ISTITUTO DI ISTRUZIONE SUPERIORE
"Buontalenti - Cappellini - Orlando"
LIVORNO - LI

Formazione

08.03.2024

PRIVACY E SCUOLA

Relatore:

Ing. Pietro Collevecchio: Titolare dello Studio Collevecchio
Responsabile della Protezione dei Dati dell'Istituto Buontalenti - Cappellini – Orlando di Livorno

INCONTRO DI FORMAZIONE :

- **RGPD: definizioni, principi, diritti e soggetti**
- **Focus su Policy e Trasparenza**
- **Relazione finale programma di adeguamento dell'Istituto al RGPD: registro e altri strumenti**
- **Sicurezza informatica e cybersecurity**
- **Sanzioni e casi di studio**
- **La scuola a prova di privacy**

RIFORMA EUROPEA PRIVACY - RGDP

IL PERCORSO LEGISLATIVO DI ADOZIONE DEL GDPR E' INIZIATO IL **4 NOVEMBRE 2010,** SI E' CONCLUSO IL **24 MAGGIO 2016,** APPLICAZIONE DIRETTA IN TUTTI GLI STATI DELL'UE A PARTIRE DAL **25 MAGGIO 2018.**

PRINCIPALI OBIETTIVI

ARMONIZZARE ED UNIFORMARE la normativa nella UE e nella SEE (Spazio Economico Europeo), per consentire la libera circolazione dei dati personali in tutto il territorio

ADEGUARE LA NORMATIVA ALLE NUOVE TECNOLOGIE (Social, Cloud computing, App, Mobile, Big Data, etc.) **e GESTIRE LA VELOCITA' DELL'INNOVAZIONE**

GOVERNARE LA DIMENSIONE GLOBALE DI INTERNET. Il GDPR si applica a chiunque offre servizi, anche gratuiti e opera nella UE

RGPD: FINALITA' DELL'INCONTRO

- **Sensibilizzazione al tema della protezione dei dati nell'ambito delle proprie attività presso l'Istituto scolastico, ma anche come consapevolezza dell'esistenza di un complesso normativo semplificato che restituisce ai cittadini il controllo dei propri dati personali in una società con un'evoluzione tecnologica sempre più spinta.**

- **Il Regolamento Generale sulla Protezione dei dati è il presidio dei diritti fondamentali nella società digitale. È fondamentale, infatti, comprendere che lo sviluppo della società digitale mette a rischio la libertà individuale e i diritti fondamentali delle persone, ma che proprio in difesa di tali diritti l'Europa ha voluto issare il baluardo del Regolamento.**

RGPD: ELEMENTI ESSENZIALI

- La protezione dei dati personali è un **diritto fondamentale** (art. 8 par. 1 Carta dei diritti fondamentali dell'Unione Europea)

- Al fine di assicurare **un livello coerente e elevato** di protezione delle persone e **rimuovere gli ostacoli alla circolazione dei dati personali**, il livello di protezione dei diritti e delle libertà delle persone riguardo al trattamento dei dati personali deve essere **equivalente** in tutti gli Stati membri

- **Oggetto:** norme relative **alla protezione delle persone fisiche con riguardo al trattamento dei dati personali**, nonché norme relative alla **libera circolazione di tali dati**

- Si applica a tutti i trattamenti di **dati personali di persone fisiche**

RGPD: DEFINIZIONI

Un **DATO PERSONALE** è qualsiasi informazione riguardante una **persona fisica identificata o identificabile (**ovvero riconoscibile da un soggetto esterno**)**. Dipende dal contesto.

CATEGORIE DI DATI PERSONALI:

Dati personali che rivelino l'origine razziale o etnica

Dati personali che rivelino le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale

Dati relativi alla salute – fisica o mentale, servizi di assistenza sanitaria

Dati genetici – informazioni univoche sulla fisiologia e sulla salute

Dati biometrici – ottenuti da un trattamento tecnico specifico

Dati giudiziari – relativi ad atti e procedimenti giudiziari

PRIVACY – Riservatezza dei dati personali (in relazione alla possibilità di accesso da parte di terzi)

TRATTAMENTO è **qualunque tipo di attività che riguarda un dato personale.**

PRINCIPI GENERALI DEL TRATTAMENTO AI SENSI DEL GDPR

liceità, correttezza e trasparenza

limitazione delle finalità

minimizzazione dei dati

Responsabilizzazione del Titolare

esattezza

Limitazione della conservazione

integrità e riservatezza

PRINCIPI DEL GDPR: LICEITA', CORRETTEZZA E TRASPARENZA

liceità, correttezza e trasparenza

Le organizzazioni devono assicurarsi che le loro attività di raccolta dei dati personali degli utenti non infrangano la legge e che non nascondano nulla agli interessati.
Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il **principio della trasparenza** impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro.

INFORMATIVE

Esempio: Per gli Istituti scolastici è lecito trattare i dati senza richiesta di consenso ma solo per finalità istituzionali, occorre però l'informativa estesa

PRINCIPI DEL GDPR: LIMITAZIONE DELLE FINALITA’

limitazione delle finalità

Raccolti per finalità **determinate, esplicite e legittime**, e successivamente trattati in modo che non sia incompatibile con tali finalità. Tale principio si fonda sulla stretta corrispondenza tra i motivi della raccolta dei dati personali e l’effettivo impiego degli stessi.

determinate – il titolare deve prevedere in modo sufficientemente chiaro quali siano le finalità effettive per cui ha intenzione di raccogliere e trattare i dati personali. Non sono pertanto ammesse indicazioni generiche ovvero finalità, per così dire, in corso di definizione, indefinite e/o illimitate;

esplicite – le finalità devono essere sufficientemente inequivocabili e chiaramente espresse. L’interessato deve, quindi, essere messo a conoscenza dei motivi per i cui i suoi dati sono trattati;

legittime – le finalità del trattamento devono essere lecite rispetto alla normativa applicabile e, allo stesso tempo, legittime. Non sono dunque ammesse finalità *contra legem* e men che meno finalità lecite ma illegittime.

PRINCIPI DEL GDPR: MINIMIZZAZIONE DEI DATI

minimizzazione dei dati

I dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati **(minimizzazione dei dati)**. Una raccolta di dati è **eccedente** quando risulta eccessiva, esagerata in termini numerici, troppo vasta rispetto all'intenzione di chi raccoglie le informazioni; è **non pertinente** quando non si lega all'obiettivo da raggiungere, non serve per la finalità che si prestabilisce, in sintesi è superflua. Solo prendendo in considerazione lo scopo è, quindi, possibile stabilire se i dati raccolti rispettino le condizioni di liceità (cioè se rispettino finalità determinate, esplicite e legittime) e se la loro raccolta sia strettamente necessaria al raggiungimento dello scopo prefissato.

Esempio – Newsletter – Se una società commerciale decidesse di inviare ai propri utenti una newsletter,l'unico dato personale necessario per tale attività sarebbe l'indirizzo e-mail a cui inviarla; inoltre, tale dato potrebbe essere utilizzato solo e soltanto per lo scopo indicato.

PRINCIPI DEL GDPR: LIMITAZIONE DELLA CONSERVAZIONE

limitazione della conservazione

I dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.
il criterio per determinare i tempi di cancellazione è **la necessità del dato per il raggiungimento della finalità del trattamento**.
Se un dato è necessario, non si pone nemmeno il problema della cancellazione: finché ne ho effettivo bisogno per raggiungere le finalità del trattamento, posso conservarlo. Al contrario, se un dato non è necessario significa che non verrà usato per la finalità del trattamento per la quale è stato raccolto: e se non verrà usato, allora posso cancellarlo senza alcuna conseguenza negativa.
La politica relativa alla *data retention* deve esser predisposta dal titolare con particolare attenzione tenuto conto di quanto stabiliti da norme di legge, dai provvedimenti del Garante nonché dalla giurisprudenza sviluppatasi in materia di conservazione e cancellazione di dati personali.

PRINCIPI DI LIMITAZIONE DELLE FINALITA', MINIMIZZAZIONE, CONSERVAZIONE

- **Tratta solo i dati di cui hai bisogno**
- **Raccogli meno dati possibili**
- **Fino a quando avrai bisogno dei dati raccolti ?**

Sondaggio ragazzi di una scuola:

Non raccogliere dati non inerenti allo scopo - Professione genitori, retribuzioni , luogo vacanze

Attenzione quando si pubblicano graduatorie:

Non allegare dati non necessari – indirizzi, email, numero cell.

Non tutto ciò che è pubblico è pubblicabile

Dove pubblicare gli scrutini ?
Nella sezione accessibile a tutti gli studenti – Ammesso o non Ammesso senza voti
Nell'area personale del singolo studente, con i voti
NON vanno pubblicati sul sito Internet

PRINCIPI DEL GDPR: ESATTEZZA, INTEGRITA' E RISERVATEZZA

esattezza

integrità e riservatezza

Il **GDPR** afferma che devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti.
Dato "esatto" si distingue da dato "integro". In quest'ultimo caso, infatti, rientrano tutte le alterazioni che può subire il dato derivanti da errore o da cause volontarie.

Il principio di **integrità e riservatezza** stabilisce che i dati devono essere sempre trattati in modo da garantirne una sicurezza adeguata al rischio.

Integrità – protezione dei dati e delle informazioni nei confronti delle modifiche del contenuto, accidentali (involontarie) oppure effettuate volontariamente da una terza parte

Riservatezza – I soggetti autorizzati al trattamento dei dati per finalità specifiche sono tenute a proteggere i dati dal rischio di violazioni

RESPONSABILIZZAZIONE (ACCOUNTABILITY) DEL TITOLARE

Responsabilizzazione (accountability) del titolare

L'art. 5 del regolamento europeo aggiunge, tra i vari principi da osservare nell'operare un trattamento di dati, il principio di **responsabilizzazione** (***accountability***) del titolare del trattamento.
Il regolamento europeo, infatti, sposta il fulcro della normativa in materia di protezione dei dati personali dalla tutela dell'interessato e dei suoi diritti alla **responsabilizzazione del titolare del trattamento**. Occorre precisare che *accountability* in inglese vuol dire "*dover rendere conto del proprio operato*", per cui è qualcosa in più della semplice responsabilizzazione.
Il titolare del trattamento, quindi, tenuto conto della natura, del contesto e della finalità del trattamento, dovrà garantire, ed essere in grado di dimostrarlo (appunto, renderne conto), che il trattamento è effettuato non solo in maniera conforme alla normativa ma in maniera tale da non determinare rischi e quindi gravare sui diritti e le libertà degli interessati. Si supera, quindi, la concezione formalistica del passato, quando bastava avere il consenso per sentirsi in regola, perché oggi l'essere conformi al regolamento non è più sufficiente, in quanto il titolare ha sempre la responsabilità di tutelare l'interessato e la collettività dai rischi impliciti del trattamento. E non è sufficiente adottare misure di conformità alle norme, ma occorre anche documentarle (principio di trasparenza) e garantirne l'efficacia.

RESPONSABILIZZAZIONE (ACCOUNTABILITY) DEL TITOLARE

Invio di una comunicazione contenente dati sensibili

- Un docente del Lazio ha inviato a molte persone una mail contenente dati sensibili che era ad uso interno
- Il Garante ha sanzionato e la Pubblica Amministrazione si è rivalsa nei confronti del dirigente e dei docenti coinvolti nella divulgazione
- La Corte dei Conti ha verificato che non vi fossero indicazioni adeguate per il trattamento dei dati
- Mancando istruzioni adeguate, la Corte ha sanzionato solo il dirigente

In caso di errore, chi sbaglia paga !

