



**ISTITUTO COMPRESIVO STATALE
"DANIELA SETTESOLDI"**

Via del Capannone, 19 - 56019 Vecchiano (PI)
codice fiscale: 93044960503 - codice meccanografico: PIIC811002
Tel. + 39 050 868 444 - Fax + 39 050 864 393
PEO: piic811002@istruzione.it - PEC: piic811002@pec.istruzione.it
sito: <http://www.icvecchiano.gov.it> - codice univoco ufficio: UFZNY3



FORMAZIONE GDPR (RGDP)

GENERAL DATA PROTECTION REGULATION (REGOLAMENTO GENERALE PROTEZIONE DATI)

CORSO FORMAZIONE SULLA PROTEZIONE DEI DATI PERSONALI A SCUOLA

Dott. Fabio Marfori
Responsabile Protezione Dati (RPD-DPO)
Vecchiano, novembre 2021

GLI OBIETTIVI

Questo corso vuole raggiungere i seguenti obiettivi:

- Spiegare l'**importanza** al personale dell'Istituto del trattamento dei dati personali
- Aumentare la **consapevolezza** del personale sul principio che la legislazione, gli standard e le politiche si applicano a tutti i dati personali trattati e mantenuti dall'Istituto e include dati che appartengono all'Istituto, ai dipendenti, agli studenti e ai loro genitori
- Impostare gli **standard minimi** per il personale riguardo alla protezione dei dati
- Descrivere la **legislazione**, in modo specifico il GDPR, che si applica al trattamento dei dati personali



LEGISLAZIONE SULLA PROTEZIONE DEI DATI

GDPR

- ✓ **REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI - GENERAL DATA PROTECTION REGULATION** in vigore da 25 maggio 2018 - [Regolamento \(UE\) 2016/679](#)
- ✓ **Decreto legislativo 10 agosto 2018 n. 101** recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679.

