I ISTRUZIONI
O OPERATIVE
P PRIVACY

REDATTO AI SENSI E PER GLI EFFETTI DELL'ART. 29 REL REGOLAMENTO U.E. 2016/679 AL FINE DI ISTRUIRE GLI AUTORIZZATI AL TRATTAMENTO CIRCA LE MODALITA' DELLO STESSO.

COMPLETO DI:

PRINCIPI BASE DI IGIENE INFORMATICA

MODELLO REV. 2022

STUDIO TECNICO LEGALE
CORBELLINI
Studio AG.I.COM. S.r.l.

Redatto a cura e negli uffici del D.P.O. :

STUDIO AG.I.COM. S.R.L. UNIPERSONALE
Via XXV Aprile, 12 – 20070 SAN ZENONE AL LAMBRO (MI)
Tel. 02 90601324 Fax 02 700527180 info@agicomstudio.it

www.agicomstudio.it

SCOPO DEL PRESENTE MANUALE

E' da precisare in premessa che le presenti Istruzioni Operative Privacy (I.O.P.), costituiscono parte integrante della lettera di autorizzazione che ha ricevuto in qualità di soggetto che opera all'interno dell'Istituto Scolastico e che quindi è necessitato a trattare dati personali al fine di svolgere correttamente le mansioni previste dal proprio profilo professionale.

Con la locuzione "istruzioni operative" intendiamo una raccolta di obblighi, indicazioni, procedure e divieti, presentata al fine di ottemperare all'obbligo di cui all'Art. 29 del Regolamento U.E. 2016/679: "*Il responsabile del trattamento o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali, non può trattare tali dati se non è stato istruito in tal senso dal titolare del trattamento…"*.

Questo manuale viene messo nella disponibilità di tutti gli autorizzati ed inoltre viene utilizzato come testo di riferimento in occasione dei corsi di formazione che devono essere svolti all'interno dell'Istituto.

Ma qual è lo scopo ultimo che si prefigge l'Istituto fornendo queste istruzioni operative?
Semplificando, ma non troppo, possiamo dire che tutte le istruzioni contenute in questo documento si prefiggono l'obiettivo di scongiurare che dati personali appartenenti ad allievi, dipendenti o fornitori dell'Istituto, vengano divulgati e quindi posti nella disponibilità di chi non è autorizzato a conoscerli (in altre parole l'obiettivo di tutelare la loro privacy).

DEFINIZIONI

Perché tutti possano comprendere al meglio quanto scritto nel presente manuale, prendendo spunto dall'articolo 4 del Regolamento UE 2016/679 (GDPR), diamo alcune definizioni di base:

Dato anonimo / personale: Si parla di "dato personale" quando ci troviamo di fronte ad una informazione riferibile ad una persona fisica identificabile (ad es. Mario Rossi di 3C ha i capelli biondi), mentre se l'informazione non fa riferimento a nessuno nello specifico (p.es. il 30% degli allievi che frequentano l'Istituto ha i capelli biondi) allora siamo di fronte ad un dato anonimo.
Le normative sulla privacy, dalla loro nascita a tutt'oggi, tutelano solo ed esclusivamente i dati personali.
E' chiaro a tutti che il livello di tutela richiesto dipende non solo dal fatto che il dato sia personale, ma anche dalla delicatezza dell'informazione.
Una informazione come "*essere diversamente abile*" è ovviamente molto più delicata rispetto ad "*avere i capelli biondi*" e quindi la normativa ha introdotto diverse gradazione al concetto di dato personale: il dato comune, il dato particolare ed il dato giudiziario.

Dato comune / particolare / giudiziario: Un dato personale si dice "particolare" quanto fa riferimento: allo stato di salute, all'orientamento sessuale, all'orientamento politico o alla fede religiosa di un soggetto. Si parla inoltre di dato particolare quando si tratta di informazioni genetiche (D.N.A. etc.) o biometriche (impronte digitali etc.).
Con il termine "dato giudiziario" invece si intendono i precedenti penali ed i carichi pendenti di un soggetto, ossia i suoi trascorsi giudiziari. Tutti i dati che, pur essendo personali, non rientrano nelle definizioni sopra date (anagrafici, andamento scolastico, importo dello stipendio, orari etc.) si definiscono "dati comuni".
E' bene precisare che, anche i dati comuni, in quanto dati personali, sono tutelati ma con una intensità minore rispetto a quanto non sia previsto per i dati particolari e giudiziari.