DIRITTI DELL'INTERESSATO AI SENSI DEL GDPR

chiedere al titolare **l'accesso ai dati** che li riguardano

revocare il consenso prestato in qualsiasi momento

ottenere, per i dati che lo riguardano, **la rettifica, l'integrazione** dei dati incompleti**, la limitazione** del trattamento

proporre reclamo all'Autorità

ricevere i dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico **("diritto alla portabilità")**

ottenere la **cancellazione** dei dati personali che lo riguardano **("diritto all'oblio")**

I SOGGETTI INTRODOTTI DAL GDPR

IL TITOLARE DEL TRATTAMENTO nella Scuola

Come si individua?

Chi sceglie strumenti e finalità del trattamento

Titolari del trattamento a Scuola:

- L'istituto scolastico nella persona del Dirigente
- Il Ministero dell'Istruzione contitolare di alcuni trattamenti
- Soggetti esterni per i quali strumenti e finalità sono di sua competenza (Comune)
- Altri – Pago PA , INDIRE*, medici, psicologi

***Istituto nazionale di documentazione innovazione e ricerca educativa**

I SOGGETTI INTRODOTTI DAL GDPR

IL RESPONSABILE DEL TRATTAMENTO

Chi e'

Nella scuola è stato individuato il DSGA come Responsabile interno di trattamento per l'articolo 2-quaterdecies del D. L. 101/2018 "Attribuzione di funzioni e compiti a soggetti designati"

figura in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.

Il responsabile del trattamento dei dati è individuabile come quella figura che ha :

- una **conoscenza specialistica** della materia
- **affidabilità**;
- possesso di **risorse** che permettano di attuare misure tecniche e organizzative in grado di soddisfare tutti i requisiti stabiliti dal Regolamento per il trattamento dei dati personali, anche sotto il profilo della sicurezza.

SOGGETTI INCARICATI O AUTORIZZATI AL TRATTAMENTO

Chi sono

"Incaricati, o autorizzati, sono i soggetti persone fisiche che effettuano materialmente le operazioni di trattamento sui dati personali"

Il Titolare o il Responsabile del trattamento possano prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti **a persone fisiche, espressamente designate**, che operano sotto la loro autorità e che sono state **istruite** in tal senso attraverso specifiche e opportune modalità

I SOGGETTI INTRODOTTI DAL GDPR

IL DATA PROTECTION OFFICER

Chi e'

"E' la persona designata in funzione della qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti"

Fra le competenze e le conoscenze specialistiche pertinenti rientrano le seguenti:

- conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, un'approfondita conoscenza del GDPR
- familiarità con le operazioni di trattamento svolte
- familiarità con tecnologie informatiche e misure di sicurezza dei dati
- conoscenza dello specifico settore di attività e dell'organizzazione
- capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione

COMPITI DEL DPO - FUNZIONI

Svolge un ruolo fondamentale all'interno del nuovo sistema di *governance* dei dati

CONSULENZA
informare e consigliare il titolare del trattamento, il responsabile del trattamento e i dipendenti in merito agli obblighi del GDPR

COOPERAZIONE
con l'autorità di controllo

VIGILANZA
sorvegliare l'osservanza del GDPR

FORNIRE UN PARERE
in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento

PUNTO DI CONTATTO
per l'Autorità di controllo e tutti gli interessati

DATA PROTECTION OFFICER

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il **Garante per la protezione dei dati personali** è un'autorità amministrativa indipendente poi disciplinata dal Codice in materia di protezione dei dati personali. E' un organo collegiale, composto da quattro membri eletti dal Parlamento

COLLABORARE
con le altre autorità di controllo

CONTROLLARE
che i trattamenti di dati personali siano conformi al Regolamento nonché a leggi e regolamenti nazionali (nel caso, prescrive le misure da adottare)

ADOTTARE
I provvedimenti previsti dalla normativa in materia di protezione dei dati personali;

ESAMINARE
I reclami

FORMULARE
pareri

POLICY

Che cosa sono le policy ?

- Le policy sono una formalizzazione delle procedure
- Le prassi non codificate possono essere comprese male, dimenticate, modificate, tramandate in maniera sbagliata

La policy deve contenere indicazioni chiare e precise

Esempi di policy per la Scuola

- Le policy sullo svolgimento delle operazioni di trattamento
- Le policy sulle informative
- Le policy sulle istanze di accesso
- Le policy per l'utilizzo di materiali foto/video raccolti nelle attività
- Le policy per la gestione dei dati relativi a studenti con particolari esigenze (DSA)
- Le policy sul data breach

POLICY

Policy sul Green Pass, sulla DAD, sullo smartworking

Policy sull'utilizzo dei sistemi di comunicazione con i genitori

Capita che i docenti della scuola usino app di messaggistica per comunicare con i genitori, direttamente o all'interno dei gruppi di classe. Si può elaborare una policy ad hoc per ricordare ai docenti quali strumenti utilizzare per gestire al meglio questo tipo di comunicazioni in modo da avere il rischio minimo di violazione dei dati personali

Policy per la pubblicazione di documenti

TRASPARENZA : L'INFORMATIVA

L'informativa è lo strumento indispensabile per attuare il principio di trasparenza

Deve essere chiara e comprensibile al destinatario

Deve essere adattata in base a finalità, dati e interessati

Contenuti:

Titolare
RPD
Base giuridica del trattamento
Finalità del trattamento
Categorie particolari di dati
Categorie di destinatari
Modalità di trattamento e conservazione
Trasferimento dei dati personali
Processo decisionali automatizzato
Diritti dell'interessato

INFORMATIVA PRIVACY

TITOLARE DEL TRATTAMENTO : Istituto di Istruzione Superiore Buontalenti - Cappellini - Orlando

liis00900c@istruzione.it

058 6405149

Piazza 2 Giugno, 22 - Livorno

L'istituto è il **TITOLARE DEL TRATTAMENTO** dei dati personali che La riguardano e che saranno gestiti in modalità cartacea o attraverso i sistemi informatici

RESPONSABILE della PROTEZIONE dei DATI : Ing. Pietro Collevecchio

pietro@studiocollevecchio.it

Il **RESPONSABILE della PROTEZIONE dei DATI** (o Data Protection Officer - DPO) è il Suo riferimento per qualsiasi questione legata all'applicazione del GDPR

DATI TRATTATI
(Categorie, requisito necessario)

Generalmente sono richiesti e trattati dati personali "comuni". In alcuni casi è necessario trattare anche dati "particolari" come l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, lo stato di salute, i dati di carattere giudiziario; sarà cura del personale di segreteria comunicare a Lei e ai Suoi familiari tutte le informazioni necessarie.

Fornire i Suoi dati personali è obbligatorio e necessario sia per l'iscrizione, sia per poter usufruire dei servizi forniti dall'Istituto

PERCHE' TRATTIAMO I DATI
(Finalità, Base giuridica)

I Suoi dati personali sono richiesti per finalità come l'istruzione e la formazione degli studenti, ma anche per il monitoraggio dei progressi conseguiti, il comportamento, le assenze, l'autenticazione ai sistemi informatici e la gestione degli accessi, la valutazione della qualità dei servizi erogati, l'adempimento degli obblighi di legge.

Se richiesto, possiamo anche trattare i dati relativi ai bisogni educativi speciali, comprese esigenze e classificazione, informazioni sulla salute, allergie, farmaci, diete e stato vaccinale.

La base giuridica su cui si basa il trattamento dei Suoi dati personali è l'**esecuzione di compiti di interesse pubblico**, l'adempimento di obblighi di legge, nonché i motivi di interesse pubblico rilevante quale il diritto all'istruzione - **PER TUTTO CIO', NON E' NECESSARIO RICHIEDERE IL SUO CONSENSO**

INFORMATIVA PRIVACY

QUANDO CHIEDIAMO IL SUO CONSENSO

Il Suo consenso è indispensabile quando il trattamento dei dati riguardano attività che richiedono una Sua autorizzazione esplicita e indipendente per:

1. effettuare pubblicazioni di **foto** su dépliant e quotidiani locali relative a iniziative didattiche o istituzionali, nonché la pubblicazione sul sito web o sui profili *social* dell'Istituto di **immagini** e **video** degli studenti ripresi nel corso di attività formative e culturali;
2. l'attivazione dei servizi di **didattica a distanza (e-learning)**, incluso l'utilizzo delle piattaforme di **instant messaging**, **videoconferenza**, condivisione di materiali, specie nel caso di datacenter posizionati in Paesi extra UE o con normative sulla protezione dei dati personali non allineate ai principi del GDPR;
3. l'attivazione del **servizio di comunicazione** tramite **sms o e-mail** ai familiari che desiderano ricevere informazioni sullo studente tramite questi media.

COME CHIEDIAMO I SUOI DATI E CON QUALI MEZZI

(Modalità di trattamento)

Trattiamo i Suoi dati personali presso gli uffici dell'Istituto, in formato cartaceo e digitale.

Adottiamo tutte le misure tecniche ed organizzative utili a evitare problemi di accesso non autorizzato, divulgazione, modifica o distruzione. Per alcuni trattamenti usiamo anche il cloud, ma con i datacenter posizionati esclusivamente in Unione Europea. Soltanto il personale autorizzato dal Titolare può accedere per effettuare le operazioni di trattamento o manutenzione dei sistemi.

Non sono utilizzati sistemi di decisione automatica, compresa la **profilazione**.

TRASFERIMENTO DATI

(Comunicazione a terzi e categorie di destinatari)

In alcuni casi i Suoi dati personali possono essere comunicati a professionisti o aziende che svolgono attività per nostro conto, istruite a trattare i dati in massima sicurezza e comunque nominate Responsabili esterni di trattamento. Tra di esse possiamo annoverare il fornitore della piattaforma web del Registro elettronico.

Non è previsto il trasferimento verso Paesi terzi non appartenenti all'Unione Europea.

INFORMATIVA PRIVACY

TEMPO DI CONSERVAZIONE DEI DATI
(Periodo di conservazione)

I Suoi dati personali sono conservati solo per il tempo necessario al perseguimento delle finalità sopra riportate, a meno che la Legge non preveda un periodo di conservazione più lungo.

Le norme nazionali sulla conservazione prevedono che i Suoi dati personali continuino ad essere memorizzati per tutto il tempo necessario al perseguimento delle finalità sopra riportate e per il tempo di conservazione previsto dal Massimario di conservazione e scarto degli archivi scolastici del Ministero dei Beni Culturali

DA CHI RICEVIAMO I SUOI DATI
(Fonte dei dati)

Raccogliamo sempre, laddove possibile, i dati personali dell'interessato a chi ne esercita legalmente la rappresentanza o la responsabilità genitoriale, nel caso di soggetto minore.

Se necessario ai fini del rapporto con l'interessato, richiediamo a enti pubblici o svolgiamo delle ricerche presso registri e/o banche dati pubbliche.

QUALI SONO I SUOI DIRITTI E COME ESERCITARLI
(accesso ai dati, rettifica ed integrazione, cancellazione, portabilità, reclamo)

Può richiedere direttamente al Titolare del trattamento di prendere visione, di correggere, cancellare o limitare i dati che trattiamo e che La riguardano. In alcuni casi, può anche opporsi o revocare il Suo consenso al trattamento; se tecnicamente possibile, ha anche il diritto alla portabilità dei dati e quindi in qualsiasi momento può richiedere una copia digitale degli stessi o il trasferimento automatico tra enti pubblici. Può anche richiedere l'applicazione del diritto all'oblio, ma solo per i trattamenti con richiesta di consenso. Può esercitare i suoi diritti contattando il Titolare o il Responsabile per la Protezione dei Dati oppure può rivolgersi al Garante per la protezione dei dati personali.