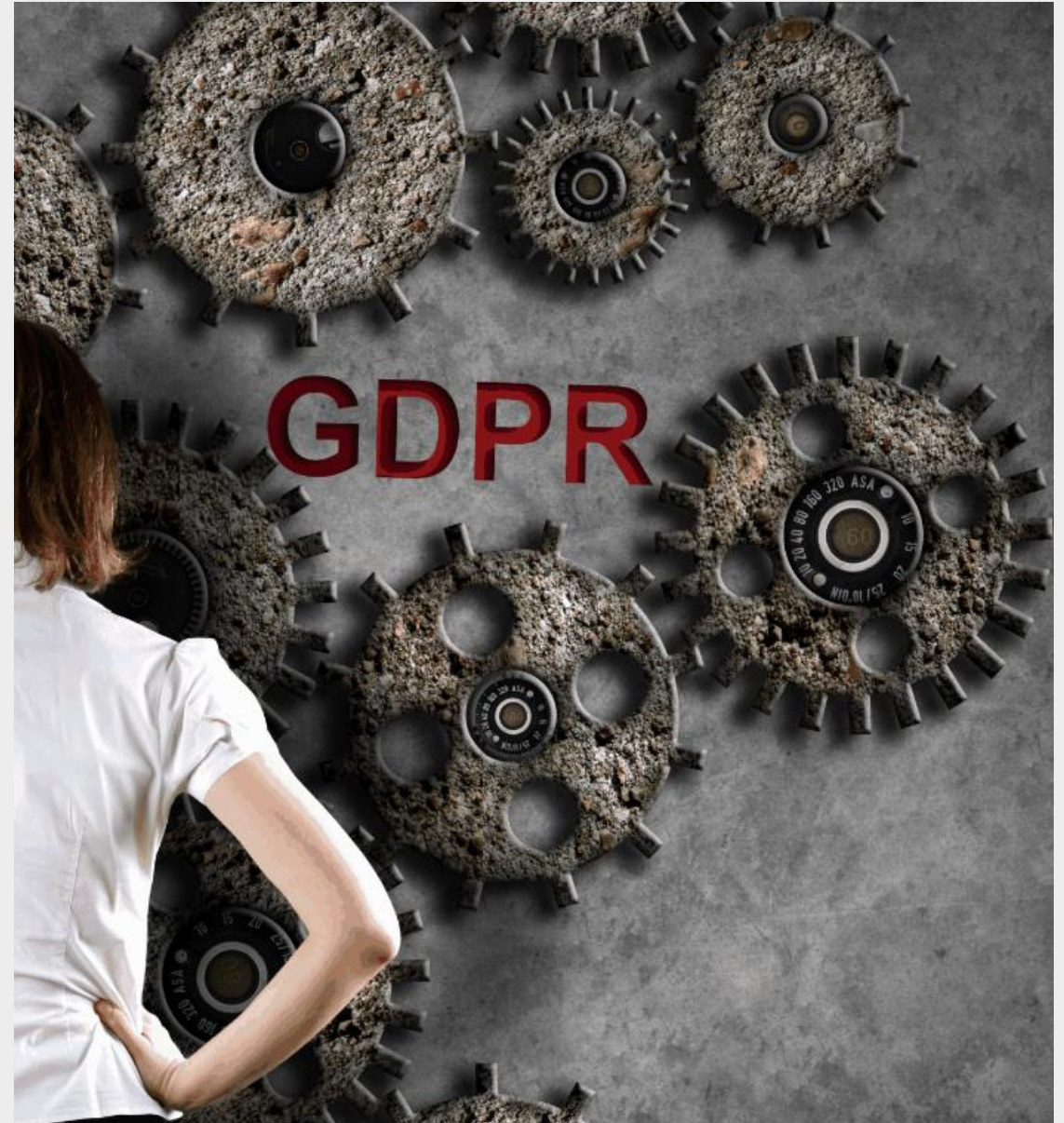


- Si applica agli stati membri della UE e a tutte le organizzazioni che trattano dati di soggetti della UE o che offrono servizi a soggetti dell'UE – dovunque esse si trovino
- Introduce diritti specifici e significativi per i soggetti sulla compensazione, diritto alla cancellazione, rettifica, etc. La **compensazione** può essere richiesta nei confronti dell'organizzazione e dei suoi impiegati
- Multe fino a **20.000.000 di euro o il 4% del fatturato globale annuo** per perdita di dati/non conformità

CHI E' RESPONSABILE?

La responsabilità non solo è del titolare del trattamento ma in generale di chi tratta i dati – quindi di **tutti**

- Rispettare la **privacy** degli individui e proteggere qualsiasi dato al quale si accede o tratta
- Comprendere gli individui hanno **diritti** che si applicano ai loro dati personali
- Inoltrare immediatamente qualsiasi **richiesta di accesso** dei propri dati personali alla **SEGRETERIA** a meno che non sia già coperta da una procedura interna (es Amministrazione che fornisce copia dei cedolini paga al personale)
- Segnalare eventuali **dubbi** riferiti alla protezione e trattamento dei dati personali
- Assicurarci di archiviare o processare dati personali solo se è stato fornito **permesso e approvazione** per farlo



TIPOLOGIE DI DATI

Sono **dati personali** le informazioni che identificano o rendono identificabile, **direttamente o indirettamente**, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..



PERSONALI

Particolarmente importanti sono:

- i **dati che permettono l'identificazione diretta** - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i **dati che permettono l'identificazione indiretta**, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);

- i **dati rientranti in particolari categorie**: si tratta dei dati c.d. "*sensibili*", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute, alla vita o all'orientamento sessuale.

Il [Regolamento \(UE\) 2016/679](#) (articolo 9) ha incluso nella nozione anche i **dati genetici** e i **dati biometrici**;



PARTICOLARI
(SENSIBILI)

- i **dati relativi a condanne penali e reati**: si tratta dei dati c.d. "*giudiziari*", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Il [Regolamento \(UE\) 2016/679](#) (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.



