• inviare messaggi di posta solo se espressamente autorizzati;

• in caso di invio di un’email a più destinatari, laddove ciascuno di essi debba essere informato privatamente dei contenuti della mail, inserire gli indirizzi dei destinatari all’interno del campo “Ccn” (Copia carbone nascosta);

• nella comunicazione multimediale per fini istituzionali con alunni e genitori utilizzare esclusivamente le piattaforme informatiche messe a disposizione dall’Istituto; è fatto divieto utilizzare social network e di utilizzare le credenziali fornite dalla scuola per l’iscrizione a

siti/newsletter/social network;

• per l’attività didattica utilizzare esclusivamente le piattaforme approvate dall’Istituto.

In ogni caso, ogni dipendente deve

• mantenere il segreto e la riservatezza sui dati;

• non comunicare a terzi, al di fuori dell’ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale.

Attenzione: Il mancato rispetto di quanto sopra riportato e in particolare dell’obbligo di segretezza e di riservatezza potrà comportare gravi responsabilità amministrative e civili a carico dell’Istituto e del soggetto inadempiente.

Trattamento dati particolari

All’interno dei dati trattati dalla Fondazione Enac Puglia particolare attenzione dovrà essere riservata ai dati e ai documenti contenenti informazioni sanitarie e/o psicologico comportamentali afferenti agli utenti (certificati L.104, relazioni DSA, ect…).

I certificati e i documenti cartacei ufficiali sono archiviati in un armadio in presidenza chiuso a chiave al quale si può avere accesso soltanto su richiesta del docente. Di tali documenti è vietato fare copie sia cartacee che digitali. Nel caso in cui gli interessati li forniscano direttamente agli addetti, tali documenti dovranno essere consegnati quanto prima in segreteria senza trattenerne nessuna copia. I PEI e i PDP, in formato solo digitale, sono tenuti direttamente dai docenti di sostegno/classe che provvederanno a pesudonimizzarli e a fare una tabella di conversione codice/alunno che terranno in cartaceo in un luogo diverso da quello dei files; è fatto divieto assoluto di divulgare la documentazione e nel caso di necessità di condivisione dei files dovranno essere utilizzati canali ufficiali quali per esempio una email ufficiale dell’istituto.

Certificati ed immagini

I certificati medici di giustificazione delle assenze degli utenti devono essere conservati in un luogo chiuso a chiave e distrutti al temine dell’anno scolastico (concluse tutte le operazioni di scrutinio). Ad inizio anno dovrà essere richiesta ai genitori una autorizzazione a fare foto o video durante tutte le attività scolastiche previste. Tali autorizzazioni, una volta raccolte, devono essere consegnate in segreteria per essere riposte nel fascicolo personale dell’utente. Per concorsi o attività non previste è necessario far sottoscrivere dai genitori una apposita autorizzazione.

Dove vengono conservati i dati personali

I dati personali in uso vengono conservati all’interno della segreteria all’interno di computer e di armadi chiusi a chiave. L’ingresso a tali locali è presidiato e controllato, nonché ammesso solo previa autorizzazione. I documenti non più in uso vengono poi collocati in appositi locali chiusi a chiave.

Diritti dell'interessato

La normativa attribuisce specifici diritti all'interessato, il quale, per l'esercizio di tali diritti, può rivolgersi direttamente al titolare del trattamento.

I diritti esercitabili dall'interessato sono i seguenti:

- diritto di revocare il consenso in qualsiasi momento (nei casi previsti dal GDPR);
- diritto di ottenere informazioni su quali dati sono trattati dal titolare (diritto di informazione);
- diritto di chiedere ed ottenere i dati in possesso del titolare (diritto di accesso);
- esercitare l'opposizione al trattamento in tutto o in parte; - diritto di opporsi ai trattamenti automatizzati;
- ottenere la cancellazione dei dati in possesso del titolare;
- ottenere l'aggiornamento o la rettifica dei dati conferiti;
- chiedere ed ottenere trasformazione in forma anonima dei dati;
- chiedere ed ottenere il blocco o la limitazione dei dati trattati in violazione di legge e quelli dei quali non è più necessaria la conservazione in relazione agli scopi del trattamento;
- diritto alla portabilità dei dati.

L’interessato ha inoltre la facoltà di proporre una segnalazione e un reclamo avanti all’Autorità di controllo dello Stato di residenza (Garante per la protezione dei dati personali).