PRIVACY E TRASPARENZA NELLA PUBBLICAZIONE DEI DATI

Nell'attuale contesto normativo l' accessibilità viene realizzata attraverso la pubblicazione sul sito web istituzionale della scuola e quindi la circolazione dei dati sulla rete internet. La dimensione digitale della trasparenza espone l'istituto ad elevati rischi di provocare lesioni ai diritti e alle libertà delle persone fisiche come conseguenza alla diffusione non consentita/illecita di dati e informazioni attraverso la rete.

Occorre che tutti gli operatori sappiano effettuare il bilanciamento tra trasparenza da un lato, e protezione dei dati personali dall'altro lato.

PROCEDURA PUBBLICAZIONE DEI DATI

Il documento da pubblicare contiene **DATI PERSONALI** ovvero qualunque informazione relativa a persona fisica identificata o identificabile mediante qualsiasi informazione, ivi compreso un numero di identificazione personale

Se esiste una **NORMA DI LEGGE** che preveda la pubblicazione obbligatoria nel sito istituzionale per **FINALITA' DI TRASPARENZA**, occorre distinguere la natura dei dati personali soggetti a diffusione

DATI COMUNI – nome e cognome, sesso, data e luogo di nascita, indirizzo, codice fiscale

PRINCIPIO DI PERTINENZA E NON ECCEDENZA – i soggetti pubblici non possono rendere intellegibili i dati personali non necessari, eccedenti o non pertinenti con la finalità di pubblicazione

DATI SENSIBILI E GIUDIZIARI – convinzioni religiose e filosofiche, opinioni politiche, stato di salute, vita sessuale, provvedimenti in materia di casellario giudiziale

DIVIETO ASSOLUTO
di pubblicazione per finalità di trasparenza

RELAZIONE ADEGUAMENTO DELL'ISTITUTO AL REGOLAMENTO EUROPEO

1. Premessa
2. Contesto e formazione
3. Piano di adeguamento
4. Mappatura dei processi
5. Analisi di sicurezza dei sistemi
6. Registro dei trattamenti dei dati
7. Vademecum privacy per l'Istituto
8. Gestione Privacy

Relazione finale

9. Documenti allegati:

Allegato A – Relazione sull'analisi di sicurezza dei sistemi

Allegato B – Registro unico delle attività di trattamento

Allegato C – Vademecum privacy per l'Istituto

Allegato D – Modelli di nomina

Allegato E – Istruzioni operative

Allegato F – Informative privacy

Allegato G – Data breach – Violazione dei dati personali

ESEMPIO DI REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

TRATTAMENTO						DATI PERSONALI			INTERESSATI			DESTINATARI		ANALISI DI RISCHIO		MISURE DI PREVENZIONE
n° progr.	Servizio	Descrizione	Tipologia (1-12)	Finalità	Modalità	Categoria	Sensibili (Si/No)	Conservazione	Categoria	Fondamento trattamento	Consenso (Si/No)	Categoria	Trasferimento	Rischi specifici	Livello di rischio	Organizzative Fisiche e Tecniche
3	Amministrazione	Gestione documentazione aggiuntiva	1-2-3-4-5-6-7-9-10-11	Trattamento studenti con disabilità o disturbi di apprendimento	cartacea	1-2-3	Si	Da prevedere	Studenti con stato di salute particolare	Norma di legge	No	No	No	Tutti	medio	**Archiviare la cartella studenti con particolare cura nella protezione dei dati**
4	Amministrazione	Gestione carriera scolastica	1-2-3-4-5-6-7	Gestire i registri elettronici	Telematica, registri elettronici	1-2	Si	Prevista da ARGO	Studenti	Norma di legge	No	Docenti con registro elettronico	Si, su ARGO	Tutti	basso	**Curare i sistemi di autorizzazione sul portale, istruzioni operative ai docenti**
5	Amministrazione	Gestione assenze	1-2-3-4-5-6-7-9-10-11	Gestione assenze	Telematica, registri elettronici	1-2	Si	Prevista da ARGO	Studenti	Regolamento	No	Docenti con registro elettronico	Si, su ARGO	Tutti	basso	**Curare i sistemi di autorizzazione sul portale**

Tipologia di trattamento

1 Raccolta
2 Registrazione
3 Conservazione
4 Estrazione
5 Consultazione
6 Uso
7 Comunicazione
8 Divulgazione
9 Raffronto
10 Limitazioni
11 Cancellazione
12 Distruzione

Categoria di dati

1 Personali
2 Sensibili
3 Salute
4 Giudiziari
5 Biometrici

In un contesto in cui l'innovazione tecnologica rivoluziona i processi formativi – dall'uso del web ai tablet su cui consultare i libri, dai sistemi di messaggistica e i social media al registro elettronico – resta centrale la necessità di riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà e rispetto, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino di oggi e di domani.

SICUREZZA INFORMATICA

La sicurezza informatica ha lo scopo di minimizzare i rischi che incombono sulle informazioni digitali (non solo sui dati personali in essi contenuti) andando a perseguire il raggiungimento di tre obiettivi: la riservatezza, l'integrità e la disponibilità delle informazioni.

Riservatezza

insieme di regole che consentono di mantenere il controllo sull'accesso a determinate informazioni escludendo i soggetti non legittimati

(Autorizzazioni, Password)

Integrità

regole finalizzate a far sì che le informazioni i dati e documenti siano trattati in modo da prevedere, prevenire e ripristinare i sistemi informatici a seguito di eventi accidentali o volontari

(Disaster recovery)

Disponibilità

regole e accorgimenti attraverso i quali mantenere i sistemi informatici e telematici costantemente operativi, affidabili, funzionali e accessibili.

(Gruppi di continuità)

CYBERSECURITY

Consiste nel difendere computer, server, dispositivi mobili, sistemi elettronici, reti e dati dagli attacchi dannosi

La cybersecurity è quindi la prassi di proteggere i sistemi, le reti e i programmi dagli attacchi digitali. Questi attacchi informatici sono solitamente finalizzati all'accesso, alla trasformazione o alla distruzione di informazioni e dati, nonché all'estorsione di denaro agli utenti o all'interruzione dei normali processi aziendali.

L'implementazione di misure di cybersecurity efficaci è particolarmente impegnativa oggi perché ci sono più dispositivi che persone e gli hacker stanno diventando sempre più innovativi.

Mentre La **sicurezza delle informazioni** è un approccio completo alla gestione della sicurezza che coinvolge aspetti umani ed organizzativi, la **cybersecurity** si occupa degli aspetti di sicurezza delle informazioni attuate attraverso l'uso di strumenti tecnologici

Il **cybercrime** (o reato informatico) consiste in una attività criminosa, analoga a quella tradizionale ma caratterizzata dall'abuso di componenti della tecnologia dell'informazione (sia hardware che software).

TIPOLOGIE DI ATTACCHI

Malware è la contrazione di "malicious software" (software malevolo). Il malware, una delle minacce informatiche più comuni, è costituito da software creato da cybercriminali o hacker con lo scopo di danneggiare o provocare il malfunzionamento del computer di un utente legittimo. Spesso diffuso tramite allegati e-mail non richiesti o download apparentemente legittimi, il malware può essere utilizzato dai cybercriminali per ottenere un guadagno economico o sferrare cyberattacchi per fini politici.

Ransomware: malware che blocca l'accesso ai file e ai dati dell'utente, minacciandolo di cancellarli se non paga un riscatto.

Phishing - In un attacco di phishing, i cybercriminali inviano alle vittime e-mail che sembrano provenire da aziende legittime, per richiedere informazioni sensibili. Gli attacchi di phishing hanno solitamente lo scopo di indurre gli utenti a fornire i dati della carta di credito o altre informazioni personali.

Tecniche di Social Engineering- Il social engineering riunisce una serie di tecniche rivolte a spingere le persone a fornire informazioni personali come password o dati bancari o a consentire l'accesso a un computer al fine di installare segretamente software dannosi. I ladri e i truffatori utilizzano il social engineering in quanto è più facile spingere una persona a rivelare le proprie password rispetto all'ottenere tali informazioni mediante tecniche da hacker.

AXIOS - HACKERATO IL REGISTRO ELETTRONICO

Axios Italia, una delle aziende che offrono il servizio di **Registro elettronico** alle scuole italiane, in data 6 aprile 2021 ha subito un attacco hacker con un **ransomware**, cioè un virus che cripta tutti i dati, li blocca e poi chiede un riscatto per sbloccarli

Servizio irraggiungibile, disservizio creato conseguenza di un attacco ransomware portato all'infrastruttura dell'azienda

Chi usa il registro elettronico di Axios potrebbe subire alcune ripercussioni. L'azienda afferma che «*non risultano perdite e/o esfiltrazioni di dati*», quindi nessun dato è stato rubato, ma la cautela in questi casi è sempre la scelta migliore

Il Registro elettronico gestito da Axios è solo uno dei tanti disponibili per le scuole italiane, quindi il problema non coinvolge gran parte degli insegnanti e degli alunni.
Se insegnanti e alunni accedono alla piattaforma Axios tramite nome utente e password, questi dati possono essere criptati dal ransomware.
Se quei dati di accesso sono utilizzati per accedere anche ad altri profili online, allora sono a rischio.
In questi casi è molto importante cambiare subito la password di tutti gli altri account online per i quali si usa la stessa password e, una volta sbloccata la piattaforma, cambiare anche la password per accedere al Registro elettronico.

RISCHI : PHISHING

Poste Italiane: Azione Imminente - Messaggio (HTML)

Messaggio

Da: sicurezza@poste.it [ciente.hqsoY@postepay.it]
A: [redacted]
Cc:
Oggetto: Poste Italiane: Azione Imminente

Inviato: giovedì 24/11/2016 17:35

L'indirizzo email è ingannevole ma non proviene dal dominio reale di Poste Italiane

Posteitaliane PT

Gentile cliente,

Questa e-mail e stata inviata da Poste Italiane per informarvi che non siamo stati in grado di verificare i tuoi identità.

Questo potrebbe essere dovuto a uno dei seguenti motivi:
1. Abbiamo rilevato molti tentativi di accesso non riusciti.
2. Recente cambiamento delle vostre informazioni personali (Telefono, indirizzio).
3. O sei stata vittima di un furto di dati elettronici.

Per assicurarsi che il servizio non venga interrotto chiediamo di confermare e aggiornare i suoi dati.
Per verificare la vostra identitá si prega cliccare sul link qui sotto e eseguire questa procedura online.

https://securelogin.poste.it/jod-fcc/fcc-authentication.html

Il link dirotta su una pagina WEB che non ha nulla a che vedere con il sito ufficiale di Poste Italiane

Grazie per la vostra attenzione rapida in questa materia.