Trattamento: senza scomodare la definizione di legge, possiamo ben dire che costituisce un trattamento di dato personale qualsiasi operazione io svolga con un dato personale (raccolta, registrazione, organizzazione, trasmissione, cancellazione etc.) anche la mera detenzione.
Questo significa che la sola custodia all'interno della nostra borsa di un foglietto riportante il numero di telefono di un allievo o la memorizzazione del medesimo numero sul nostro telefono, costituisce un trattamento di dato personale ed è quindi regolamentato dalla legge.
Nel primo caso (foglietto in borsa) saremo di fronte ad un trattamento di dato in formato cartaceo, nel secondo caso (memorizzazione nel telefono) in formato digitale.

Titolare del Trattamento: E' l'Istituto Scolastico, incarnato nella persona che ne ha la rappresentanza legale. Nel caso delle Scuole Statali, tale incarico è del Dirigente Scolastico, mentre per le Scuole Paritarie, dipende dalla loro forma giuridica (società, cooperativa, ente etc.).

Autorizzato al Trattamento: Partendo dal presupposto che il Titolare del Trattamento, da solo, non può portare avanti l'intera attività scolastica, tutti i suoi collaboratori interni che lo affiancano nell'attività (Segreteria, Docenti, Collaboratori Scolastici, Assistenti Tecnici etc.) sono da considerarsi "Autorizzati al Trattamento".
Naturalmente non tutte le autorizzazioni hanno lo stesso perimetro, esistono autorizzazioni molto ampie (Collaboratore vicario, D.S.G.A., Segretario Generale etc.), altre più ridotte (Docente che presta servizio in 2B, Assistente Amministrativo etc.) ed altre ancora solo eventuali (Collaboratore Scolastico, Ausiliario, Tecnico etc.).
Il perimetro dell'autorizzazione è evidenziato nella lettera di autorizzazione a cui il presente manuale è allegato.

Responsabile del Trattamento: Il concetto è affine a quello sopra definito di autorizzato, cambia il fatto che il responsabile è normalmente un soggetto esterno (che quindi non ha un contratto di lavoro con la scuola), con una propria organizzazione autonoma, a cui l'Istituto attribuisce compiti di trattamento dati (gestore del registro elettronico, della segreteria digitale, tesoreria, RSPP, DPO, Medico Competente etc.).
In questo caso la sua designazione avviene mediante un vero e proprio contratto.

ADEMPIMENTI GENERALI

Apriamo elencando alcune regole generali valide per tutti:

- rispettare i principi generali del GDPR, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi, è vietato trattare i dati in modo diverso rispetto a quanto previsto dalle procedure interne;

- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;

- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti dell'azienda/ente;

- rispettare le misure di sicurezza adottate, atte a salvaguardare la riservatezza e l'integrità dei dati;

- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;

- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;

- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;

- mantenere riservate le proprie credenziali di autenticazione;

- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;

- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;

- informare senza ritardo il proprio responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;

- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;

- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

ISTRUZIONI OPERATIVE

All'interno dell'Istituto Scolastico, al fine di scongiurare ogni violazione di dati personali, tutti gli Autorizzati al Trattamento dei dati sono tenuti ad adottare le seguenti misure di sicurezza:

MISURE DI SICUREZZA DI NATURA TECNICA

Queste misure di sicurezza sono rivolte a tutti i soggetti autorizzati che siano anche utenti informatici (ossia che abbiano a disposizione delle credenziali per l'accesso ad una o più reti, locali o remote, di Istituto).
Si precisa che, all'interno delle regole che seguono, talvolta si fa riferimento genericamente al "servizio tecnico" quale riferimento per ogni questione di natura informatica; Con tale termine si intende il soggetto interno o esterno a cui ordinariamente l'Istituto si rivolge per la gestione e la manutenzione del sistema informatico.

