# La protezione dei dati a scuola

Guida dell'Incaricato cantonale della protezione dei dati e della trasparenza all'attenzione delle autorità scolastiche e del corpo insegnanti

luglio 2016

# Sommario

# 1. La guida

## 1.1. Introduzione

La scuola ha una visione a tutto campo sulla personalità dello scolaro: dalla sua condotta alle prestazioni scolastiche, dalla salute ai rapporti con la famiglia. Essa rappresenta pertanto un ambiente particolarmente produttivo di dati personali, anche di natura sensibile. L'avvento delle nuove tecnologie in ambito scolastico (gestione elettronica degli incarti, siti Internet, trasmissione elettronica dei dati, ecc.) ha facilitato e razionalizzato l'elaborazione dei dati, creando però nello stesso tempo i presupposti tecnici per elaborazioni non necessarie a fini scolastici. Ne sono un esempio quelle categorie di dati personali non necessarie nell'ambito scolastico, ma previste in modo standardizzato nei programmi di gestione di dati per coprire la più ampia gamma di potenziali bisogni degli utilizzatori. All'avvento delle nuove tecnologie a scuola va dunque inevitabilmente accostata una rinnovata riflessione sulla protezione dei dati personali. La necessità di garantire la protezione dei dati non deve tuttavia dissuadere la scuola dal restare al passo con i tempi e dallo sfruttare le nuove tecnologie, al contrario! Esse permettono delle applicazioni, cui si potrebbe difficilmente rinunciare e che possono essere utilizzate senza violare la personalità degli allievi e del personale scolastico.

Anche lo scolaro è tenuto a responsabilizzarsi quanto alla protezione dei dati nell'uso delle nuove tecnologie. Esse facilitano infatti anche il compimento di atti illeciti. Si pensi ad esempio al cyber-mobbing (pressione psicologica, in particolare tramite diffusione di dati personali in formato video), al cyberbullismo (atti persecutori) e al cyber-stalking (atti di pedinamento), tre dei fenomeni penalmente rilevanti che hanno trovato supporto e rinnovato slancio proprio grazie alle nuove tecnologie. Fotografando o videoregistrando i propri compagni o docenti durante l'insegnamento o in pausa, lo scolaro elabora dati personali di terzi. Per queste elaborazioni di dati lo scolaro ne è direttamente responsabile ai sensi della legislazione sulla protezione dei dati.

Sebbene il problema si ponga, dal punto di vista legale, principalmente tra le persone coinvolte, alla scuola spetta l'educazione degli allievi al reciproco rispetto e in particolare al corretto uso delle nuove tecnologie in sede scolastica.
Più in generale, la scuola nella sua funzione di educatrice e formatrice della personalità degli allievi e in qualità di organo responsabile della protezione dei dati nell'ambito scolastico deve regolare l'uso delle nuove tecnologie e adottare le necessarie misure tecniche idonee a ridurre gli abusi.

### 1.2. Obiettivo e campo di applicazione

La Guida vuole sensibilizzare i responsabili del settore scolastico - in particolare la direzione scolastica, il corpo docenti e l'amministrazione - sui diritti e doveri inerenti alla protezione dei dati personali elaborati in ambito scolastico. Essa è inoltre intesa quale sprone al disciplinamento delle elaborazioni di dati a scuola. Nel 2016, il Legislatore ha introdotto nella Legge della scuola un pacchetto di norme sulla protezione dei dati (art. 91*a* e seguenti).
Sono interessate dalla Guida le scuole pubbliche ticinesi, cantonali e comunali, nonché le scuole private con mandato pubblico d'insegnamento.
Per le restanti scuole private valgono le direttive dell'Incaricato federale della protezione dei dati e della trasparenza (IFPDT)[i].

## 2. La scuola

Dal punto di vista della protezione dei dati, la scuola è un organismo complesso. I vari attori che la compongono costituiscono, nel loro insieme, una rete interattiva a più livelli che può implicare lo scambio di dati personali per l'espletamento dei vari compiti loro attribuiti.
Essa rappresenta dunque una pluralità di organi responsabili della protezione dei dati, di organi partecipanti e di persone interessate dalle elaborazioni di dati. La scuola non si lascia sempre circoscrivere entro limiti di spazio e tempo ben definiti e statici, ma ha una configurazione variabile, a seconda del posto, rispettivamente del periodo, in cui

l'insegnamento viene impartito. La pista di sci oppure il luogo in cui si svolge un workshop estivo rientrano nel concetto di scuola.

## 2.1. Gli attori principali della scuola

ART. 3 CPV. 1 LEGGE SULLA SCUOLA

La Legge sulla scuola prevede tre categorie di persone che compongono la scuola, e cioè i docenti (compresi i maestri di tirocinio, i supplenti e gli stagisti), gli allievi e i genitori (rispettivamente i detentori dell'autorità parentale o i rappresentanti legali).

## 2.2. Organi di conduzione e di rappresentanza

ART. 25 CPV. 2 E 3, ART. 27 CPV. 1 LEGGE SULLA SCUOLA

Gli organi di conduzione della scuola possono essere la direzione e il collegio dei docenti, l'assemblea degli allievi, l'assemblea dei genitori e il consiglio d'istituto. La direzione è composta dal direttore, da uno o più vicedirettori e dal consiglio di direzione. Esistono pure altri organi, non necessariamente di conduzione e di rappresentanza, come il consiglio di classe, composto dai docenti che insegnano nella stessa classe.

## 2.3. Autorità scolastiche

ART. 8 LEGGE SULLA SCUOLA

La legge sulla scuola prevede una serie di autorità scolastiche a vari livelli, che vanno dal Consiglio di Stato - il quale esercita la direzione generale della scuola, per il tramite del Dipartimento dell'educazione, della cultura e dello sport - al Dipartimento, alle autorità scolastiche comunali e consortili, agli organi di promovimento, di coordinamento, di vigilanza e di organizzazione amministrativa. Seppur non siano, di principio, organi responsabili di dati personali degli allievi, anche queste autorità possono, in singoli casi, venire a conoscenza di dati personali di singoli allievi.