P.IVA 04107060966 - © Poste Italiene 2016

Sono stati inseriti dei FALSI dati identificativi di Poste Italiane per rendere il messaggio più credibile

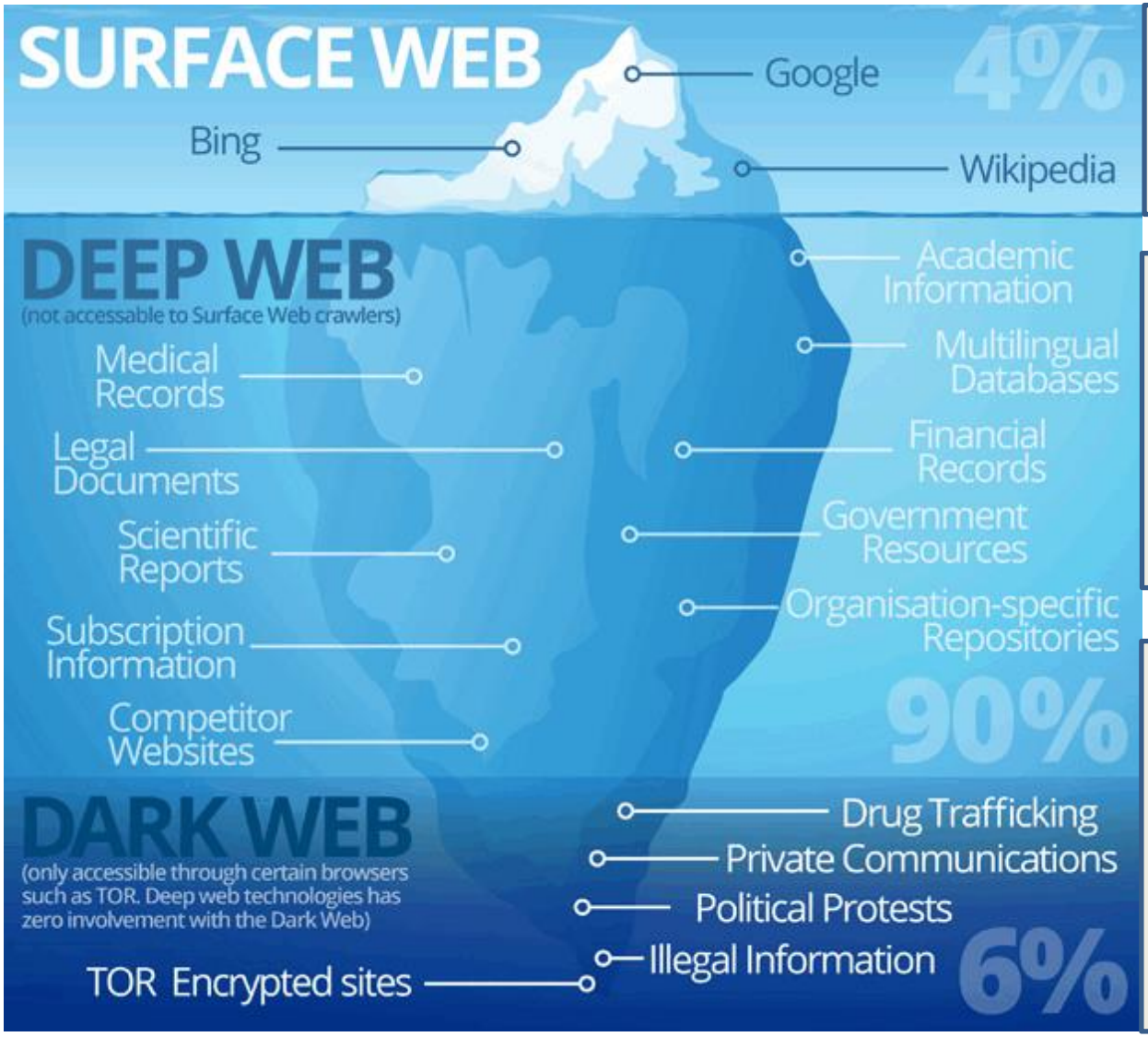
RISCHI : RANSOMWARE

Rischio Ransomware: malware che blocca l'accesso ai file e ai dati dell'utente, minacciandolo di cancellarli se non paga un riscatto.

- **Difficilmente rilevabili dagli antivirus**
- **Rimedio: backup dei dati**
- **Non cliccare su link ed allegati in e mail sospette**

WORLD WIDE WEB

Il WEB è la parte grafica, multimediale, interattiva e ipertestuale di Internet.

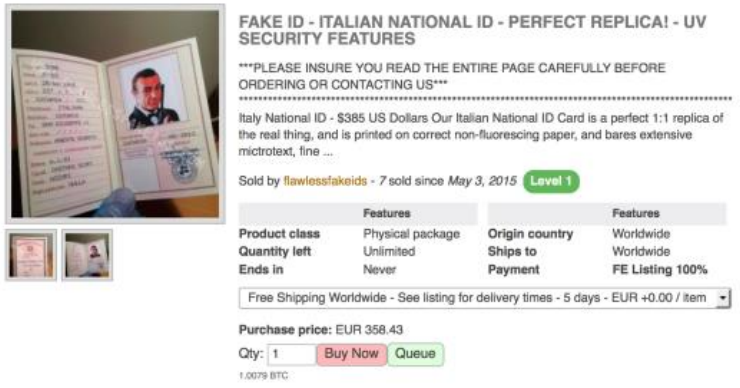


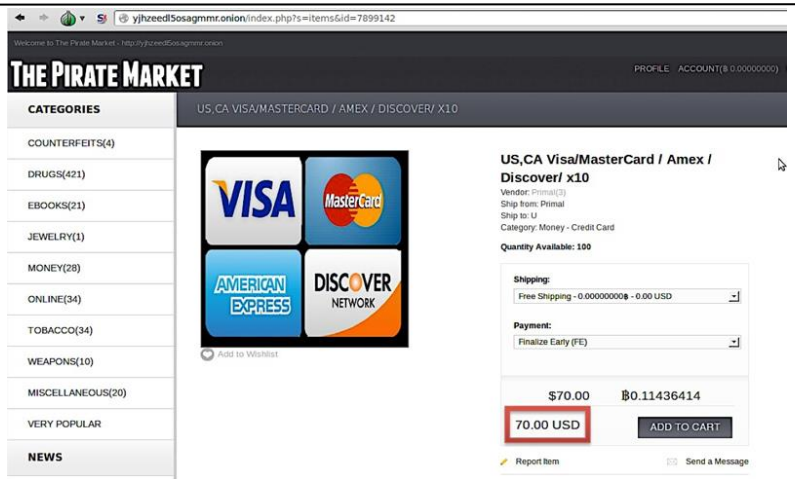
Parte di rete mappata dai motori di ricerca tramite browser

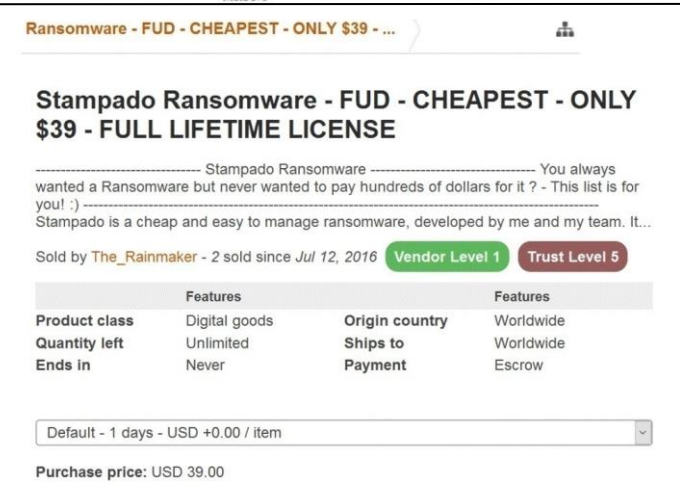
Parte di rete non indicizzata dai motori di ricerca.
Per accedere occorre autenticarsi e fare il login.

Specifici software che consentono agli utenti la navigazione anonima con *Tor* per visitare i domini *.onion*

Dark Web e mercato nero







Rischi sulle credenziali di accesso

- Evitare password ispirate a nome di battesimo, animale, attore o cantante, squadra del cuore;

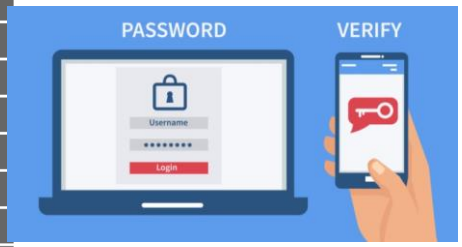
- Mai adoperare credenziali troppo facili, evitare di risultare prevedibili;

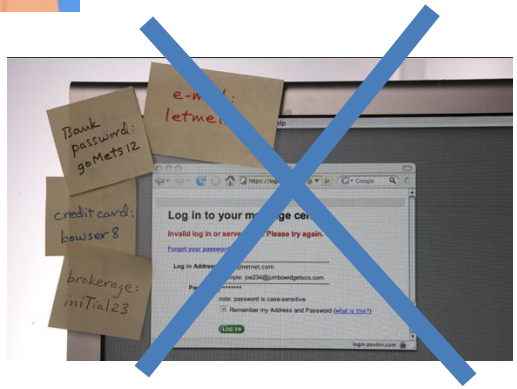
- Password unica e diversa per ogni account e servizio utilizzato;

- Richiedere l'autenticazione a due fattori.

- NO POST-IT

	2007	2017
1	password	123456
2	123456	123456789
3	qwerty	qwerty
4	abc123	12345678
5	letmein	111111
6	monkey	1234567890
7	myspace1	1234567
8	password1	password
9	blink182	123123
10	nome di battesimo	987654321





Gestione strumenti informatici e posta elettronica

Policy di Sicurezza per l'utilizzo degli strumenti di elaborazione dati e della posta elettronica.

- Regolamentare l'uso di internet e dei social network

- Vietare scaricare ed installare software non autorizzato

- Non utilizzare l' e mail per uso personale

- Accertarsi, prima dell'invio di una mail, che l'indirizzo del destinatario sia corretto

RISCHI : FURTO D'IDENTITA'

Il **furto d'identità** consiste nel sostituirsi ad un'altra persona dopo averle carpito alcuni dati, assumendone le sembianze digitali tramite l'uso di informazioni personali.

- Non condividere dati sensibili sui Social
- Non collegarsi a reti Wi-Fi free
- Non inviare documenti a sconosciuti
- Non inviare i codici di accesso
- I criminali possono commettere reati e difficilmente possono essere individuati

RISCHI : PROFILAZIONE

Per **profilazione** si intende il processo di automatizzazione del trattamento dei dati, ossia l'attività di raccolta ed elaborazione dei dati relativi agli utenti di un servizio, al fine di suddividerli in gruppi a seconda delle loro preferenze. Questi gruppi vengono chiamati tecnicamente "**Cluster**".

L'attività di profilazione si compone di:

- Trattamento automatizzato (ricerca su internet)
- Svolgimento su dati personali (preferenze, interessi, ubicazione, spostamenti)
- Finalità valutativa degli aspetti personali di una persona fisica

Ad esempio, siamo in presenza di un'attività di profilazione quando ci viene proposta una **pubblicità comportamentale**, ossia quando viene inserita una locandina pubblicitaria a margine di un sito web relativa ad un servizio che precedentemente avevamo ricercato. Cos'è successo in questo caso? Attraverso un'attività di profilazione, ossia di raccolta automatizzata del dato, è stato rilevato il bisogno espresso di un utente di ottenere un determinato **servizio** e, quindi, il dato è stato elaborato al fine di riproporre tale pubblicità in una successiva ricerca.