GIUDIZIARI

Con l'evoluzione delle nuove tecnologie, **altri dati personali** hanno assunto un ruolo significativo, come **quelli relativi alle comunicazioni elettroniche** (via Internet o telefono) e **quelli che consentono la geolocalizzazione**, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

COSA SIGNIFICA TRATTARE?

- RACCOGLIERE
- REGISTRARE
- CONSERVARE
- MODIFICARE
- ALTERARE
- USARE
- MOSTRARE
- TRASMETTERE
- DIFFONDERE
- CANCELLARE
- Distruggere

Il trattamento è consentito solo in determinate circostanze, giustificato da basi giuridiche.



BASE GIURIDICA DEL TRATTAMENTO DEI DATI

- ✓ CONSENSO
- ✓ ADEMPIMENTO DI OBBLIGHI CONTRATTUALI O MISURE PRECONTRATTUALI
- ✓ OBBLIGHI DI LEGGE CUI È SOGGETTO IL TITOLARE DEL TRATTAMENTO
- ✓ INTERESSI VITALI DELLA PERSONA INTERESSATA O DI TERZI
- ✓ LEGITTIMO INTERESSE PREVALENTE DEL TITOLARE O DI TERZI CUI I DATI VENGONO COMUNICATI
- ✓ INTERESSE PUBBLICO O ESERCIZIO DI PUBBLICI POTERI



Il CONSENSO deve essere specifico e liberamente espresso dalle persone interessate
Non sempre è necessario richiedere il consenso.
Esempi di consenso sono le informative fatte firmare al personale, studenti/genitori sul trattamento di foto e audio/video.

DIRITTI DEGLI INTERESSATI

- ✓ **Diritto a essere informato** – ciascun individuo comprende cosa è fatto dei suoi dati
- ✓ **Diritto di accedere** – ciascun individuo può richiedere di accedere ai propri dati
- ✓ **Diritto alla rettifica** – ciascun individuo può richiedere di modificare i propri dati
- ✓ **Diritto alla cancellazione** - ciascun individuo può richiedere la cancellazione dei propri dati
- ✓ **Diritto a limitare il trattamento** – ciascun individuo può richiedere che i propri dati non vengano trattati
- ✓ **Diritto di obiettare** - ciascun individuo deve avere un punto di contatto dove poter reclamare

Nelle informative questi diritti devono essere ricordati

VIOLAZIONI DELLA PROTEZIONE DEI DATI

Se sospettate o siete stati informati che dati personali sono stati violati dovete farlo presente ai responsabili.

Il riferire subito le violazioni è fondamentale perché il GDPR richiede che sia fatta una indagine entro **72 ore** e comunicata alle autorità nello stesso periodo.

Tipi di violazioni sono

- **Compromissione dei dati personali** – es spedire email a destinatari non autorizzati, danneggiamento (hacking) di un sistema, permettere a persone non autorizzate di accedere a un sistema attraverso account non autorizzati
- **Perdita/furto di dati personali** – es furto di documenti cartacei, computer, chiavi USB
- **Uso non autorizzato di dati personali** – uso dei dati per scopi non collegati a quelli dell'Istituto – es creare mailing list per propri affari o ragioni politiche o proprie ricerche



COME POSSO SAPERNE DI PIU'?

- Modelli di informative conservate nell'Istituto
- Regolamento degli incaricati
- Testo del regolamento
- Sito web del Garante della Privacy
<https://www.garanteprivacy.it/>

<https://www.garanteprivacy.it/scuola>



COME POSSO SAPERNE DI PIU'?