MISURA DI SICUREZZA	RISCHIO CONTRASTATO
La parola chiave (password) relativa all'utenza creata per Lei per accedere alle reti, locali o remote, di Istituto, deve essere custodita con grande cura in modo da scongiurare che possa venire nella disponibilità di altri soggetti. E' vietato utilizzare password eccessivamente banali (data di nascita, nome del figlio etc.), devono essere complesse, formate da almeno 8 caratteri e costituite almeno da una lettera maiuscola, una minuscola ed un numero.	**ACCESSO AI DATI DIGITALI DA PARTE DI SOGGETTI NON AUTORIZZATI**
Le parole chiave (password) devono essere modificate al primo accesso dopo la loro consegna e poi con una frequenza trimestrale.	
E' vietato comunicare, anche se richiesta, la password personale a chiunque. Se questo dovesse accadere per questioni di natura tecnica, è necessario modificarla immediatamente dopo.	
E' vietato collocare file contenenti dati personali, in qualsiasi formato, in aree (cartelle) comuni accessibili a chiunque, in tali aree è consentito salvare esclusivamente documenti anonimi quali la modulistica.	
E' vietato utilizzare chiavette o altri device personali sui sistemi informatici scolastici prima di aver eseguito una scansione antivirus degli stessi.	**DISTRUZIONE E CONSEGUENTE PERDITA DEI DATI**
E' vietato trasferire dati personali di natura particolare o giudiziaria tramite e-mail in chiaro, ossia senza averli preventivamente criptati (protetti con password) ed aver trasmesso la password mediante una altro canale (altra e-mail, telefonata etc.).	**COMUNICAZIONE INDEBITA DI DATI PERSONALI**
E' vietato utilizzare drive o cloud o altri strumenti che non siano espressamente autorizzati dal Titolare del Trattamento per collocare dati personali riferibili ad interessati (allievi, dipendenti, fornitori). Per il collocamento dei dati è necessario che il Titolare intrattenga un rapporto contrattuale con il soggetto gestore del servizio remoto.	
I supporti informatici contenenti dati personali (chiavette, dischi removibili etc.), prima della loro dismissione, devono essere trattati in modo che tali dati non siano in alcun modo recuperabili (formattazione a basso livello dei dischi o distruzione fisica).	
Tutti i supporti magnetici rimovibili (chiavette USB, dischi etc.) contenenti dati particolari e giudiziari, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati, ciascun utente potrà contattare il personale del Servizio Tecnico (interno od esterno) ed seguire le istruzioni da questo impartite per la loro distruzione. In ogni caso, i supporti magnetici contenenti dati particolari o giudiziari devono essere dagli utenti adeguatamente custoditi in armadi chiusi o, in alternativa, criptati mediante impiego di password L'utente è responsabile della custodia dei supporti e dei dati in essi contenuti.	**USO IMPROPRIO DI SUPPORTI REMOVIBILI**

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. È fatto divieto di utilizzare le caselle di posta elettronica ufficiali per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per: l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa; l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list; la partecipazione a catene telematiche (o di Sant' Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Servizio Tecnico e non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. È obbligatorio porre la massima attenzione nell'aprire gli allegati di posta elettronica, non eseguire download di file eseguibili o documenti da siti Web o FTP non conosciuti. Sarà comunque consentito al Titolare del trattamento o persona da lui individuata, di accedere alla casella di posta elettronica dell'utente per ogni ipotesi rilevante ed urgente per cui si renda necessario.	**USO IMPROPRIO DELLA POSTA ELETTRONICA**
Il PC, laptop o notebook, assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa. È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo che tale comportamento, durante l'orario di lavoro, sia espressamente autorizzato dal Titolare del Trattamento. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per: l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione; l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal Titolare del trattamento e comunque nel rispetto delle normali procedure di acquisto; ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa; la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Titolare; Gli eventuali controlli, compiuti dal personale incaricato dal Titolare del Trattamento del Servizio Tecnico, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta.	**USO IMPROPRIO DI INTERNET**

MISURE DI SICUREZZA DI NATURA COMPORTAMENTALE

Queste misure di sicurezza sono rivolte, in generale, a tutti i soggetti autorizzati.