Il GDPR indica il **divieto generale** di prendere decisioni che abbiano risvolti giuridici con il sistema di raccolta ed **elaborazione automatizzata dei dati**.

RISCHI : SOCIAL NETWORK

Rischio Social Network

- Proteggere la propria riservatezza ottimizzando le impostazioni privacy;

- Impostare una buona password per accedere ai Social Network;

- Non postare foto ed informazioni troppo personali e/o sensibili;

- Non fare sapere quando sei fuori casa o in vacanza;

- Non compromettere la propria reputazione: fare attenzione a ciò che si pubblica;

- Stare attento alle cose che si condividono, esse non si cancellano.

Social network quando ti connetti, connetti anche la testa! (1)

SANZIONI E CASI DI STUDIO

SANZIONI

Le principali sanzioni alle scuole

Nel 2020, il 50% delle sanzioni comminate alle scuole in Europa riguardava scuole italiane

la maggior parte delle sanzioni. in ambito scolastico riguarda il trattamento dei dati sensibili.

DATO SENSIBILE VS DATO PERSONALE

Dato sensibile vs dato personale

Dati personali

Sono i **dati che permettono l'identificazione, diretta o indiretta, di una persona, ad esempio:** nome, cognome, mail, dati o codici come codice fiscale, indirizzo IP, numero di targa, ecc.

Dati sensibili

I dati particolari (c.d. dati sensibili) permettono di rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

LE SANZIONI PIU' RILEVANTI

Scuola: le sanzioni più rilevanti

Fonte: Euservice

NAZIONE	IMPORTO IN EURO	MOTIVO
Norvegia	170.000	Mancanza di misure di sicurezza idonee a proteggere i device scolastici
Norvegia	120.000	Mancanza di misure di sicurezza idonee nelle app per i messaggi scuola - famiglia
Norvegia	73.600	Trattamento dati sensibili tramite piattaforme DAD non sicure
Svezia	18.630	Utilizzo di riconoscimento facciale sproporzionato rispetto alle finalità
Islanda	9.000	L'insegnate ha inviato una mail ai genitori contenente dati sensibili di altri alunni
Polonia	4.600	Utilizzo di impronta digitale senza idoneo consenso
Italia	4.000	Pubblicazione di graduatorie senza oscurare i dati in eccesso rispetto alle finalità

SITUAZIONI DI RISCHIO

- UTILIZZO DI STESSE PASSWORD PER PIU' SERVIZI
- CREDENZIALI DI ACCESSO A REGISTRO ELETTRONICO
- ACCOUNT PERSONALI IN PC IN DOTAZIONE DELLA SCUOLA
- UTILIZZO CHIAVETTE USB CON DATI IN CHIARO
- DUPLICAZIONE DATI DEL REGISTRO ELETTRONICO
- UTILIZZO DI SISTEMI DI MESSAGISTICA

ESEMPIO : COMUNICAZIONE CON DATI SENSIBILI

L'INVIO DI UNA COMUNICAZIONE CONTENENTE DATI SENSIBILI

- Un docente del Lazio ha inviato a molte persone una mail contenente dati sensibili che era ad uso interno
- Il Garante ha sanzionato e la Pubblica Amministrazione si è rivalsa nei confronti del Dirigente e dei docenti coinvolti nella divulgazione
- La Corte dei Conti ha verificato che vi fossero indicazioni adeguate per il trattamento dei dati
- Mancando istruzioni adeguate, la Corte ha sanzionato solo il Dirigente

PERCHE' NON USARE APP DI MESSAGISTICA?

Es. Telegram, WhatsApp, Signal

PERCHÉ È MEGLIO EVITARE QUESTI SISTEMI?

- Vengono utilizzati con un account personale: la scuola non ha controllo su quello che succede
- In caso di data breach ne risponde direttamente il docente
- Il ruolo del titolare della protezione dati passa al sistema di messaggistica

PERCHE' NON USARE APP DI MESSAGISTICA?

Attenzione, il docente, se invitato, partecipa al gruppo non come docente ma come comune cittadino e non deve fornire dati che ha in virtù del ruolo che ricopre

Problema del controllo

- L'utilizzo di app di messaggistica crea un grosso problema nel rapporto insegnante e genitori
- L'utilizzo di sistemi di messaggistica porta a perdere la formalità
- In una chat utilizziamo un registro linguistico diverso
- I genitori leggono dell'ufficialità anche nelle comunicazioni in chat
- La chat può generare incomprensioni
- I genitori si sentono legittimati ad avere accesso alla vita privata del docente

CASO DI STUDIO – IL REGISTRO ELETTRONICO

CHE COSA È SUCCESSO?

- L'alunno fa una richiesta davanti a tutta la classe, dando informazioni di salute
- L'informazione viene inserita nell'area pubblica del registro

COME SI DIFENDE LA SCUOLA?

- Secondo le difese della scuola, si trattava di un dato noto
- Non è stato divulgato l'effettivo problema medico dello studente
- Il registro elettronico ha un'accessibilità limitata

CASO DI STUDIO – IL REGISTRO ELETTRONICO

MA

Il fatto che il dato sensibile sia stato condiviso solo con i genitori della classe non lo rende conforme alle norme

Il fatto era stato reso noto ai presenti e non ai genitori

COSA AVREBBE DOVUTO FARE LA SCUOLA?

- I dati sensibili non vanno annotati in un'area accessibile a tutti
- La soluzione più conforme era appuntare l'informazione nell'area del registro accessibile a tutti i docenti e ai genitori del ragazzo in questione
- Quanto annotato nel registro elettronico non deve essere reso accessibile a tutti

CASO DI STUDIO – IL REGISTRO ELETTRONICO

IL GARANTE HA DECISO DI NON SANZIONARE LA SCUOLA CHE HA DIMOSTRATO UN COMPORTAMENTO PROATTIVO PER RIMEDIARE ALL'ERRORE

E' POSSIBILE SBAGLIARE, L'IMPORTANTE E' PRENDERE SUBITO PROVVEDIMENTI PER LIMITARE IL DANNO

L'utilizzo del registro elettronico

Provvedimento n. 45 del 5 marzo 2020

Principi ricavabili

I **dati sensibili non vanno annotati sul registro elettronico.** Se ciò fosse estremamente necessario, è opportuno che l'annotazione venga resa visibile solo ai genitori dell'interessato e agli altri docenti della classe; non a tutti i genitori della classe.

Il principio appena espresso vale anche se le persone della classe di fatto **conoscono già l'informazione** sensibile che si sta annotando.

Il **comportamento proattivo** volto a eliminare gli effetti della condotta illecita, è idoneo a incidere sulla natura e sulla quantificazione della sanzione.

In un contesto in cui l'innovazione tecnologica rivoluziona i processi formativi – dall'uso del web ai tablet su cui consultare i libri, dai sistemi di messaggistica e i social media al registro elettronico – resta centrale la necessità di riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà e rispetto, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino di oggi e di domani.

REGOLE GENERALI

VITA DELLO STUDENTE

MONDO CONNESSO E NUOVE TECNOLOGIE

PUBBLICAZIONE ONLINE

VIDEOSORVEGLIANZA E ALTRI CASI

REGOLE GENERALI

PRIMA DI TUTTO... TRASPARENZA!

Tutte le scuole hanno l'obbligo di far conoscere agli "interessati" (studenti, famiglie, docenti e altro personale) come vengono trattati i loro dati personali.

Il linguaggio dell'informativa deve essere facilmente comprensibile anche dai minori e deve contenere, in particolare, gli elementi essenziali del trattamento, specificando che le finalità perseguite sono limitate esclusivamente al perseguimento delle funzioni istituzionali necessarie per assicurare il diritto all'istruzione e alla formazione attraverso l'erogazione dell'attività didattica.

TRATTAMENTO DEI DATI NELLE ISTITUZIONI SCOLASTICHE

Il Regolamento e il Codice non prevedono un regime differenziato basato sulla natura pubblica o privata della scuola che tratta i dati per finalità di istruzione e formazione, rilascio di titoli di studio aventi valore legale, o connessi allo svolgimento di attività comunque soggette alla vigilanza del Ministero.

Pertanto tutte le scuole possono trattare i dati personali degli studenti, anche relativi a categorie particolari, funzionali all'attività didattica e formativa, per il perseguimento di specifiche finalità istituzionali quando espressamente previsto dalla normativa di settore. Basi giuridiche quali, il consenso e/o il contratto, possono trovare invece applicazione per attività, non strettamente connesse a quelle didattiche o non previste dall'ordinamento scolastico se poste in essere da scuole private (ad es. per l'erogazione di corsi di musica, lezioni di lingua straniera o attività sportive, teatrali non previste dal curricolo scolastico).

Il GDPR impone la nomina del "Data Protection Officer" o "DPO" a tutti gli organismi pubblici, comprese le scuole. Gli istituti scolastici che trattano i dati personali degli interessati (alunni, genitori, docenti, personale ATA e altri) **esclusivamente** per finalità istituzionali, secondo le regole del GDPR, non devono richiedere il consenso

CHI TRATTA I DATI A SCUOLA?

All'interno della scuola, titolare del trattamento, il dirigente scolastico, in quanto legale rappresentante, prende decisioni sulle attività di trattamento da intraprendere e sulle modalità attraverso cui queste verranno svolte mediante il personale amministrativo e/o docente.
Tale personale è quindi autorizzato a trattare i dati nell'ambito delle attività didattiche o amministrative.

Soggetti:

Titolare (accountability)

Responsabile del trattamento

Personale autorizzato al trattamento

CATEGORIE PARTICOLARI DI DATI RELATIVI AD ALUNNI
ALCUNI ESEMPI CONCRETI

Origini razziali ed etniche
I dati che rilevino le origini razziali ed etniche possono essere trattati dalla scuola per favorire l'integrazione degli alunni stranieri. Tali informazioni possono essere in alcuni casi desumibili anche dai nominativi o dai dati anagrafici degli alunni.

Convinzioni religiose
Gli istituti scolastici possono utilizzare ***i dati che rivelino le convinzioni religiose*** al fine di garantire la libertà di culto e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento.

Stato di salute
I dati relativi alla salute possono essere trattati per l'adozione di specifiche misure di sostegno o strumenti di ausilio per gli alunni con disabilità, con disturbi specifici di apprendimento o con Bisogni Educativi Speciali; per la gestione delle assenze per malattia; per l'insegnamento domiciliare e ospedaliero a favore degli alunni affetti da gravi patologie; per la partecipazione alle attività sportive, alle visite guidate e ai viaggi di istruzione; in presenza di un regime alimentare differenziato dovuto a intolleranze, allergie o specifiche patologie.

Dati personali relativi a condanne penali e reati
I dati personali relativi a condanne penali e reati possono essere trattati per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione o di protezione, come i testimoni di giustizia.

Secondo il GDPR il trattamento di categorie particolari di dati personali è vietato. Per gli istituti scolastici il trattamento è previsto in casi particolari, con le relative cautele imposte dal GDPR.

Opinioni politiche
Le opinioni politiche possono essere trattate dalla scuola esclusivamente per garantire la costituzione e il funzionamento degli organismi di rappresentanza: ad es., le consulte e le associazioni degli studenti e dei genitori.

IL RAPPORTO DI LAVORO

Dirigenti, docenti e personale ATA sono anche soggetti interessati in quanto lavoratori cui si riferiscono i dati personali, anche relativi a categorie particolari.