ART. 9 SEGG. LEGGE SULLA SCUOLA

## 2.4. Organi di sostegno pedagogico

ART. 63 LEGGE SULLA SCUOLA

I servizi di sostegno pedagogico coadiuvano il docente con un adeguato aiuto agli allievi con difficoltà di adattamento o di apprendimento. In questa funzione, sono responsabili di dati personali che rappresentano, nel loro insieme, un profilo della personalità.

## 2.5. Aiuto sociale

ART. 84 CPV. 11 LEGGE SULLA SCUOLA

Il Cantone elargisce un aiuto allo studio quando un allievo non può sopperire ai costi della scuola pubblica. Nell'adempimento di questa funzione, l'organo cantonale competente elabora dati personali dell'allievo.

# 3. La protezione dei dati

## 3.1. Motivo giustificativo

*Motivo giustificativo* ART. 6 LPDP

Ogni elaborazione di dati personali deve essere giustificata. La LPDP prevede, quali possibili motivi giustificativi la base legale e - per elaborazioni in singoli casi - la necessità di dati personali per l'adempimento di un compito legale o il consenso della persona interessata[ii]. Il consenso deve essere libero e informato, espresso cioè senza pressioni di sorta e previa esplicita ed esauriente informazione sull'elaborazione di dati in questione, in particolare sullo scopo e sull'organo responsabile. Dai 18 anni, è sufficiente l'accordo della persona interessata, mentre quello dei suoi rappresentanti legali (genitori o detentori dell'autorità parentale) – seppur possibile cumulativamente - non è più necessario. Prima del raggiungimento della maggiore età è necessario l'accordo dello scolaro e dei detentori dell'autorità parentale. Se, indipendentemente dalla sua età, lo scolaro non ha la capacità di discernimento, è necessario e sufficiente l'accordo dei rappresentanti legali.

*Esempi:*

*a) L'allievo deve chiedere e ottenere il consenso dell'insegnante e/o dei propri compagni, se intende fotografarli o filmarli durante l'insegnamento o la ricreazione.*

*b) L'insegnante deve chiedere ed ottenere il consenso degli allievi, se intende videoregistrarli durante l'insegnamento per puntuali scopi didattici.*

Gli art. 91*a* e seguenti della Legge della scuola costituiscono le basi legali in particolare per l'elaborazione di dati scolastici nei sistemi GAS e GAGI, per la procedura di richiamo, la trasmissione di dati a terzi, la durata di conservazione dei dati e la delega al Consiglio di Stato per il disciplinamento dei particolari.

## 3.2 Principi

*Principi*

Oltre ad essere giustificata, ogni elaborazione di dati personali deve ottemperare a diversi principi generali della protezione dei dati.

*a) Principio della liceità*
ART. 7 CPV. 1 LPDP

In base al principio della liceità ogni elaborazione di dati personali deve essere conforme all'insieme del diritto.

> *Esempio:*
> *Le banche dati del settore scolastico rappresentano delle elaborazioni sistematiche che possono contenere dati meritevoli di particolare protezione e profili della personalità e prevedono, di regola, degli accessi tramite procedura di richiamo. Presuppongono una base legale specifica (motivo giustificativo) e il rispetto dell'ordine giuridico nel suo insieme (principio della liceità). Il Legislatore ha disciplinato le banche dati del settore scolastico agli art. 91a e 91b della Legge della scuola.*

*b) Principio della buona fede*
ART. 7 CPV. 2 LPDP

Dal principio della buona fede si deduce, in particolare, l'obbligo d'informazione precedente ed esauriente delle persone interessate da una determinata elaborazione di dati personali.

> *Esempio:*
> *Qualsiasi formulario scolastico inteso alla raccolta di dati personali deve contenere l'informazione sullo scopo dell'elaborazione, sui diritti delle persone interessate e sull'organo responsabile dei dati.*

*c) Principio della proporzionalità*
ART. 7 CPV. 3 LPDP

I dati personali e il modo della loro elaborazione devono essere idonei e necessari allo scopo per il quale sono stati raccolti. In particolare, un trattamento di dati personali non è proporzionato se esistono altre soluzioni, meno invasive nella personalità, che permettono di raggiungere lo scopo dell'elaborazione di dati.

*Esempi:*
*a) La scuola non può elaborare dati personali relativi alle attività private dello scolaro, se non sono necessari alla sua gestione amministrativa e scolastica;*
*b) La videosorveglianza dell'area scolastica è sproporzionata se esistono altre misure, meno invasive della personalità, e altrettanto idonee a garantire lo scopo perseguito.*

*d) Principio della finalità*
ART. 7 CPV. 4 LPDP

I dati personali non possono essere utilizzati o trasmessi per uno scopo che, secondo la buona fede, sarebbe incompatibile con quello per il quale originariamente sono stati raccolti.

*Esempio:*
*La scuola non può vendere o cedere i dati degli scolari a terzi per scopi pubblicitari, salvo gli interessati vi abbiano acconsentito e la cessione avvenga nell'interesse dell'allievo.*

*e) Principio dell'esattezza dei dati*
ART. 7 CPV. 5 LPDP

I dati personali devono essere esatti e, nella misura in cui lo scopo dell'elaborazione lo esiga, completi.

*Esempio:*
*Le valutazioni sulle prestazioni scolastiche contenute nel sistema centrale di gestione dei dati personali degli scolari devono riprodurre fedelmente e accuratamente le valutazioni espresse in sede scolastica.*

## 3.3 I diritti delle persone interessate

*a)Diritto all'informazione*

L'art. 91*e* Legge della scuola riserva la Legge sulla protezione dei dati

ART. 23 E 24 LPDP

personali (LPDP) e, quindi, tra l'altro, i diritti delle persone interessate. Secondo la LPDP, chiunque può esigere dall'organo responsabile informazioni in merito all'eventuale elaborazione di dati che lo riguardano. A meno che importanti interessi lo impediscano, la persona interessata può, su richiesta, consultare direttamente i propri dati e ottenerne copia.

