Istituto Comprensivo di Medesano

Via De Gasperi 2 — tel 0525.420.403
43014 Medesano (PR) — fax 0525.422.659
C.M. PRIC80900A — mail pric80900a@istruzione.it
C.F. 92103030349 — web www.icmedesano.edu.it

VADEMECUM INCARICATO A. S. 2022/23

Gentile incaricato al fine di consentirle il trattamento di dati personali relativi a nostri clienti / fornitori, / alunni famiglie / dipendenti e collaboratori, Le è stato affidato con provvedimento contestuale all'invio della presente uno specifico incarico. A tutela Sua e dei dati che dovrà trattare nello svolgimento della collaborazione in essere con noi, è previsto che l'accesso ai programmi software e/o agli strumenti elettronici utilizzati nello svolgimento dell'attività lavorativa sia protetto da una password associata all'identificativo della sua identità (user id). Per garantire l'esatto adempimento delle disposizioni di legge, La invito a leggere attentamente il seguente documento e a rispettare le prescrizioni in esso contenute.

MANUALE SULLA SICUREZZA DEL TRATTAMENTO DEI DATI PERSONALI

Il diritto della Privacy è stato interamente riscritto dalla normativa comunitaria contenuta nel Regolamento Europeo 679/2016, pubblicato sulla Gazzetta ufficiale dell'Unione Europea il 4 maggio 2016 e definitivamente entrato in vigore a partire dal 25 maggio 2018.

Ai sensi del Reg. UE 679/2016 per trattamento si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Va innanzitutto rilevato che le categorie di dati previste dal Regolamento sono le seguenti.

« dato personale »: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificati- vo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

« dati particolari »: dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici,

dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

« dati giudiziari » dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza,

La legge prevede che l'accesso ai programmi software e/o agli strumenti elettronici utilizzati nello svolgimento dell'attività lavorativa sia protetto da una password associata all'identificativo delle sua identità (user id).

L'obiettivo di questa prescrizione è evitare che persone non conosciute e non autorizzate accedano a dati personali.

A QUESTO SCOPO LA SICUREZZA DELLA PASSWORD E' ESSENZIALE per garantire tale segretezza occorre rispettare le seguenti norme:

1) Nel momento in cui ha assunto la qualità di incaricato del trattamento di dati personali Le è stato assegnato un codice identificativo e una password utile per il primo accesso: la password dovrà essere modificata al primo accesso in modo da essere nota solo all'utilizzatore.

Qualora abbia accesso a più sistemi di gestione, potranno essere forniti diversi codici indentificativi. Per ciascuno di essi dovrà effettuare quanto indicato al punto 1). La password può essere la stessa.

3) Successivamente al primo utilizzo la password dovrà essere periodicamente modificata.

4) La password impostata non deve contenere riferimenti agevolmente riconducibili a lei (nome di battesimo, data di nascita, nome del coniuge, dei figli ecc.); è preferibile alternare lettere maiuscole, minuscole, caratteri speciali, es. *%).

5) La lunghezza della password deve superare n. …… caratteri. Qualora il sistema consenta password più corte, la lunghezza deve essere quella massima consentita dal sistema.

6) La password non deve essere comunicata a nessuno, né all'interno dell'ufficio, né all'esterno.

7) A nessuno è consentito in base a ragioni di servizio o di gerarchia di chiederle di comunicare la sua password.

8) Non è consentito lasciare la password in formato intellegibile (post it appunti ecc….) in evidenza presso la sua postazione di lavoro. Se si ritiene di dover disporre della password in forma scritta per ragioni pratiche, si deve conservare in un cassetto chiuso o tenerla presso di sé.

In base al codice identificativo e alla conferma dell'identità dell'utilizzatore ottenuta tramite password, vengono stabiliti dal sistema i diritti d'accesso agli specifici trattamenti e a i dati.

Chiunque dovesse utilizzare un identificativo altrui per accedere a dati a cui non è autorizzato può acquisire o modificare informazioni usando l'identità di altro utilizzatore, e dunque

facendo ricadere su quello ogni conseguenza.

Al fine di evitare confusioni e/o abusi, la legge prescrive che il codice identificativo assegnato non possa essere più riassegnato ad altri, anche in caso di dimissioni o di trasferimento.

A completamento di quanto sopra sempre al fine di assicurare la tutela dei dati personali e l'autotutela degli incaricati, dovranno essere poste in essere le seguenti norme:

- tutti i PC in uso dovranno essere dotati di salvaschermo con parola chiave associata.
- - la password associata al salvaschermo dovrà essere definita e modificata secondo le regole previste per tutte le password e descritte nella presente comunicazione.
- qualora gli strumenti in uso non consentissero l'uso di salvaschermo sarà cura dell'incaricato spegnere o disattivare il dispositivo di accesso ai dati (terminale o PC) ogni qual volta dovrà assentarsi dal posto di lavoro senza poter controllare eventuali usi illegittimi durante l'assenza.

Per quanto riguarda il materiale cartaceo, è invitato a non lasciare mai cartelle fascicoli o quant'altro possa contenere dati personali di soggetti interessati privi di custodia, intendendosi con ciò anche la semplice dimenticanza degli stessi sopra scrivanie o all'interno di mobili non provvisti di chiusura a chiave.

Sarà quindi sua cura, nel caso in cui dovesse venire meno il Suo controllo effettivo sul materiale cartaceo, riporre lo stesso all'interno di appositi archivi non accessibili da parte di persone non autorizzate in quanto ad esempio provvisti di chiusura con lucchetto.

Nel caso in cui per necessità di servizio dovesse trasportare fuori dai locali dell'ufficio materiale contenente dati personali sarà sua cura non lasciare che soggetti non autorizzati possano accedere a detti documenti e/ fiels.