La scuola tratta tali dati per la gestione del rapporto di lavoro nel rispetto delle norme di settore che regolano, ad es., le procedure di assunzione, l'adempimento degli obblighi di legge (quali gli specifici obblighi di comunicazione alle autorità previdenziali o assicurative), la gestione delle assenze, i procedimenti disciplinari, i procedimenti valutativi, gli adempimenti in materia di salute e sicurezza nei luoghi di lavoro e quelli necessari alla cessazione del rapporto.

La scuola infatti – quando agisce come datore di lavoro – tratta i dati nel rispetto delle norme di settore e per adempiere a obblighi o compiti previsti dalla legge, non potendo invece il consenso del lavoratore costituire, di regola, un valido presupposto su cui fondare il trattamento. Ciò considerato lo squilibrio tra le parti del rapporto.

Specifiche garanzie e misure a tutela della riservatezza e della libertà dei lavoratori sono state stabilite dal Garante in relazione ai trattamenti delle categorie particolari di dati nel contesto lavorativo.

Tali dati sono infatti particolarmente delicati e possono comportare il rischio di conseguenze discriminatorie. Pertanto solo in casi tassativi e in presenza di particolari cautele il datore di lavoro può trattare informazioni relative ad es., alle convinzioni religiose o all'adesione a sindacati (vedi: Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1, del d.lgs 10 agosto 2018, n. 101, doc web n. 9124510, in appendice).

Come per tutti gli altri ambiti lavorativi, sono vietate, a tutela della sfera privata del dipendente, indagini o trattamenti di dati personali che non siano pertinenti rispetto alla mansione e all'attività lavorativa svolta (art. 113 del Codice).

I dati personali trattati dalla Scuola riguardano anche i dirigente, i docenti e il personale ATA.

Anche per questa categoria di interessati occorre seguire il GDPR per la gestione del rapporto di lavoro in tutte le fasi

NO ALLE COMUNICAZIONI DI DATI A TERZI E ALLA CIRCOLAZIONE DI INFORMAZIONI TRA COLLEGHI

Nel trattare i dati dei lavoratori la scuola deve **adottare misure tecniche e organizzative per prevenire la conoscibilità ingiustificata di dati personali dei propri dipendenti da parte di soggetti terzi** (famiglie, studenti, OO.SS., altri soggetti), al fine di evitare la comunicazione illecita di informazioni personali (ad es., riguardanti informazioni particolarmente delicate come lo stato di salute del lavoratore o l'assunzione di provvedimenti di carattere disciplinare o valutativo).

La scuola deve anche **evitare la circolazione nell'ambiente di lavoro di dati personali riferiti ai docenti o al personale amministrativo** in favore di altri dipendenti che non siano specificamente autorizzati (questi principi sono stati stabiliti, fin dal 2007, nelle "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico", del 14 giugno 2007, doc. web n. 1417809, vedi appendice).

La scuola deve prestare attenzione, anche in occasione della predisposizione dell'orario delle lezioni, a non rendere reciprocamente note a tutti i colleghi informazioni relative alle specifiche causali di assenza dal servizio, anche attraverso acronimi o sigle.

Ciò soprattutto quando dalle stesse sia possibile evincere categorie particolari di dati personali (es. permessi sindacali o dati sanitari).

Nel trattare i dati dei lavoratori la scuola deve adottare misure tecniche ed organizzative idonee pe assicurare la riservatezza dei dati da parte di soggetti terzi, ma anche da parte del personale non specificatamente autorizzato al trattamento dei dati personali di questa categoria di interessati

DIRITTO DI ACCESSO

Anche in ambito scolastico, ogni persona ha diritto di conoscere se sono conservate informazioni che la riguardano, di apprenderne il contenuto, di farle rettificare se erronee, incomplete o non aggiornate, cancellare o di opporsi al loro trattamento.

Per esercitare questi diritti è possibile rivolgersi al "titolare del trattamento" (in genere l'istituto scolastico di riferimento) anche per il tramite del Responsabile della Protezione dei Dati (RPD).

In tale caso il genitore, o l'alunno se maggiorenne, può formulare una specifica istanza per l'esercizio dei diritti utilizzando il modello disponibile sul sito web del Garante, www.gpdp.it, nella sezione "I miei diritti" (doc. web n. 1089924 e doc. web n. 9038275).

Se non si ottiene risposta, o se il riscontro non risulta adeguato, è possibile rivolgersi al Garante o alla magistratura ordinaria.

Diverso è il caso dell'accesso agli atti amministrativi che, infatti, non è regolato dal Codice privacy, né vigilato dal Garante per la protezione dei dati personali. Come indicato nella legge n. 241 del 1990 (e successive modifiche), spetta alla singola amministrazione (ad es. alla scuola) valutare se esistono i presupposti normativi che permettono di prendere visione e di estrarre copia di documenti amministrativi ai soggetti con un "interesse diretto, concreto e attuale" alla conoscibilità degli atti.

L'ulteriore diritto di chiunque di accedere a dati e documenti detenuti dalle pubbliche amministrazioni, anche ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del decreto 33/2013 **(accesso civico e accesso civico generalizzato)** – per favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche – è consentito nelle forme e nei limiti di cui al d.lgs. n. 33 del 2013, come modificato dal d.lgs. n.97 del 2016.

La **richiesta di accesso ai dati** è uno dei diritti dell'interessato ai sensi del Regolamento Europeo sulla Protezione dei Dati

Il **diritto di accesso agli atti amministrativi** è regolamentato dal «Decreto Trasparenza» – d.lgs.33/2013

DIRITTI DELL'INTERESSATO AI SENSI DEL RGPD

chiedere al titolare **l'accesso ai dati** che li riguardano

revocare il consenso prestato in qualsiasi momento

ottenere, per i dati che lo riguardano, **la rettifica, l'integrazione** dei dati incompleti**, la limitazione** del trattamento

proporre reclamo all'Autorità

ricevere i dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico **("diritto alla portabilità")**

ottenere la **cancellazione** dei dati personali che lo riguardano **("diritto all'oblio")**

TUTELA DINANZI AL GARANTE

In caso di violazione della normativa in materia di protezione dei dati personali – come ad es. quando si verifica una diffusione sul sito internet della scuola dei dati personali in assenza di una idonea base giuridica – oppure in caso di trattamento dei dati senza aver ricevuto adeguate informazioni, la persona interessata (studente, famiglia, docente, altro personale) può rivolgersi al Garante **presentando un reclamo**.

Il reclamo può essere presentato **solo** dall'interessato e contiene un'indicazione dettagliata dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste, gli estremi identificativi del titolare o del responsabile del trattamento.

In alternativa, la persona interessata può rivolgersi all'autorità giudiziaria ordinaria.

Chiunque abbia conoscenza di una possibile violazione del Regolamento o del Codice può invece presentare una **segnalazione** per sollecitare un controllo da parte del Garante, che però non comporta necessariamente l'adozione di un provvedimento nei confronti del titolare del trattamento.

Il **diritto di proporre reclamo** è uno dei diritti dell'interessato ai sensi del Regolamento Europeo sulla Protezione dei Dati

VITA DELLO STUDENTE

ISCRIZIONE A SCUOLE E ASILI

Tutti gli istituti di ogni ordine e grado ma anche gli enti locali eventualmente competenti devono prestare particolare attenzione alle **informazioni che richiedono ai fini dell'iscrizione scolastica** (effettuata, ad es., attraverso il sistema di iscrizioni online predisposto dal Ministero oppure attraverso moduli cartacei).

Le istituzioni scolastiche che intendono integrare e adeguare il modulo di iscrizione per offrire agli alunni ulteriori servizi in base al proprio Piano triennale dell'offerta formativa e alle risorse disponibili **non** possono richiedere informazioni personali non pertinenti rispetto alla finalità di iscrizione (ad es. lo stato di salute dei nonni o la professione dei genitori).

Particolare attenzione deve essere prestata inoltre all'eventuale raccolta delle **categorie particolari di dati personali**. Il trattamento di questi dati, oltre a dover essere espressamente previsto dalla normativa di settore, richiede infatti specifiche garanzie a tutela dei diritti degli interessati e della integrità e riservatezza dei dati *(vedi nota del Ministero dell'Istruzione e del merito del 30 novembre 2022, in appendice)*.

Procedura di iscrizione scolastica on line o attraverso moduli cartacei oggetto di analisi nel Registro dei trattamenti. Informazioni richieste standardizzate, moduli precompilati, informativa disponibile.

TEMI E VITA DI CLASSE

Non lede la privacy l'insegnante che assegna ai propri alunni lo svolgimento di **temi in classe** riguardanti il loro mondo personale o familiare. Nel momento in cui gli elaborati vengono letti in classe – specialmente se riguardano argomenti delicati – è affidata alla sensibilità di ciascun insegnante la capacità di trovare il giusto equilibrio tra le esigenze didattiche e la tutela dei dati personali.

Restano comunque validi gli obblighi di riservatezza già previsti per il corpo docente riguardo al segreto d'ufficio e professionale, nonché quelli relativi alla **conservazione** dei dati personali eventualmente contenuti nei temi degli alunni.

In generale, nelle varie iniziative didattiche, considerata la particolare interazione che caratterizza la relazione e il dialogo educativo tra docente e alunni occorre sempre tenere in considerazione l'interesse primario del minore e le eventuali conseguenze, anche sul piano relazionale, che potrebbero derivare dalla conoscibilità/circolazione di informazioni personali o vicende familiari dell'alunno all'interno della classe o della comunità scolastica.

La tutela dei dati personali degli alunni all'interno della classe è affidata all'insegnante che deve sempre tenere in considerazione l'interesse primario del minore.

In caso di temi di classe su argomenti delicati deve essere prevista una procedura di conservazione idonea per evitare casi di violazione.

VOTI ED ESAMI

Le informazioni sul rendimento scolastico e sulla pubblicazione dell'esito degli esami sono soggette ad un regime di conoscibilità stabilito dalla normativa di settore e dal Ministero.

Salvo lo specifico regime di pubblicità relativo agli esiti degli esami di Stato, non è ammessa la pubblicazione online degli esiti degli scrutini (vedi appendice, doc. web n. 9367295).

La pubblicazione dei voti online costituisce una forma di diffusione di dati particolarmente invasiva e non conforme all'attuale quadro normativo in materia di protezione dei dati. Una volta pubblicati, infatti, i voti rischiano di rimanere in rete per un tempo indefinito e possono essere utilizzati da soggetti estranei alla comunità scolastica, determinando un'ingiustificata violazione del diritto alla riservatezza degli studenti che sono in gran parte minori, con possibili ripercussioni anche sullo sviluppo della loro personalità.

Pertanto gli esiti degli scrutini delle classi intermedie delle scuole secondarie di primo e di secondo grado e di ammissione agli esami di Stato del secondo ciclo di istruzione vanno resi disponibili, con la sola indicazione "ammesso" e "non ammesso" alla classe successiva, (ivi compresi, per le classi finali, i crediti scolastici attribuiti ai candidati) nell'area riservata del registro elettronico cui possono accedere solo gli studenti della classe di riferimento.

I voti riportati nelle singole discipline dall'alunno, invece, sono riportati nell'area riservata del registro elettronico a cui può accedere esclusivamente, con le proprie credenziali il singolo studente o la propria famiglia.

Qualora, invece, l'istituzione scolastica sia sprovvista di registro elettronico è consentita l'affissione dei tabelloni, evitando di fornire, anche indirettamente, informazioni sulle condizioni di salute degli studenti, o altri dati personali non pertinenti.