*Esempi:*

*a) Lo scolaro o il suo rappresentante legale possono richiedere un estratto completo e gratuito dei propri dati contenuti nel sistema scolastico centrale di gestione dei dati. Il diritto d'accesso ai dati da parte dei genitori può tuttavia essere limitato o differito se lo esige un interesse preponderante dello scolaro (p. es. se la trasmissione di dati ai detentori dell'autorità parentale potrebbe ledere i suoi interessi);*

*b) Lo scolaro può chiedere l'accesso gratuito alla documentazione dei suoi esami di ammissione alla scuola, una volta questi terminati e se non sussistono interessi preponderanti contrari;*

*c) Lo scolaro può chiedere all'insegnante informazioni relative a un procedimento disciplinare in corso a suo carico, se interessi preponderanti contrari non lo impediscono;*

*d) L'insegnante può chiedere all'allievo l'accesso alle videoregistrazioni e/o fotografie che lo concernono e chiederne, se necessario, la distruzione;*

*e) La trasmissione dei dati che si riferiscono al luogo di soggiorno dello scolaro ai detentori dell'autorità parentale può essere differita o rifiutata se la loro trasmissione può compromettere gli interessi dello scolaro.*

I detentori dell'autorità parentale possono accedere ai dati dell'allievo; tuttavia lo scolaro capace di discernimento può opporsi alla trasmissione di dati meritevoli di particolare protezione (p. es. concernenti la sfera intima), se fa valere un interesse preponderante contrario.

In caso di ricorso contro una decisione delle autorità scolastiche, i diritti di accesso sono retti dalla legge di procedura applicabile (diritto di essere sentito).

*b)Diritto di rettifica*
ART. 25 LPDP

Chiunque dimostri un interesse meritevole di tutela può esigere dall'organo responsabile che dati personali inesatti siano rettificati.

*Esempio:*
*Lo scolaro può far correggere o completare i dati erronei o incompleti contenuti nel sistema centrale o in altri supporti di dati che lo concernono.*

*c)Diritto di blocco*
ART. 25a LPDP

La persona interessata può far bloccare in ogni momento la trasmissione dei suoi dati.

*Esempi:*
*a) Lo scolaro può, in qualsiasi momento, richiedere e ottenere dalla scuola che la propria fotografia non sia pubblicata sul sito Internet scolastico. Il diritto di blocco vale anche nel caso in cui l'allievo ha in precedenza dato il suo consenso alla pubblicazione.*
*b) L'insegnante può chiedere all'allievo di bloccare ogni ulteriore pubblicazione dei suoi dati (p. es. una videoregistrazione della lezione) in Internet.*

*d)Diritto all'interruzione*
ART. 26 LPDP

Chiunque dimostra un interesse meritevole di tutela può esigere dall'organo responsabile che l'elaborazione illecita di dati personali che lo concernono sia interrotta, che i dati personali siano distrutti, che le conseguenze dell'elaborazione illecita siano eliminate o che l'illegalità di un'elaborazione sia constatata.

*Esempio:*
*Se i dati personali sono errati, la persona interessata può chiedere all'organo o alla persona responsabile, oltre alla*

*rettifica, anche l'interruzione dell'elaborazione o la distruzione dei dati. Se del caso, la persona interessata può far valere i suoi diritti in giustizia*[iii]*, in particolare il diritto alla constatazione del carattere illecito di una determinata elaborazione di dati e, eventualmente, un risarcimento per il torto subito.*

## 3.4 Sicurezza dei dati

La sicurezza informatica, riservata all'art. 91*e* Legge della scuola, gioca un ruolo centrale nella corretta elaborazione di dati. Per questo motivo, la definizione, la messa in opera e la manutenzione di un sistema di sicurezza compete agli specialisti del settore.
La questione della sicurezza concerne in particolare *1)* gli accessi logici ai dati (chi può leggere, introdurre, modificare e/o distruggere quali dati), *2)* la sicurezza fisica del server (compresi i backup) e *3)* le trasmissioni di dati.

*Accessi logici ai dati*

I diritti d'accesso alle banche dati informatiche dei singoli utenti devono essere compatibili con i rispettivi compiti. Spetta all'organo responsabile del sistema definire chi ha accesso a quali dati, a quale scopo e in quale misura (modulazione degli accessi). Egli ha inoltre il compito di definire le misure tecniche e organizzative per garantire la sicurezza degli accessi. Dal punto di vista tecnico esistono due tipi di misure di sicurezza:

- **La protezione dell'hardware**: È importante evitare che il computer usato per accedere ai dati scolastici possa essere infettato da programmi nocivi (virus, spyware, keylogger, ecc.). E' necessario proteggerlo, implementando un sistema di protezione completo che comprenda, quali misure minime, in particolare un antivirus aggiornato quotidianamente, un programma per la rimozione di tracce elettroniche, un sistema di Firewall e una costante analisi della rete per individuare eventuali sniffer. Una particolare attenzione va data ai computer privati usati per una connessione remota (p. es. da casa) alla banca dati scolastica. Tuttavia non è possibile, per la scuola, monitorare tutti i singoli computer privati.

La gente deve però perlomeno allestire un regolamento che obblighi gli utenti ad assumere le misure di sicurezza adeguate, informandoli nel contempo delle conseguenze di un'eventuale violazione della prescrizione. Queste regole devono valere anche per l'eventuale uso di computer privati e/o apparecchi multimediali allacciati (tramite cavo o rete wireless) alla rete informatica delle scuole o che contengono dati scolastici (ad esempio, tablets privati contenenti dati sugli scolari).

- **La protezione degli account personali**: gli account di accesso ai dati sono personali. Ogni utente deve avere un proprio account protetto da una password sufficientemente complessa. È compito della scuola verificare (tramite ad esempio condizioni sulla complessità delle password) che le regole riguardanti la password siano rispettate come pure rendere attenti gli utenti del fatto che la password è da considerarsi come un'informazione confidenziale e che quindi non deve essere accessibile a terzi[iv].

Se, tecnicamente, è relativamente semplice garantire la sicurezza e la confidenzialità dei dati, non si può dire lo stesso per la loro organizzazione. I diversi processi all'interno del sistema scolastico devono essere analizzati accuratamente, per definire quali utenti (o funzioni) hanno necessità di accedere a quali dati e con quali prerogative (le quali, peraltro, possono cambiare con il tempo). Questo lavoro di (costante) analisi dei processi deve avvenire prima di implementare e attivare i differenti strumenti informatici. La prima misura di ordine organizzativo da adottare è la giornalizzazione degli accessi.