Per approfondimenti si rimanda all’allegato A dedicato all’informativa al trattamento dei dati personali per utenti dei servizi e famiglie , e allegato B riguardante il trattamento delle “categorie particolari di dati personali”

SEZIONE 2

-Uso degli strumenti informatici-

All'inizio del rapporto lavorativo o di consulenza, si valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari dispositivi aziendali, di internet e della posta elettronica da parte degli incaricati.
Successivamente, e periodicamente, l'Istituto valuta la permanenza dei presupposti per l'utilizzo dei dispositivi aziendali, di internet e della posta elettronica.
È fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici aziendali. I casi di esclusione possono riguardare:

1. L'utilizzo del COMPUTER o di altri DISPOSITIVI.
2. L'utilizzo della posta elettronica.
3. L'accesso a internet.

Le eventuali esclusioni sono strettamente connesse al principio della natura lavorativa degli strumenti informatici, nonché al principio di necessità di cui al Codice Privacy e GDPR. Più specificatamente, hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo i responsabili per funzioni lavorative.
I casi in cui le esclusioni dovranno risultare operative in forza di tali motivazioni verranno comunicati individualmente e potranno riguardare sia tutti i casi sopra descritti, sia solo uno o due degli stessi.
Si informa che tali esclusioni sono divenute necessarie alla luce del Provvedimento del Garante 1° marzo 2007, che indica di ridurre a titolo cautelativo e preventivo l'utilizzo degli strumenti informatici in considerazione dei pericoli e delle minacce indicate in questo documento.

-Titolarità dei dispositivi e dei dati-

La Fondazione è esclusiva titolare e proprietaria dei dispositivi messi a disposizione dei responsabili, ai soli fini dell'attività lavorativa.
Inoltre è l'unico esclusivo titolare e proprietario di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri dispositivi digitali o archiviati in modo cartaceo nei propri locali.
L'incaricato non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei dispositivi (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i files di filmati o altre tipologie di files) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da copiati, comunicati o diffusi senza l'autorizzazione.

Finalità nell’utilizzo dei dispositivi

I dispositivi assegnati sono uno strumento lavorativo nelle disponibilità dell’incaricato esclusivamente per un fine di carattere lavorativo. I dispositivi, quindi, non devono essere utilizzati per finalità private , se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare.

Restituzione dei dispositivi

A seguito di una cessazione del rapporto lavorativo o di consulenza dell’incaricato con l’organizzazione o, comunque, al venir meno della permanenza dei presupposti per l’utilizzo dei dispositivi , gli incaricati hanno divieto assoluto di formattare o alterare o manomettere o distruggere i dispositivi assegnati o rendere inintelligibili i dati in essi contenuti, tramite qualsiasi processo.

SEZIONE 3

-PASSWORD-

Le password possono essere un metodo di autenticazione assegnato dall'istituto per garantire l'accesso protetto ad uno strumento hardware, oppure ad un applicativo software.

La prima caratteristica di una password è la segretezza e, cioè, il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può essere causa di gravi danni al proprio lavoro, a quello dei colleghi e dell'Istituto nel suo complesso. Nel tempo, anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle con una certa frequenza. Il personale di segreteria dovrà tenere la Direttore a conoscenza delle password dei computer dell'ufficio.

Altra buona norma è quella di non memorizzare la password su supporti facilmente intercettabili da altre persone. Il miglior luogo in cui conservare una password è la propria memoria.

In qualsiasi momento, l'istituto si riserva il diritto di revocare all'incaricato il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

-Regole per la corretta gestione delle password-

L'incaricato, da parte sua, per una corretta e sicura gestione delle proprie password, deve rispettare le regole seguenti:

- Le password sono assolutamente personali e non vanno mai comunicate ad altri
- Occorre cambiare immediatamente una password, non appena si abbia alcun dubbio che sia diventata poco "sicura".
- Le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali e numeri.
- Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare).

- Le password devono essere sostituite almeno nei tempi indicati dalla normativa, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password.
- Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti . In alcuni casi, sono implementati meccanismi che consentono all'incaricato un numero limitato di tentativi errati di inserimento della password, oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene bloccato per alcuni minuti. In caso di necessità,contattare il Titolare.

-OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO-

In questa sezione vengono trattate le operazioni a carico dell'incaricato e il quadro di riferimento generale per l'esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell'integrità del patrimonio dell'istituto.

Login e Logout

Il "Login" è l'operazione con la quale l'incaricato si connette al sistema informativo del Miur, del Registro elettronico ,della segreteria digitale o dell'area riservata del sito internet dichiarando il proprio Username e Password (ossia l'Account), aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet), ognuno dei quali richiede uno username e una password.