Il riferimento alle "prove differenziate" sostenute dagli studenti portatori di handicap o con disturbi specifici di apprendimento (DSA), ad esempio, non va inserito nei tabelloni, ma deve essere indicato solamente nell'attestazione da rilasciare allo studente.

Non è ammessa la pubblicazione on line dell'esito degli scrutini (Registro elettronico)

I voti nelle singole discipline sono riportati nell'area riservata del Registro elettronico

COMUNICAZIONI SCOLASTICHE

Il diritto–dovere di informare le famiglie sull'attività e sugli avvenimenti della vita scolastica deve essere sempre **bilanciato** con l'esigenza di tutelare la personalità dei minori. È quindi necessario evitare di inserire, nelle **circolari** e nelle **comunicazioni scolastiche** non rivolte a specifici destinatari, dati personali che rendano identificabili, ad es., gli alunni coinvolti in casi di bullismo o destinatari di provvedimenti disciplinari o interessati in altre vicende particolarmente delicate.

Comunicazioni scolastiche non devono contenere dati personali.

DISABILITÀ E DISTURBI SPECIFICI DELL'APPRENDIMENTO

Le istituzioni scolastiche devono prestare particolare attenzione a non diffondere, anche per mero errore materiale, dati relativi alla salute. **Non** è consentito, ad es., pubblicare online una **circolare contenente i nomi degli studenti con disabilità**. Occorre fare attenzione anche a chi ha accesso ai dati degli allievi con disabilità o disturbi specifici dell'apprendimento (DSA), limitandone la conoscenza ai soli soggetti a ciò legittimati dalla normativa scolastica e da quella specifica di settore, come ad es. i docenti, i genitori e gli operatori sanitari che congiuntamente devono predisporre il piano educativo individualizzato.

Particolare attenzione al trattamento dei dati degli allievi con disabilità e disturbi specifici dell'apprendimento (DSA).

GESTIONE DEL SERVIZIO MENSA

Gli enti locali che offrono il servizio mensa possono trattare **i dati particolari degli alunni indispensabili per la fornitura di pasti** nel caso in cui debbano rispondere a particolari richieste delle famiglie legate, ad es., a determinati precetti religiosi o a specifiche condizioni di salute. Alcune particolari scelte, infatti (pasti vegetariani o rispondenti a determinati dettami religiosi) possono essere idonee a rivelare le convinzioni (religiose, filosofiche o di altro genere) dei genitori e degli alunni.

Nel caso di gestione del servizio mensa generalmente il Comune è titolare del trattamento, la cooperativa responsabile esterno di trattamento nominato con personale autorizzato al trattamento, il docente è informato della particolare richiesta ai fini di controllo

DALLA SCUOLA AL LAVORO

Su richiesta degli studenti interessati, le istituzioni del sistema nazionale di istruzione, i centri di formazione professionale regionale, le scuole private non paritarie, le istituzioni di alta formazione artistica e coreutica e le università statali e non, **possono** comunicare o diffondere, anche a privati e per via telematica, **i dati relativi agli esiti formativi, intermedi e finali e altri dati personali** (ad esclusione delle particolari categorie di dati e dei dati relativi a condanne penali) al fine di agevolare l'orientamento, la formazione e l'inserimento professionale anche all'estero. **Prima** di adempiere alla richiesta, gli istituti scolastici devono comunque provvedere a **informare gli studenti su quali dati saranno utilizzati per tali finalità**.

D. Lgs. 101/2018
Trattamento di dati relativi a studenti.
Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, le scuole, su richiesta degli interessati, possono comunicare o diffondere, anche dati relativi agli esiti formativi.

MONDO CONNESSO E NUOVE TECNOLOGIE

CYBERBULLISMO E ALTRI FENOMENI DI RISCHIO

Gli studenti, anche i più giovani, rappresentano spesso l'avanguardia tecnologica all'interno della scuola, grazie alla loro capacità di utilizzare le opportunità offerte da smartphone, tablet e altri strumenti che consentono la connessione costante in rete. Tuttavia alla capacità tecnologica non corrisponde spesso eguale maturità nel comprendere la necessità di difendere i propri diritti e quelli di altre persone, a partire dagli stessi compagni di studio.

I giovani devono essere consapevoli che le proprie azioni in rete possono produrre effetti negativi anche nella vita reale e per un tempo indefinito. Troppi ragazzi, insultati, discriminati, vittime di cyberbulli, soffrono, possono essere costretti a cambiare scuola o, nei casi più tragici, arrivare al suicidio. È quindi estremamente importante prestare attenzione in caso si notino comportamenti anomali e fastidiosi su un social network, su sistemi di messaggistica istantanea (come Whatsapp, Snapchat, Skype, Messenger, etc.) o su siti che garantiscono comunicazioni anonime.

Se si è vittime di commenti odiosi, di **cyberbullismo** *(vedi al riguardo: www.gpdp.it/cyberbullismo)*, di **sexting**, di **revenge porn** *(vedi al riguardo: www.gpdp.it/revengeporn)* o di altre ingerenze nella propria vita privata, non bisogna aspettare che la situazione degeneri ulteriormente.

Occorre avvisare subito i compagni, i professori, le famiglie se ci si rende conto che qualcuno è insultato o messo sotto pressione da compagni o da sconosciuti.

Si può chiedere al gestore del social network di intervenire contro eventuali abusi o di cancellare testi e immagini inappropriate. In caso di violazioni, è bene segnalare immediatamente il problema all'istituzione scolastica (in cui, di regola, è presente un referente per il cyberbullismo), al Garante della privacy e alle altre autorità competenti.

Cyberbullismo - come proteggersi:

- Utilizzare delle password sicure e non rivelarle a nessuno.
- Proteggere la propria sfera privata. Non divulgare dati e informazioni sensibili.
- Sui social media accettare come amici soltanto le persone che si conoscono veramente.
- Non postare foto o filmati imbarazzati.
- Vietato il sexting (scambio di testi e/o immagini sessualmente espliciti in rete).
- I genitori devono parlare apertamente con i propri figli sulle modalità di utilizzo dei nuovi media.

SMARTPHONE E TABLET

L'utilizzo di telefoni cellulari, di apparecchi per la registrazione di audio e immagini è in genere consentito, ma esclusivamente per fini personali, e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte, siano essi studenti, docenti o altro personale.

Le istituzioni scolastiche hanno, comunque, la possibilità di regolare o di inibire l'utilizzo di registratori, smartphone, tablet e altri dispositivi elettronici all'interno delle aule o nelle scuole stesse.

Gli studenti e gli altri membri della comunità scolastica, in ogni caso, non possono diffondere audio, foto, video (ad es. pubblicandoli su Internet) senza avere prima informato adeguatamente e aver ottenuto l'esplicito consenso delle persone coinvolte.

Si deve quindi prestare particolare attenzione prima di caricare immagini e video su blog o social network, o di diffonderle attraverso mms o sistemi di messaggistica istantanea. Succede spesso, tra l'altro, che una fotografia inviata a un amico o a un familiare venga poi inoltrata ad altri destinatari, generando involontariamente una comunicazione a catena dei dati personali raccolti.

Tale pratica può dar luogo a gravi violazioni del diritto alla riservatezza delle persone riprese, e fare incorrere in sanzioni disciplinari, pecuniarie e in eventuali reati *(vedi sul punto i documenti di indirizzo riportati nella pagina informativa del Garante su minori, nuove tecnologie e protezione dei dati, all'indirizzo: www.gpdp.it/minori).*

E' in vigore **il divieto** di utilizzare il cellulare durante le lezioni, trattandosi di un elemento di distrazione propria e altrui e di una mancanza di rispetto verso i docenti, anche se può essere ammesso con il controllo dell'insegnante per usi scolastici. In tal caso gli studenti possono creare delle mappe oppure realizzare dei progetti in modo più semplice e veloce rispetto a quello tradizionale.

Anche l'insegnante può trarne vantaggio, facendo sviluppare agli studenti dei test e delle prove intercorso sicuramente più stimolanti e innovative.

In ogni caso è vietato diffondere audio, foto e video senza il consenso a scuola come fuori da scuola.

SHARENTING

I genitori devono prestare particolare attenzione se intendono condividere online contenuti che riguardano i propri figli (foto, video, ecografie, storie).

Postare foto e video di diversi momenti della vita dei minori, magari accompagnati da informazioni tra cui l'indicazione del nome o dell'età o il luogo in cui è stato ripreso, contribuisce a definire l'immagine e la reputazione online.

Ciò che viene pubblicato online o condiviso nelle chat di messaggistica rischia di non essere più nel nostro controllo e questo vale maggiormente nel caso dei minori.

I minori, inoltre, potrebbero non essere contenti di ritrovare loro immagini a disposizione di tutti o non essere d'accordo con l'immagine di sé stessi che si sta costruendo.

Se proprio si decide di pubblicare immagini dei propri figli, è importante provare almeno a seguire alcune accortezze, come:

- rendere irriconoscibile il viso del minore o coprirlo con una "faccina" emoticon;
- limitare le impostazioni di visibilità delle immagini sui social network;
- evitare la creazione di un account social dedicato al minore;
- leggere e comprendere le informative sulla privacy dei social network su cui carichiamo le fotografie.

DIDATTICA A DISTANZA

Le scuole che utilizzano sistemi di didattica a distanza nell'ambito delle proprie finalità istituzionali **non** devono chiedere il **consenso** al trattamento dei dati di studenti, genitori e docenti.

Le scuole sono però tenute ad **assicurare la trasparenza del trattamento** informando, con un linguaggio facilmente comprensibile anche dai minori, gli interessati (studenti, genitori e docenti) in merito, in particolare, alle caratteristiche essenziali del trattamento che viene effettuato specificando che le finalità perseguite sono limitate esclusivamente all'erogazione della didattica a distanza, sulla base dei medesimi presupposti e con garanzie analoghe a quelle della didattica tradizionale.

Se la piattaforma prescelta per l'erogazione dell'attività didattica a distanza comporta il trattamento di dati personali di studenti, genitori, docenti o altro personale scolastico per conto della scuola, il rapporto con il fornitore dovrà essere regolato con contratto o altro atto giuridico e le istituzioni scolastiche dovranno assicurarsi che i dati trattati per loro conto siano utilizzati solo per finalità didattiche.

Particolare attenzione dovrà essere prestata alle questioni inerenti la sicurezza e la protezione dei dati affidati a tali piattaforme *(per un approfondimento su tali tematiche Provvedimento del 26 marzo 2020 - "Didattica a distanza: prime indicazioni" doc. web 9300784, in appendice)*.

Rapporto con il fornitore prevede la nomina di responsabile esterno di trattamento.

Se data center posizionati extra UE richiesto il consenso

(vedi informativa)

IMMAGINI DI RECITE E GITE SCOLASTICHE

Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione.

Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su Internet e sui social network.

In tali casi la diffusione di immagini dei minori richiede, di regola, il consenso informato degli esercenti la responsabilità genitoriale e delle altre persone presenti nelle fotografie e nei video.

REGISTRAZIONE DELLA LEZIONE E STRUMENTI COMPENSATIVI E DISPENSATIVI

È possibile registrare la lezione esclusivamente per scopi personali, ad es. per motivi di studio individuale, compatibilmente con le specifiche disposizioni scolastiche al riguardo. Per ogni altro utilizzo o eventuale diffusione, anche su Internet, è necessario prima informare adeguatamente le persone coinvolte nella registrazione (docenti, famiglie, studenti, altro personale) e ottenere il loro consenso.