- Modelli di informative conservate nell'Istituto
- Regolamento degli incaricati
- Testo del regolamento (GDPR)
- Sito web del Garante della Privacy

<https://www.garanteprivacy.it/scuola>



LA SCUOLA A PROVA DI PRIVACY

Il vademecum è stato realizzato prima dell'applicazione del Regolamento UE 679/2016, avvenuta in data 25 maggio 2018, circostanza di cui occorre tener conto nella consultazione



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Il vademecum è stato realizzato prima dell'applicazione del Regolamento UE 679/2016, avvenuta in data 25 maggio 2018, circostanza di cui occorre tener conto nella consultazione



REGOLE GENERALI

- ✓ Studenti e famiglie informate
- ✓ Trattamento dei dati nelle istituzioni scolastiche pubbliche
- ✓ Trattamento dei dati nelle istituzioni scolastiche private
- ✓ Dati sensibili e giudiziari: alcuni esempi concreti
- ✓ Diritto di accesso ai dati personali
- ✓ Violazione della privacy



VITA DELLO STUDENTE

- ✓ Iscrizione a scuole e asili
- ✓ Temi in classe
- ✓ Voti ed esami
- ✓ Comunicazioni scolastiche
- ✓ Disabilità e disturbi specifici dell'apprendimento Gestione del servizio mensa
- ✓ Dalla scuola al lavoro
- ✓ Curriculum e identità digitale dello studente



MONDO CONNESSO E NUOVE TECNOLOGIE

- ✓ Cyberbullismo e altri fenomeni di rischio
- ✓ Smartphone e tablet
- ✓ Immagini di recite e gite scolastiche
- ✓ Registrazione della lezione e strumenti compensativi



VIDEOSORVEGLIANZA E ALTRI CASI

- ✓ Videosorveglianza contro furti e vandalismi
- ✓ Questionari per attività di ricerca
- ✓ Marketing e promozioni commerciali



PUBBLICAZIONE ON LINE

- ✓ Pubblicità e trasparenza
- ✓ Portale unico dei dati della scuola
- ✓ Graduatorie del personale e supplenze
- ✓ Pagamento del servizio mensa
- ✓ Servizi di scuolabus



Prassi operative collaboratori scolastici

NOMINA AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI

- Ai sensi dell'art. 29 del Regolamento, in relazione alle operazioni di trattamento dei dati personali, su supporto cartaceo e/o elettronico, ai quali avete accesso nell'espletamento delle funzioni e dei compiti assegnati nell'ambito del rapporto di lavoro con l'istituzione scolastica e disciplinati dalla normativa in vigore e dai contratti di settore.
- In particolare, in qualità di Collaboratori scolastici, Vi può essere affidata temporaneamente la custodia, lo spostamento, l'archiviazione o la riproduzione (nell'ambito dei locali dell'istituzione scolastica) di documenti contenenti dati personali, nonché la ricezione di documentazione (quale, ad esempio, richieste di uscite anticipate o domande di iscrizione a scuola) da parte delle famiglie degli alunni o di altre persone.

PROTEZIONE DEI DOCUMENTI CARTACEI

- ✓ Conservare POSSIBILMENTE i dati del cui trattamento si è incaricati in appositi armadi, dotati di serratura
- ✓ Non consentire l'accesso alle aree in cui sono conservati dati personali su supporto cartaceo a estranei e a soggetti non autorizzati
- ✓ Conservare i documenti ricevuti da genitori/studenti o dal personale in apposite cartelline non trasparenti
- ✓ Effettuare esclusivamente copie fotostatiche di documenti per i quali si è autorizzati
- ✓ Provvedere personalmente alla distruzione quando è necessario eliminare documenti inutilizzati



PROTEZIONE DEI DOCUMENTI CARTACEI (FOTOCOPIE)

- ✓ Non consentire a estranei l'accesso al fax e alla stampante che contengano documenti non ancora ritirati dal personale
- ✓ Assicurarsi di non lasciare copie nella macchina (stampante o fotocopiatrice) e quando necessario eliminare le stampe mal riuscite utilizzando la macchina distruggi-documenti o stracciare manualmente il documento prima di gettarlo
- ✓ Non lasciare incustodito il registro contenente gli indirizzi e i recapiti telefonici del personale e degli studenti e non annotare il contenuto su fogli di lavoro



PARTICOLARE ATTENZIONE AI CERTIFICATI

- Accertarsi che non restino incustoditi i seguenti documenti:
 - certificati medici esibiti dagli alunni a giustificazione delle assenze;



- qualunque altro documento contenente dati personali o sensibili degli alunni o dei docenti.