In questi casi, sebbene sia preferibile che ogni utente abbia un suo specifico username e password, l'Istituto potrà assegnare un univoco username e password per gruppi di responsabili per l'accesso alla macchina fisica, mentre rimarranno separati ed univoci per l'accesso agli applicativi che contengono dati.

Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.

Il "blocco del computer" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla.

Obblighi

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati. L'incaricato deve quindi eseguire le operazioni seguenti:

- Se si allontana dalla propria postazione, dovrà mettere in protezione il suo dispositivo affinché persone non autorizzate non abbiano accesso ai dati protetti.
- Bloccare il suo dispositivo prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
- Chiudere la sessione (Logout) a fine giornata;
- Spegnere il PC dopo il Logout;
- Controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo dispositivo.

-USO DEL PERSONAL COMPUTER DELL'ENTE-

Corretto utilizzo del COMPUTER

Il computer consegnato all'incaricato è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema,costi di manutenzione e, soprattutto, minacce alla sicurezza.
L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Il computer che viene consegnato contiene tutti i software necessari a svolgere le attività affidate dall'organizzazione. Per necessità aziendali, gli amministratori di sistema utilizzando la propria login con privilegi di amministratore e la password dell'amministratore, potranno accedere, con le regole indicate nel presente documento, sia alle memorie di massa locali di rete (repository e backup) che ai server aziendali nonché, previa comunicazione al dipendente, accedere al computer, anche in remoto.
In particolare l'incaricato deve adottare le seguenti misure:

1. Utilizzare solo ed esclusivamente le aree di memoria della rete dell'Istituto ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri file fuori dalle unità di rete.

2. Spegnere il computer, o curarsi di effettuare il Logout, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi, senza che vi sia la possibilità di provarne in seguito l'indebito uso.

3. Mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori), disposti dall'organizzazione.

4. Non dare accesso al proprio computer ad altri utenti, a meno che siano responsabili con cui condividono l’utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo.

ANTIVIRUS

I virus (o, per essere precisi, il malware, il software malevolo) possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, via mail …

L’Istituto impone su tutte le postazioni di lavoro l’utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana.

L’incaricato, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer e, in particolare, deve rispettare le regole seguenti:

1. Comunicare all’Istituto ogni anomalia o malfunzionamento del sistema antivirus.

2. Comunicare all’Istituto eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, all’ incaricato:

1. È vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione.

2. È vietato ostacolare l’azione dell’antivirus aziendale.

3. È vietato disattivare l’antivirus senza l’autorizzazione espressa dell’Istituto, anche e soprattutto nel caso sia richiesto per l’installazione di software sul computer.

4. È vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani. Contattare i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

-POSTA ELETTRONICA-

L’utilizzo della posta elettronica è connesso allo svolgimento dell’attività lavorativa.

Le caselle e-mail possono meglio essere assegnate con natura impersonale (tipo info, amministrazione, fornitori, direttore, collaboratore, consulenza, …) proprio per evitare ulteriormente che il destinatario delle mail possa considerar l’indirizzo assegnato al dipendente “privato”, ai sensi dei suggerimenti del Garante a tal proposito. Gli Incaricati assegnatari delle caselle di posta elettronica sono incaricati del corretto utilizzo delle stesse.

-DIVIETI ESPRESSI-

È vietato inviare, tramite la posta elettronica, anche all’interno della rete aziendale, materiale a contenuto violento,sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazionedel pensiero, anche politico.

È vietato inviare messaggi di posta elettronica, anche all’interno della rete aziendale, che abbiano contenuti contrari anorme di legge ed a norme di tutela dell’ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, oche siano in qualche modo discriminatori della razza, dell’origine etnica, del colore della pelle, della fede religiosa,dell’età, del sesso, della cittadinanza, dello stato civile, degli handicap.

Qualora l’incaricato riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all’organizzazione.

- USO DI ALTRI DISPOSITIVI –

(NOTEBOOK, TABLET, CELLULARE, SMARTPHONE E DI ALTRI DISPOSITIVI ELETTRONICI)

Il computer portatile, il tablet (di seguito generalizzati in “dispositivi mobili”) possono venire concessi in uso dall’istituto agli Incaricati che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell’istituzione.

L’incaricato è responsabile dei dispositivi mobili assegnatigli e deve custodirli con diligenza sia durante gli spostamenti sia durante l’utilizzo nel luogo di lavoro.