*Sicurezza del server (e del backup)*

Spesso, i dati elaborati in un determinato ambito sono conservati in uno o più server[v]. Questi ultimi devono essere protetti con misure adeguate. In particolare, vanno custoditi in appositi locali, ai quali solo le persone autorizzate hanno accesso, utilizzando una chiave, un badge o un pin personale. Idealmente, tutti gli accessi al locale dei server devono essere giornalizzati al fine di poter disporre dei necessari strumenti di prova in caso di necessità.

I dati sono, di norma, elaborati in specifiche banche dati gestite fisicamente da sistemisti. Di principio, l'accesso ai dati produttivi da parte dei sistemisti non è necessario per l'esecuzione dei loro compiti, per cui non va concesso. Tuttavia, può essere loro concesso per motivi di praticabilità, a condizione di prevederne la giornalizzazione. I backup contengono per definizione gli stessi dati dei server e vanno quindi protetti applicando le stesse misure di sicurezza.

*Trasmissione elettronica dei dati*

*In generale*

Quando si valuta la necessità di proteggere una trasmissione di dati in formato elettronico, si può partire dal presupposto che se avviene tramite Internet in modo non criptato o utilizzando delle reti wireless non protette, non è garantita nessuna riservatezza. Il grado di riservatezza di una simile trasmissione di dati personali è equiparabile a quello di una cartolina postale.

Di conseguenza, le informazioni che non si trasmetterebbero con una cartolina postale, non vanno trasmesse nemmeno tramite Internet, sempre che ciò non avvenga in modo criptato.

*Tramite browser*

Gli accessi a dati tramite browser costituiscono, dal punto di vista dell'organo responsabile, una trasmissione elettronica di dati tramite procedura di richiamo. La riservatezza dei dati può essere garantita utilizzando un sistema di criptaggio (protocollo "https").

*Tramite posta elettronica*

La trasmissione elettronica di dati tramite posta elettronica è più complessa. Una cifratura della posta elettronica presuppone l'implementazione di un'infrastruttura di chiavi pubbliche (*Public Key Infrastructure, PKI*). Queste tecnologie esistono da molti anni, ma una loro diffusione su ampia scala è complessa e costosa.

Questa difficoltà di implementare una soluzione che risolva il problema alla radice con una misura di ordine tecnico costringe spesso le persone interessate a cercare delle soluzioni di natura organizzativa.

Una possibile soluzione consiste nella protezione dei documenti contenenti dati personali con una password prima di inviarli tramite e-mail, per poi comunicare la password con un altro mezzo di comunicazione sicuro (p. es. tramite posta o telefono, sempre che in quest'ultimo caso si sia in grado di identificare con certezza l'interlocutore).
Per quanto riguarda la comunicazione d'informazioni alle scuole da parte dei genitori o degli studenti, una possibile soluzione consiste nell'uso di formulari online (che dovrebbero essere disponibili sui siti Internet delle scuole).

Questo accorgimento permette di rientrare nella trasmissione di dati via browser, e dunque, idealmente, di criptarla, risolvendo così il problema. Tale soluzione va dunque preferita a quella basata sulla posta elettronica.
Per quanto riguarda, infine, la comunicazione ai genitori o agli studenti da parte delle scuole, è necessario optare per una soluzione radicale: non si trasmettono dati personali meritevoli di particolare protezione tramite posta elettronica, a meno che non si trovi un accorgimento tecnico o organizzativo capace di garantire la protezione dei dati. Il problema può essere aggirato se gli studenti o i genitori hanno un account presso il sistema di gestione della scuola, facendo rientrare la comunicazione nella trasmissione di dati via browser. È compito della scuola sensibilizzare le persone coinvolte riguardo questi accorgimenti.

*Trasmissione di dati tramite telefono*

Quando sono richiesti dati personali al telefono, l'identità del richiedente non è sempre verificabile, per cui la prudenza è d'obbligo. Nel caso in cui una persona non possa essere identificata con certezza, va evitata la trasmissione di dati personali al telefono.

# 4. L'elaborazione di dati a scuola

## 4.1. I dati personali

*Dati standard*

La scuola necessita una serie di dati personali di base, o standard, riguardanti gli allievi, a scopi essenzialmente amministrativi. Di norma, la

scuola elabora i seguenti dati standard:

- Dati riguardanti l'identità: numero AVS, nome, cognome, indirizzo, sesso, data di nascita, numero di telefono, nazionalità, lingua materna, detentori dell'autorità parentale, eventualmente numero ed età di fratelli e sorelle;
- Dati riguardanti i detentori dell'autorità parentale: nomi, cognomi, indirizzi, numeri di telefono;
- Dati necessari in caso d'emergenza: informazioni di contatto delle persone da contattare in caso d'emergenza (di regola, o genitori).

Per contro, dati quali l'attinenza, la professione dei detentori dell'autorità parentale, le malattie senza importanza diretta per il quotidiano scolastico, l'assicuratore malattia, non sono necessari. Questi dati possono essere richiesti all'autorità parentale, indicando sul formulario che la compilazione di questi campi è facoltativa.

*Dati meritevoli di particolare protezione*

Tra tutti i dati elaborati dalla scuola, possono essere classificati come meritevoli di particolare protezione i dati riguardanti i reati commessi, la religione e la salute.

Il seguente capitolo descrive le principali categorie di dati meritevoli di particolare protezione elaborate nel settore scolastico.

## 4.2. I dati meritevoli di particolare protezione

*Dati su reati commessi*

La scuola può detenere informazioni su reati commessi da allievi. Questi dati sono confidenziali e non possono essere accessibili a persone non autorizzate, come ad esempio i genitori di altri allievi o i docenti di altre classi, purché non vi sia un interesse preponderante all'informazione. L'esistenza di un simile interesse va valutato in ogni singolo caso.

Più in generale, la scuola può essere portata ad agire preventivamente contro fenomeni di criminalità. Un'educazione efficace presuppone che gli istituti scolastici garantiscano il rispetto delle regole di comportamento e

che vi sia una convivenza sicura, perlomeno nell'ambito scolastico.