MISURA DI SICUREZZA	RISCHIO CONTRASTATO
I dati personali detenuti in formato cartaceo, devono essere custoditi all'interno di cassetti, schedari o armadi chiusi a chiave.	**ACCESSO AI DATI DA PARTE DI SOGGETTI NON AUTORIZZATI**
La chiave dei cassetti, schedari o armadi in cui vengono custoditi i dati personali in formato cartaceo deve essere detenuta in via esclusiva da coloro che hanno l'autorizzazione a poter trattare quei dati.	
E' vietato a tutto il personale che non ne abbia titolo specifico, l'accesso ai locali di direzione, segreteria, CED ed agli archivi, in assenza di un operatore autorizzato.	
Il personale che presta servizio nei locali di direzione, segreteria, CED ed agli archivi, quando esce dagli stessi e si accorge di essere l'ultimo, si preoccupa della loro chiusura a chiave salvo che i dati personali in essi contenuti non siano resi inaccessibili mediante la loro collocazione all'interno di cassetti, schedari e armadi chiusi a chiave ed elaboratori protetti da password.	
E' vietato trasferire dati personali di natura particolare o giudiziaria tramite semplici fogli che non siano celati all'interno di buste, cartellette o altri contenitori che consentano il loro occultamento.	**COMUNICAZIONE INDEBITA DI DATI PERSONALI**
I documenti cartacei contenenti dati personali, al momento della loro dismissione, devono essere distrutti mediante impiego di distruggidocumenti o finemente triturati anche mediante metodi manuali.	
E' vietata la comunicazione di ogni dato personale al di fuori dei casi in cui la stessa sia espressamente prevista dalla legge o prevista dall'organizzazione scolastica.	
L'utente è responsabile di ogni device (PC, tablet, smartphone etc.) assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro. Quando gli stessi sono utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni sia ai dati che al device stesso.	**SOTTRAZIONE E SMARRIMENTO DEI DEVICE SCOLASTICI**
I dati personali possono essere forniti a chi non è autorizzato a conoscerli anche con la modalità più semplice del mondo ossia parlando ad alta voce con chi è autorizzato a conoscerli, senza preoccuparsi del fatto che qualcuno nelle vicinanze li possa indebitamente ascoltare. Per questo motivo, l'autorizzato deve avere cura di tenere un tono di voce adeguato all'argomento che viene trattato quando parla al telefono o durante i colloqui individuali o ancora nell'attività di sportello.	**ASCOLTO DI DATI PERSONALI DA PARTE DI SOGGETTI NON AUTORIZZATI**

DATA BREACH

Queste misure di sicurezza sono rivolte, in generale, a tutti i soggetti autorizzati, nel momento in cui vengono a conoscenza di una violazione di dati personali, commessi da loro stessi o da altri.

MISURA DI SICUREZZA	RISCHIO CONTRASTATO
Quando si verifica una violazione di dati personali, il Titolare del trattamento, entro 72 ore, deve darne notizia all'Autorità Garante per la protezione dei dati, notificando quella che, nella terminologia del G.D.P.R., si chiama "*data breach*" che in italiano significa "breccia nei dati". Chiunque si renda conto di una violazione deve pertanto darne immediata comunicazione al Titolare del Trattamento.	**MANCATA O RITARDATA NOTIFICA AL GARANTE DELLA VIOLAZIONE**

COME DIFENDERCI DAI RISCHI CONNESSI ALL'UTILIZZO DI DEVICE ?

PRINCIPI BASE DI IGIENE INFORMATICA

Tratto dal corso

"Didattica Digitale Integrata e Lavoro Agile – CYBERSECURITY & PRIVACY" – Luca Corbellini – 30/11/2020

CORBELLINI