Ai dispositivi mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare, i file creati o modificati sui dispositivi mobili, devono essere trasferiti sulle memorie di massa al primo rientro in istituto e cancellati in modo definitivo dai dispositivi mobili (Wiping). Sui dispositivi mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dall’Istituto. I dispositivi mobili utilizzati all’esterno (convegni, visite, viaggi), in caso di allontanamento, devono essere custoditi in un luogo protetto. In caso di perdita o furto dei dispositivi mobili, deve far seguito la denuncia alle autorità competenti. Allo scopo si deve avvisare immediatamente l’Istituto che provvederà – se del caso – ad occuparsi delle procedure connesse alla privacy. Anche di giorno, durante l’orario di lavoro, all’incaricato non è consentito lasciare incustoditi i dispositivi mobili.

All’incaricato è vietato lasciare i dispositivi mobili incustoditi e a vista dentro l’auto o in una stanza

d'albergo o nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.

I dispositivi mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciti privi di PIN.

Laddove il dispositivo mobile sia accompagnato da un'utenza, l'incaricato è chiamato ad informarsi preventivamente de i vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati, …) e a rispettarli. Qualora esigenze lavorative richiedessero requirements differenti, l'incaricato è tenuto ad informare tempestivamente e preventivamente l'Istituto.

-MEMORIE ESTERNE- (chiavi usb, hard disk, memory card, cd-rom, dvd, ecc.)-

Agli incaricati può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, …) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, …). Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

-DISPOSITIVI PERSONALI (BYOD)-

Ai dipendenti è permesso svolgere la loro attività su PC fissi, portatili, dispositivi personali per le finalità descritte di seguito.

Dispositivi ammessi: qualsiasi computer portatile, tablet, e-reader, smartphone;

• I dispositivi devono essere usati per soli scopi didattici (compreso il registro elettronico)

• Connessione alla rete Wi-Fi dell'Istituto: ogni lavoratore potrà usare la connessione wifi disponibile all'interno dell'Istituto solo per finalità didattiche o, comunque, istituzionali. Chi riceve le credenziali per l'accesso alla rete d'Istituto, avrà cura di conservarle in modo sicuro e l'obbligo di non diffonderle a terzi.

L'utilizzo di memorie esterne personali (quali chiavi USB, memory card, cd-rom, DVD, macchine fotografiche, videocamere, tablet, …) è autorizzato per scopi didattici e non per salvare dati sensibili.

I Responsabili non dipendenti (ovvero i consulenti e collaboratori esterni), possono utilizzare i propri dispositivi personali per memorizzare dati dell'Istituto solo se espressamente autorizzati dall'Istituto stesso e assumendone formalmente e personalmente l'intera responsabilità del trattamento.

Tali dispositivi dovranno essere preventivamente valutati dall'Istituto, per la verifica della sussistenza di misure minime ed idonee di sicurezza.

-DISTRUZIONE DEI DISPOSITIVI-

Ogni dispositivo ed ogni memoria esterna affidati ai incaricati, (computer, notebook, tablet, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del loro utilizzo dovranno essere restituiti all'Istituto, che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento.

In particolare, l'Istituto provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

GESTIONE DATI CARTACEI

- Clear Desk Policy -

Gli Incaricati sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

Gli incaricati sono invitati dall'istituto ad adottare una "politica della scrivania pulita". Ovvero si richiede agli incaricati di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dell'Istituto.

I principali benefici di una politica della scrivania pulita sono:

− Una buona impressione agli utenti che usufruiscono dei servizi dell'istituto

− La riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle.

− La riduzione che documenti confidenziali possano essere sottratti all'istituto.

In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa, oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.

Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione), sarà cura degli Incaricati riporre in luogo sicuro (armadio, cassettiera, archivio, …) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti nell'Istituto.

A fine giornata, deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania in ordine.

Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica.

Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archiviarli digitalmente.

È necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un’apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.

E’ buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti.

SEZIONE 4

APPLICAZIONE E CONTROLLO

-Il controllo -

L'Istituto, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

− Tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati.

− Evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo.

− Verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire anche con audit e vulnerability assesment del sistema informatico. Per tali controlli l'organizzazione si riserva di avvalersi di soggetti esterni.

-Modalità di verifica-

In applicazione del principio di necessità e minimizzazione dei dati art. 5 GDPR l'organizzazione promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili agli incaricati e allo scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti informatici.

L'Istituto informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

In particolare, eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte degli incaricati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.

Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (es. scarico di file pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) si effettuerà un avvertimento in modo generalizzato con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

SEZIONE 5

VALIDITA’, AGGIORNAMENTO ED AFFISSIONE

CONCLUSIONI