Per garantire queste condizioni in modo preventivo, la regolare discussione tra scuola, scolari e genitori a scopo formativo è di fondamentale importanza. A scopi di prevenzione, può essere fatto appello anche agli esperti della sicurezza, come ad esempio la polizia. Il tempestivo ricorso alla polizia può, ad esempio, permettere di riconoscere e ostacolare pericoli o reati imminenti. La collaborazione preventiva tra scuola e polizia può essere garantita di regola da un membro della direzione scolastica e da un incaricato delle questioni giovanili presso la polizia. La collaborazione può prevedere misure sia preventive (p. es. riunioni regolari), sia consecutive a eventi concreti (p. es. scambio d'informazioni, piano d'intervento multidisciplinare o Case Management). Nell'ambito delle misure preventive, non è di principio lecito elaborare dati personali riferiti ad allievi identificati o identificabili. Lo scambio d'informazioni in seno a singoli gruppi di lavoro deve dunque avvenire in modo tale da garantire il rispetto della personalità degli allievi e delle persone interessate in generale.

*Dati sulla religione*

L'elaborazione di dati sulle attività e opinioni religiose degli scolari può essere necessaria per comporre le classi di religione e per meglio gestire le attività connesse a tale insegnamento. È compito della scuola (e non dell'insegnante di religione) raccogliere i dati sul credo religioso presso gli interessati (i genitori o gli allievi). L'insegnante di religione ha il diritto di accesso ai sistemi di gestione dei dati personali riguardanti gli allievi della sua classe, conformemente alle normative sugli accessi degli insegnanti. I dati sulla religione non possono essere elaborati per scopi non legati all'insegnamento religioso.

*Dati sulla salute*

Nel rapporto che lega lo scolaro alla scuola, il primo può essere tenuto a comunicare i propri dati personali sullo stato di salute alla scuola unicamente se questo condiziona l'insegnamento. Generalmente, i dati sulla salute che la scuola necessita si concentrano sulla durata dell'assenza dall'insegnamento e sul motivo dell'assenza, indicato in modo generico (malattia o incidente, durata dell'assenza).

Altri dati dettagliati sulla salute, ad esempio la diagnosi non sono, di principio, necessari per l'adempimento dei compiti scolastici e non devono essere comunicati alla scuola, salvo decisione contraria dell'allievo stesso o dei suoi rappresentanti legali. Nel caso, ad esempio, di allergie ai pollini, l'allievo può, se lo ritiene necessario, informarne la scuola preventivamente, oppure limitarsi a informarla in singoli casi di necessità (p. es. in occasione di un workshop all'aperto). In ogni caso non è, di regola, necessario fornire alla scuola un certificato medico che indichi la diagnosi, ma unicamente l'informazione generica sulla necessità di evitare ad esempio sport e attività fisiche all'aperto.

Dati sulla salute più dettagliati possono essere elaborati da parte della scuola, anche preventivamente (cioè prima dell'ammissione dello scolaro all'insegnamento), unicamente se sono necessari per organizzare un sostegno particolare (p. es. una sedia ergonomica), per l'assegnazione del sostegno specialistico allo scolaro disabile o per l'insegnamento domiciliare o ospedaliero. In simili casi particolari, l'elaborazione di dati sulla salute si giustifica di principio, nell'interesse dello scolaro, dei genitori e della scuola. Tuttavia, anche in questi casi va valutato se non sia sufficiente fornire alla scuola unicamente un certificato medico attestante la necessità d'implementazione di determinate misure organizzative, senza indicazione della diagnosi. Non va dimenticato che la scuola generalmente non possiede competenze mediche e che dunque i dati personali dettagliati sulla salute non sono necessari e vanno sostituiti con informazioni pratiche sul modo di gestire l'allievo.

*Dati relativi al consumo di stupefacenti*

Diversi istituti scolastici in Svizzera stanno pensando di introdurre, o hanno già introdotto, i cosiddetti narcotest, al fine di contrastare le tossicomanie tra gli scolari. Essi comportano l'elaborazione di dati personali, rilevati tramite test dell'urina o del sangue, riguardanti il consumo di stupefacenti e il relativo quantitativo. Questa categoria di dati personali possono far parte, - oltre che, in singoli casi, della categoria dei dati su reati commessi - anche della categoria dei dati relativi alla salute e come tali sono meritevoli

di particolare protezione.

Gli organismi che si occupano del problema, in particolare l'Istituto svizzero di prevenzione dell'alcolismo e delle altre tossicomanie (ISPA), nonché le autorità preposte alla protezione dei dati, sconsigliano i narcotest a causa di possibili attriti con la protezione della personalità e con gli scopi pedagogici della scuola. Secondo questi organismi, i narcotest, e soprattutto le elaborazioni di dati che ne risultano, sono controproducenti da un punto di vista educativo, e dunque sproporzionati e ingiustificati. In particolare, essi possono essere lesivi dei particolari rapporti di subordinazione esistenti in ambito educativo, nonché discriminatori, cioè nocivi soprattutto per la reputazione sociale dello scolaro.

Inoltre, essi sono inutili per controllare il rispetto dei regolamenti scolastici; il valore dei risultati dei narcotest è infatti relativamente basso. In particolare, il risultato positivo di un narcotest non significa necessariamente che la persona interessata abbia consumato stupefacenti; è risaputo che certi medicamenti, come ad esempio alcuni tipi di sciroppi contro la tosse, possano dare risultati positivi. Inoltre, da un simile risultato non si può concludere che lo scolaro in questione consumi droghe in modo regolare. I narcotest possono inoltre essere falsificati facilmente, limitandone così l'effetto dissuasivo.

Per queste ragioni, i narcotest vengono relegati, da parte degli organismi specializzati, semmai, a rango di misura accompagnatoria nel quadro di un intervento terapeutico effettuato da specialisti.

Se la scuola detiene dati sul consumo di stupefacenti da parte di singoli scolari, vanno distrutti dopo la fine del periodo di conservazione, e non archiviati (per maggiori informazioni si rinvia alla Guida ISPA "École et Cannabis", capitolo 6).

Per questioni di ordine pubblico, e come visto nei capitoli precedenti, se sussiste rischio di reato da parte dello scolaro stesso o di terzi, può essere fatta intervenire la polizia o personale specializzato, fermo restando che questa soluzione deve essere sussidiaria a un approccio più pedagogico. Di regola, è compito dell'insegnante principale avviare le prime misure d'intervento adeguate, contattando la direzione scolastica.