Nel caso in cui si reperisse uno dei documenti summenzionati incustodito, sussiste l'obbligo di segnalarne tempestivamente la presenza al responsabile di sede e di provvedere temporaneamente alla loro custodia.

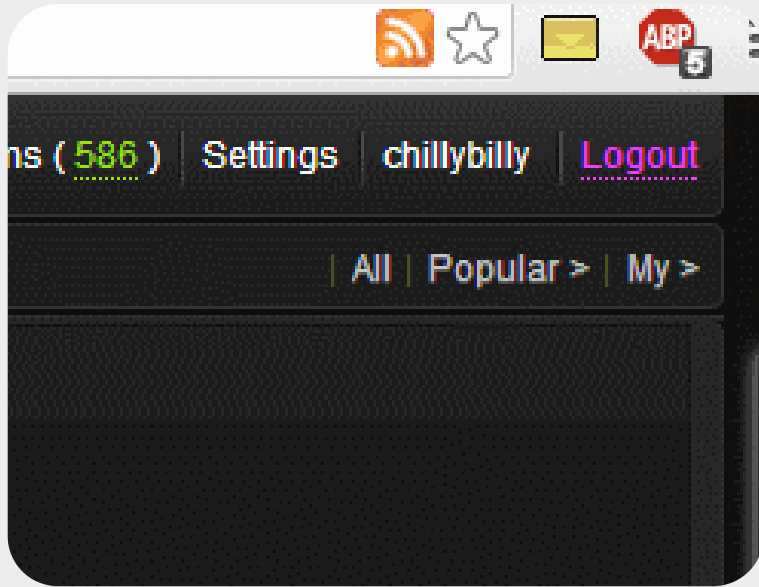
CONTROLLO DEI LOCALI

- Vigilare i locali della segreteria affinché soggetti terzi, estranei alla scuola, e quindi al trattamento dati, non entrino in contatto con le informazioni in possesso della scuola
- Procedere alla chiusura dell'edificio scolastico accertandosi che tutte le misure di protezione dei locali siano state attivate
- Procedere alla chiusura dei locali non utilizzati in caso di assenza del personale
- Procedere alla chiusura dei locali di segreteria accertandosi che siano state attivate tutte le misure di protezione e che le chiavi delle stanze siano negli appositi contenitori

PROTEZIONE DEI DOCUMENTI DIGITALI

- **Non abbandonare la postazione di lavoro per la pausa, o altro motivo, senza aver provveduto a custodire in luogo sicuro i documenti trattati**
- **Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è autorizzati dal Titolare del trattamento**

DOCUMENTI DIGITALI



Fai logout !



Usa cartelle sicure



Non salvare in pc pubblici

ATTENZIONE ALLE CHIAVETTE USB!

A volte "innocue" chiavette USB contengono un software malevolo che permette ad un criminale informatico di rubare tutti i dati presenti all'interno del PC e della rete aziendale.

COSA NON FARE

Collegare una chiavetta USB della quale non conosciamo l'esatta provenienza. Spesso questi dispositivi USB non vengono riconosciuti dall'antivirus aziendale.

COSA FARE

Contattare sempre il referente informatico.



POSTA ELETTRONICA E ALTRI MEZZI DI COMUNICAZIONE



Attenti alle email/sms/telefonate sospette

PHISHING/SMSHING/VISHING

No contenuti personali su email di scuola e viceversa

L'uomo che...

- sa quando è il tuo compleanno
- sa chi sono i tuoi amici
- sa cosa ti piace
- sa dove ti trovi

... non è il tuo uomo.
È Mark Zuckerberg.



NO AI SOCIAL NON UFFICIALI DELLA SCUOLA



GRAZIE

Dott. Fabio Marfori
Responsabile Protezione Dati (RPD-DPO)