E’ richiesto il consenso per la pubblicazione sul sito istituzionale di immagini e video per attività formative e culturali (informativa).

Altrimenti è vietato diffondere audio, foto e video senza il consenso a scuola come fuori da scuola.

REGISTRAZIONE DELLA LEZIONE E STRUMENTI COMPENSATIVI E DISPENSATIVI

È possibile registrare la lezione esclusivamente per scopi personali, ad es. per motivi di studio individuale, compatibilmente con le specifiche disposizioni scolastiche al riguardo. Per ogni altro utilizzo o eventuale diffusione, anche su Internet, è necessario prima informare adeguatamente le persone coinvolte nella registrazione (docenti, famiglie, studenti, altro personale) e ottenere il loro consenso.

Non è invece ammessa la videoregistrazione della lezione in cui si manifestano le dinamiche di classe, neanche qualora si utilizzino piattaforme per la didattica a distanza. L'utilizzo delle piattaforme deve essere, infatti, funzionale a ricreare lo "spazio virtuale" in cui si esplica la relazione e l'interazione tra il docente e gli studenti, non diversamente da quanto accade nelle lezioni in presenza.

Nell'ambito dell'autonomia scolastica, **gli istituti possono decidere di regolamentare diversamente o anche di inibire l'utilizzo di telefonini e altri strumenti che siano in grado di registrare immagini e voci**.

In ogni caso deve essere sempre **garantito** il diritto degli studenti con DSA (disturbi specifici dell'apprendimento), o altre specifiche patologie, di utilizzare strumenti di ausilio per una maggiore flessibilità didattica (come il registratore, il computer, il tablet, lo smartphone, etc.) di volta in volta previsti nei piani didattici personalizzati che li riguardano.

REGISTRO ELETTRONICO

L'impiego del registro elettronico è previsto da specifiche disposizioni normative.

Il rapporto con il fornitore del servizio che comporta anche il trattamento di dati personali di studenti, famiglie, docenti e altro personale, deve essere disciplinato anche al fine di impartire al fornitore, in qualità di responsabile del trattamento, le necessarie istruzioni.

Il personale amministrativo e i docenti, in quanto personale autorizzato a trattare i dati personali per conto della scuola, devono essere istruiti anche in merito alle specifiche funzionalità del registro elettronico, al fine di prevenire che, ad es., informazioni relative a singoli studenti o docenti siano messe a disposizione di terzi o altro personale non autorizzato.

Le funzionalità del registro elettronico, adeguatamente configurate, possono consentire la condivisione di materiali didattici, la realizzazione e consultazione di webinar o videolezioni e il dialogo in modo "social" tra docenti, studenti e famiglie, limitando il ricorso a piattaforme che offrono anche molteplici ulteriori servizi, non sempre specificamente rivolti alla didattica *(sul punto vedi doc. web 9334326 e 9300784, in appendice)*.

Al fine di garantire la massima consapevolezza nell'utilizzo degli strumenti tecnologici – delle cui implicazioni non tutti gli studenti (soprattutto se minorenni) hanno piena cognizione – sarebbero auspicabili, in ogni caso, iniziative di sensibilizzazione in tal senso, rivolte a famiglie e ragazzi.

Rapporto con il fornitore prevede la nomina di responsabile esterno di trattamento.

Personale amministrativo e docenti istruiti in merito alle funzionalità del registro elettronico con specifiche istruzioni operative.

PUBBLICAZIONE ONLINE

PUBBLICITÀ E TRASPARENZA

Le scuole di ogni ordine e grado sono tenute ad effettuare una serie di adempimenti previsti dalle disposizioni normative in materia di pubblicità e trasparenza della pubblica amministrazione. È però necessario che gli istituti scolastici prestino particolare attenzione a non rendere accessibili informazioni che dovrebbero restare riservate o a mantenerle online oltre il tempo consentito, mettendo in questo modo a rischio la privacy e la dignità delle persone a causa di un'errata interpretazione della normativa o per semplice distrazione.

In particolare, allo scopo di facilitare la corretta applicazione della normativa in materia di pubblicità e trasparenza della pubblica amministrazione, il **Garante fin dal 2014 ha fornito indicazioni e chiarimenti con le "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati"** (attualmente in corso di aggiornamento).

La pubblicazione su Internet di atti o documenti che riportano informazioni personali (graduatorie, circolari, determinazioni) deve avvenire nel rispetto dei principi generali di protezione dei dati, avendo riguardo anzitutto alla sussistenza di idonei presupposti di liceità della diffusione online dei dati personali, verificando altresì che i dati oggetto di pubblicazione siano "adeguati, pertinenti e limitati" rispetto alle finalità istituzionali perseguite.

Diversamente, tale diffusione può arrecare un pregiudizio alla riservatezza individuale (specie nei confronti di persone vulnerabili, come minori o lavoratori).

Per i documenti non liberamente disponibili online, restano comunque valide le norme che regolano presupposti, limiti e condizioni per l'accesso *(cfr., legge n. 241 del 1990 e dal d.lgs. n. 33 del 2013)*.

PROCEDURA PUBBLICAZIONE DEI DATI

Il documento da pubblicare contiene **DATI PERSONALI** ovvero qualunque informazione relativa a persona fisica identificata o identificabile mediante qualsiasi informazione, ivi compreso un numero di identificazione personale

Se esiste una **NORMA DI LEGGE** che preveda la pubblicazione obbligatoria nel sito istituzionale per **FINALITA' DI TRASPARENZA**, occorre distinguere la natura dei dati personali soggetti a diffusione

DATI COMUNI – nome e cognome, sesso, data e luogo di nascita, indirizzo, codice fiscale

PRINCIPIO DI PERTINENZA E NON ECCEDENZA – i soggetti pubblici non possono rendere intellegibili i dati personali non necessari, eccedenti o non pertinenti con la finalità di pubblicazione

DATI SENSIBILI E GIUDIZIARI – convinzioni religiose e filosofiche, opinioni politiche, stato di salute, vita sessuale, provvedimenti in materia di casellario giudiziale

DIVIETO ASSOLUTO
di pubblicazione per finalità di trasparenza

PUBBLICAZIONE DEI NOMINATIVI DEGLI ALUNNI DISTINTI PER CLASSE

La diffusione dei dati relativi alla composizione delle classi sul sito web istituzionale non è consentita in quanto la normativa in materia di protezione dei dati personali prevede che la diffusione dei dati personali è lecita solo se prevista dalle disposizioni di settore.

I nominativi degli studenti distinti per classe possono essere resi noti per le **classi prime** delle scuole di ogni ordine e grado, **tramite apposita comunicazione all'indirizzo e-mail fornito dalla famiglia in fase di iscrizione**, mentre per le **classi successive**, l'elenco degli alunni, può essere reso disponibile nell'**area del registro elettronico a cui accedono tutti gli studenti della classe di riferimento.**

Secondo una prassi ormai consolidata è consentita la pubblicazione al **tabellone esposto** nella bacheca scolastica dei nominativi degli studenti distinti per classe. Tale modalità di pubblicazione del tabellone dovrebbe essere adottata in via residuale solo qualora l'istituzione scolastica sia sprovvista di registro elettronico o sia impossibilitata ad utilizzare strumenti di comunicazione telematica dei dati.

In tutti i casi gli elenchi relativi alla composizione delle classi, resi disponibili con le modalità sopraindicate, **devono contenere i soli nominativi** degli alunni e **non** devono riportare informazioni relative allo stato di salute degli studenti o altri dati personali non pertinenti (ad es. luogo e data di nascita, etc.).

GRADUATORIE DEL PERSONALE E SUPPLENZE

Gli istituti scolastici possono pubblicare, in base a quanto previsto dalle specifiche diposizioni di settore e nei tempi ivi stabiliti, sui propri siti internet le **graduatorie di docenti e personale amministrativo tecnico e ausiliario (ATA)** per consentire a chi ambisce a incarichi e supplenze di conoscere la propria posizione e punteggio. Tali liste devono però contenere **solo i dati strettamente necessari all'individuazione del candidato**, come il nome, il cognome, il punteggio e la posizione in graduatoria.

Diversamente **non** devono essere riportati dati non pertinenti, quali, ad es., i numeri di telefono e gli indirizzi privati dei candidati. Tale diffusione dei contatti personali incrementa, tra l'altro, il rischio di decontestualizzazione e di perdita di controllo sui dati e potrebbe, in taluni casi, esporre i lavoratori interessati a forme di stalking o a eventuali furti di identità.

SERVIZI DI SCUOLABUS

Gli istituti scolastici e gli Enti locali **non possono pubblicare online (sito della scuola, profilo social, etc.), in forma accessibile a chiunque, gli elenchi dei bambini che usufruiscono dei servizi di scuolabus**, indicando tra l'altro le rispettive fermate di salita-discesa o altre informazioni sul servizio.

Tale diffusione di dati personali, che tra l'altro può **rendere i minori facile preda di eventuali malintenzionati**, non può assolutamente essere effettuata o giustificata semplicemente affermando che si sta procedendo in tal senso solo per garantire la massima trasparenza del procedimento amministrativo.

PAGAMENTO DEL SERVIZIO MENSA

Non si può pubblicare sul sito della scuola, o inserire in **bacheca**, il nome e cognome degli studenti i cui genitori sono in **ritardo nel pagamento della retta o del servizio mensa**; né può essere diffuso **l'elenco degli studenti, appartenenti a famiglie con reddito minimo o a fasce deboli**, che usufruiscono gratuitamente di tale servizio.

Gli avvisi messi online devono avere carattere generale, mentre alle singole persone ci si deve rivolgere con comunicazioni di carattere individuale. Il gestore del servizio deve inviare alle famiglie i "bollettini" di pagamento in busta chiusa. Eventuali **buoni pasto**, tra l'altro, non possono avere colori differenziati in relazione alla fascia di reddito di appartenenza delle famiglie degli studenti beneficiari.

Queste semplici accortezze evitano che soggetti non legittimati possano venire a conoscenza di informazioni idonee a rivelare la situazione economica delle famiglie dei bambini.

VIDEOSORVEGLIANZA E ALTRI CASI

VIDEOSORVEGLIANZA CONTRO FURTI E VANDALISMI

È possibile installare un sistema di videosorveglianza negli istituti scolastici quando risulti indispensabile per tutelare l'edificio e i beni scolastici, circoscrivendo le riprese alle sole aree interessate, come ad es. quelle soggette a furti e ad atti vandalici.

La necessità dell'installazione di tali sistemi deve essere valutata **evitando** di interferire con l'armonico sviluppo della personalità dei minori in relazione alla loro vita, al loro processo di maturazione e al loro diritto all'educazione, sia con la libertà di scelta dei metodi educativi e d'insegnamento.

In tale quadro, è necessario fare in modo che le telecamere, se posizionate all'interno dell'istituto, siano **attivate solo al termine delle attività scolastiche ed extrascolastiche**, avendo cura di ottemperare alla disciplina in materia di controlli a distanza dei lavoratori ove ne ricorrano i presupposti.

Di contro, le aree perimetrali esterne degli edifici scolastici possono essere oggetto di ripresa, per tutelare l'edificio e i beni ivi contenuti, anche in orario di apertura degli stessi; in tal caso, l'angolo visuale deve essere delimitato solo alle predette aree perimetrali esterne, escludendo dalle riprese quelle non strettamente pertinenti all'edificio (cfr. FAQ del Garante "Scuola e privacy", spec. FAQ n. 14,