La scuola è tenuta a elaborare una ripartizione delle competenze per le successive fasi della gestione del caso. Comunque, come già detto, oltre all'intervento della polizia, esistono altre misure che non deteriorano il rapporto di fiducia e che prendono più adeguatamente in considerazione la protezione della personalità dell'allievo e il compito pedagogico della scuola. In particolare, nella maggior parte dei casi, cambiamenti positivi del comportamento di uno scolaro possono essere indotti da misure di sostegno come i colloqui individuali. In singoli casi, è appropriato ed efficace anche l'intervento dei genitori, degli operatori sociali, di un esperto, di un consultorio o delle autorità tutorie.

Dati sulle prestazioni scolastiche

Le pagelle scolastiche con le valutazioni delle prestazioni scolastiche e della condotta sono consegnate periodicamente all'allievo. Per il loro allestimento, il corpo insegnanti è autorizzato a raccogliere i seguenti dati sugli allievi:

a) compiti, presentazioni, esami (controllo delle conoscenze);
b) note e commenti di esami emessi dal corpo insegnanti;
c) osservazioni sul comportamento e sul modo di apprendere;
d) in caso di situazione particolare dell'allievo, dati su misure di sostegno, situazione familiare, sostegno pedagogico individuale.

Questi dati, che nel loro insieme, costituiscono un profilo della personalità, possono essere utilizzati come base di decisione per misure di sostegno, di selezione o promozione.

## 4.3. Le principali fasi dell'elaborazione dei dati

### 4.3.1 Raccolta e utilizzazione di dati

Le fonti, i metodi e le procedure di raccolta di dati personali concernenti gli allievi possono variare notevolmente e vanno dalla raccolta scritta tramite questionario, alla raccolta orale (tramite domande, discussioni o altro), oppure alla raccolta di dati online. Le fonti sono soprattutto gli allievi stessi, i loro rappresentanti legali o terzi (p. es. le scuole precedenti).

In ogni caso vanno sempre rispettate le condizioni della protezione dei dati, in particolare le basi legali (art 91*a* segg. Legge della scuola) ed i principi della protezione dei dati. L'allievo va informato sulle finalità della raccolta, sul motivo giustificativo e sull'organo responsabile.

### 4.3.2 Trasmissione di dati

La scuola è autorizzata a trasmettere dati personali alle seguenti condizioni:

Per quanto riguarda la procedura di richiamo, l'art. 91b prevede che gli organi responsabili possono rendere accessibili i seguenti dati personali alle seguenti categorie di persone:

a. quelli necessari all'adempimento dei compiti di gestione dei docenti e degli allievi ai membri di organi scolastici e di conduzione degli istituti nonché al loro personale amministrativo;

b. quelli necessari all'adempimento dei compiti di gestione degli allievi ai docenti e ai supplenti;

c. quelli necessari all'adempimento dei compiti di gestione dei docenti e degli allievi ai singoli servizi dipartimentali;

d. quelli necessari all'adempimento dei compiti di ricerca o di manutenzione del sistema ai servizi interni ed esterni incaricati di queste incombenze.

Per la trasmissione di dati a organi pubblici e a privati nel singolo caso, l'art. 91c prevede che dati personali inerenti ad allievi e docenti possono essere trasmessi a organi pubblici solo se l'autorità competente è autorizzata dalla legge e se i dati nel caso specifico sono indispensabili all'organo richiedente per l'adempimento dei suoi compiti legali oppure se la persona interessata o il suo rappresentante legale, nel singolo caso, hanno dato il loro consenso libero e informato.

La trasmissione a privati di dati personali di allievi, liste di classe comprese, o di docenti è possibile solo se l'autorità competente è autorizzata dalla legge, oppure se la persona interessata o il suo rappresentante legale hanno dato il loro consenso libero e informato.

I dati possono essere trasmessi in forma anonimizzata a terzi a scopo di statistica e di ricerca sulla base di convenzioni specifiche.
La necessità di dati (b) è data nel caso dei servizi sanitari o di sostegno (il medico o il servizio psicologico della scuola, oppure il servizio sociale della scuola), dei membri del corpo insegnanti, delle direzioni e commissioni scolastiche, delle autorità di sorveglianza. La trasmissione deve avvenire nel rispetto dei principi della protezione dei dati, in particolare della proporzionalità e della finalità. In assenza di un motivo giustificativo, la trasmissione di dati non è ammessa e vige il segreto d'ufficio. Ciò vale non soltanto per le trasmissioni di dati dalla scuola a terzi esterni, ma pure tra organi e servizi della stessa scuola (ad esempio tra docente e direzione scolastica), se non sussiste un interesse preponderante contrario. La scuola è tenuta a una gestione confidenziale delle informazioni a carattere personale che detiene e di farne uso unicamente nella misura in cui i suoi compiti legali lo esigono.

### 4.3.3 Rettifica di dati

Il principio dell'esattezza dei dati implica la costante attualizzazione e, se del caso, correzione, dei dati personali.

### 4.3.4 Conservazione, archiviazione e distruzione di dati

La conservazione dei dati personali soggiace in particolare al principio della proporzionalità, per cui essi possono essere conservati unicamente fintantoché lo scopo per cui sono stati raccolti lo esige. Una volta raggiunto il loro scopo, i dati personali vanno restituiti agli allievi, rispettivamente, con il loro accordo, distrutti. Dal punto di vista della loro conservazione, vi sono sostanzialmente due categorie di dati personali in ambito scolastico: a) quelli a lunga durata di conservazione, che supera l'anno scolastico di riferimento e b) quelli a breve-media durata di conservazione, che non supera l'anno scolastico di riferimento.
Per quanto riguarda i dati a lunga durata di conservazione (in particolare i dati amministrativi dell'allievo, le pagelle, i diplomi, ecc.), l'art. 91d Legge della scuola prevede quanto segue:

I dati degli allievi possono essere conservati al massimo fino a 4 anni a partire dalla fine della carriera scolastica e in seguito solo in forma anonimizzata ai fini della statistica e della ricerca educativa; quelli meritevoli di particolare protezione possono essere conservati al massimo fino a 4 anni dalla conclusione del rispettivo ciclo scolastico e in seguito solo in forma anonimizzata ai fini della statistica e della ricerca educativa; quelli di carattere penale possono essere conservati al massimo fino alla cancellazione dal casellario giudiziale.
I dati riguardanti il personale scolastico possono essere conservati al massimo fino 10 anni dalla fine del rapporto d'impiego e in seguito solo in forma anonimizzata ai fini della statistica e della ricerca educativa; quelli di carattere penale possono essere conservati al massimo fino alla cancellazione dal casellario giudiziale.
Il dipartimento adotta i provvedimenti tecnici e organizzativi necessari per proteggere i sistemi informativi contro la perdita, il furto, l'elaborazione e la consultazione illecite dei dati.

Tra i dati a breve-media durata di conservazione figurano principalmente i dati raccolti durante l'insegnamento come gli esami, le note, i rapporti di valutazione, i disegni, i quaderni, i dettati, ecc. Queste informazioni vengono di regola conservate da parte della scuola, durante, e non oltre, l'anno scolastico in questione. Esse vengono in seguito restituite agli allievi o, con il loro accordo, distrutte.

## 4.4. Strumenti e metodi di elaborazione

I documenti in formato elettronico hanno l'indubbio vantaggio di poter essere copiati, trasmessi, consultati e diffusi facilmente. Ciò comporta anche dei rischi, poiché con la stessa facilità i dati elaborati possono finire in mani sbagliate. In particolare l'elaborazione elettronica di dati presuppone, quindi, una precedente analisi riguardante la sicurezza logica e fisica.

*Il sito Internet*

La strumento per eccellenza per diffondere documenti in formato elettronico è il sito Internet, di cui un numero crescente di scuole dispone e che spesso funge anche da albo virtuale. È opportuno non sottovalutare i rischi che ne derivano. Infatti, quanto è pubblicato su Internet, anche solo per un breve periodo, è da considerarsi accessibile a chiunque e a tempo indeterminato. È dunque importante che la scuola si distingua, nell'allestimento del proprio sito Internet, anche per il rispetto della privacy. Da notare a questo proposito che la divulgazione di dati personali sul sito Internet della scuola (ad esempio, fotografie di allievi) costituisce un'elaborazione sistematica di dati per la quale è necessaria una base legale.

*Blog di classe*

Nelle scuole si moltiplica l'uso di cosiddetti blog di classe. Sono paragonabili, per scopo, ai forum di discussione e servono, generalmente, allo scambio d'idee su un determinato tema o compito. Di regola, il blog è creato da un docente (che diventa, a quel punto, organo responsabile), il quale, oltre a fissare le regole d'uso, attribuisce gli accessi ai suoi scolari, definendo degli account personali protetti da password. Il docente deve garantire la protezione dei dati. In particolare deve garantire la sicurezza degli accessi. Per questo motivo, vanno escluse piattaforme esterne alla scuola. L'organo responsabile deve pure esercitare la supervisione sull'uso e sul contenuto del blog. Anche per i blog di classe valgono i principi generali, i diritti e le norme di sicurezza visti in precedenza.

*Il Cloud computing*

Il Cloud computing comporta il trasferimento di dati in luoghi non noti e il rischio di perdita del controllo sui dati. È quindi necessaria un'attenta valutazione dei rischi. In assenza di precise garanzie riguardo la protezione dei dati da parte del gestore, non è ammissibile, in ambito scolastico, far capo a soluzioni di cloud computing.

Per più ampie informazioni sull'uso lecito del Cloud computing, si rinvia allo specifico documento previsto nella lista dei materiali (capitolo 6).

*I computer professionali*

L'accesso ai dati scolastici avviene di regola tramite computer della scuola, i quali vanno protetti e configurati tenendo conto delle misure di sicurezza

di cui al capitolo 3.4.

*I computer privati*

L'accesso ai dati avviene spesso anche tramite computer privati. Si pensi al docente che accede all'archivio di dati della scuola direttamente da casa. Anche in questo caso deve essere garantita la protezione e la sicurezza dei dati.

*La rete wireless*

La rete wireless all'interno della scuola è una modalità di accesso ai dati personali e soprattutto ad Internet e può presentare notevoli problemi dal punto di vista della protezione dei dati.

Oltre ai possibili problemi già affrontati nei capitoli precedenti legati alla sicurezza informatica, le reti wireless presentano il rischio di uso non autorizzato da parte di terzi della rete informatica e dell'allacciamento a Internet della scuola. Gli accessi vanno quindi protetti da adeguate misure di sicurezza e giornalizzati.

*Gli apparecchi multimediali*

*In generale*

L'impiego puntuale di sistemi di registrazione (audio e/o video) da parte d'insegnanti deve essere didattico (p. es. per la registrazione di prove di teatro o di lezioni di educazione fisica).

E' consigliabile emanare una direttiva sull'uso dei telefoni cellulari a scuola. L'elaborazione puntuale di dati personali (ad esempio videoregistrazioni o fotografie per scopi puntuali) presuppone il consenso degli interessati.

*Internet*

Per l'uso da parte degli allievi di un servizio Internet messo a disposizione dalla scuola, si consiglia di focalizzare gli sforzi di prevenzione degli abusi sulle misure tecniche quali i filtri del Firewall. L'analisi dell'uso di Internet da parte degli allievi è uno strumento principalmente repressivo, e dunque non sempre adeguato nell'ambito della formazione di allievi. L'analisi delle giornalizzazioni degli accessi ad Internet va dunque fatta unicamente per ragioni statistiche o per ricostruire l'accaduto in caso di panne informatica

o di problemi legati alla sicurezza informatica.

*La videosorveglianza*

Durante l'insegnamento, le aule scolastiche, come pure la palestra, i locali di studio o di musica, il locale PC e l'aula degli insegnanti e altre aree adibite allo studio non possono essere sorvegliate da videocamere. Il controllo sistematico e prolungato del comportamento e della prestazione di scolari e insegnanti è contrario ai diritti della personalità.

La videosorveglianza durante gli orari di chiusura della scuola (orario serale e notturno, fine settimana, periodi di vacanza, giorni festivi) è ammissibile, a condizione tuttavia che la presenza dell'impianto di videosorveglianza sia segnalata tramite appositi cartelli e che misure meno incisive nella personalità delle persone interessate, ma altrettanto efficaci, non siano ipotizzabili (p. es. la recinzione dell'area scolastica in questione e/o i sistemi di allarme). Se necessario, tali misure possono essere cumulate con la videosorveglianza. La videosorveglianza, se comporta l'elaborazione sistematica di dati personali, deve poggiare su una base legale.

*La Smart Pen*

La Smart Pen è una penna in grado di registrare sia quanto l'utilizzatore scrive, sia l'audio, e di memorizzare le due registrazioni in modo sincronizzato. La Smart Pen è uno strumento utile a persone affette da dislessia. Riproducendo le registrazioni, essa permette loro di riconoscere gli errori di scrittura e di correggere sia il testo scritto sia, a più lungo termine, quelle parti di linguaggio e di scrittura che risultano essere problematici. La penna in questione registra, su uno speciale supporto tattile, unicamente le immagini di quanto scritto e l'audio dell'ambiente circostante. Le registrazioni possono essere trasferite a qualsiasi computer dotato del software necessario. Tecnicamente, è dunque possibile trasmettere le registrazioni a terzi, i quali potrebbero riprodurre il file audio senza l'ausilio del software di cui sopra.

L'utilizzo di questo strumento comporta dunque dei rischi dal punto di vista della protezione dei dati e va autorizzato previa sottoscrizione di una dichiarazione sulla protezione dei dati.

## 4.5 Alcune delle principali trasmissioni puntuali di dati nel settore scolastico (art. 91c Legge della scuola)

*Ai genitori*

Nelle informazioni ai genitori da parte del personale scolastico su particolari attività o avvenimenti scolastici (tramite giornale della scuola o degli scolari, flyer di manifestazioni scolastiche, ecc.), va evitato, di principio, di fornire dati che permettano di risalire, direttamente o indirettamente, all'identità di singoli scolari, se sono implicati in fatti delicati da un punto di vista della protezione della personalità.

*Esempi:*
*a) Se l'istituto scolastico è teatro di fatti legati allo spaccio e/o al consumo di droga rapportati a singoli allievi, l'informazione ai genitori avverrà di principio in modo neutro e generale.*
*b) L'informazione ai genitori riguardante la composizione delle classi non desta problemi.*

Alla stessa stregua del genitore che detiene l'autorità parentale, anche il padre o la madre che non detiene l'autorità parentale può informarsi presso l'insegnante o gli insegnanti del proprio figlio sul suo stato formativo e sul suo sviluppo personale, anche se il genitore che detiene l'autorità parentale si oppone. Tuttavia, gli insegnanti non sono tenuti a informare di propria iniziativa il genitore senza autorità parentale. Quest'ultimo deve dunque presentare una richiesta d'informazione. Una sola domanda presso l'insegnante può portare all'informazione concernente tutti i fatti salienti di un periodo prolungato di tempo (p. es. un anno scolastico). Il genitore senza autorità parentale può anche partecipare alle riunioni dei genitori, se portano sull'orientamento scolastico dell'allievo (accesso a una classe superiore, selezione), o ottenere informazioni in occasione delle giornate delle porte aperte della scuola. In ogni caso, il genitore senza autorità parentale può unicamente raccogliere informazioni, ma non intervenire nell'educazione e formazione del figlio.

Qualsiasi informazione che non porta sullo stato formativo o sullo sviluppo personale dell'allievo, ad esempio l'indirizzo attuale dello scolaro, non può essere divulgata al genitore senza autorità parentale.
In tutti i casi, la scuola è tenuta a ponderare gli interessi in causa prima di trasmettere dati al genitore senza autorità parentale.

*Tra la scuola e il servizio medico della scuola*

La gestione dei dati medici degli allievi da parte del servizio medico scolastico deve essere conforme alle norme generali sulla protezione dei dati previste al capitolo 3. Il servizio medico scolastico è soggetto al segreto medico. Non è di conseguenza autorizzato, senza il consenso dell'interessato, a divulgare informazioni di natura medica sugli scolari a terzi, neppure quella riguardante la semplice apertura di un incarto medico su un determinato allievo. Nei confronti della scuola, può divulgare informazioni generiche (ad esempio, conferma dell'assenza per malattia e durata).

*Tra la scuola e il servizio sociale scolastico*

Il servizio sociale scolastico assume innanzitutto dei compiti d'assistenza ai bambini e adolescenti in virtù della legislazione sull'assistenza sociale. In particolare, il servizio si occupa di prevenzione, di rilevazione precoce di determinati problemi e del rispettivo accompagnamento degli allievi in questione. L'elaborazione dei dati del servizio sociale nell'ambito scolastico si fonda sul consenso dell'interessato. Gli assistiti devono poter contare sull'elaborazione confidenziale dei propri dati.

*Trasmissione di dati in caso d'interscambio*

La trasmissione di dati personali degli allievi che partecipano a un inter-scambio tra classi (anche con scuole all'estero), sono giustificate nella misura in cui si limitano ai dati necessari a tale scopo. Il consenso degli allievi non è necessario; è sufficiente un'informazione sullo scopo della trasmissione di dati.

*Tra la scuola dell'infanzia e la scuola elementare*

È permessa la trasmissione di dati sull'identità, sulle conoscenze linguistiche, sui rapporti di valutazione (in particolare, relativi all'orientazione verso una scuola o classe speciale), nonché eventuali altri dati necessari alla scuola primaria per svolgere i suoi compiti.

*Alle autorità d'istruzione penale*

La prassi svizzera ed estera ha sviluppato il principio secondo cui più grave è il reato contestato allo scolaro, più la scuola è tenuta a sporgere denuncia, al fine di evitare un ulteriore pregiudizio all'interesse pubblico in causa. Al contrario, meno grave è il fatto, più la scelta sarà pedagogica e protettiva della personalità dello scolaro. Quest'apprezzamento degli interessi in gioco è sovente difficile. In caso di dubbio è consigliabile, per lo meno in un primo tempo, fare piuttosto appello al servizio psicologico. Nella misura del possibile, chi chiede consiglio a tale servizio lo farà senza divulgare l'identità dell'allievo in questione.

La denuncia presuppone la trasmissione dei relativi dati personali agli organi competenti. Di principio, vanno informati pure i genitori dello scolaro in questione. Nei confronti di terzi estranei al caso, ad esempio i compagni di scuola dello scolaro in questione, la scuola è tenuta al massimo riserbo quanto alla sua identità. In casi eccezionali, se un interesse preponderante lo giustifica (p. es. gli interessi dei compagni di scuola alla propria sicurezza), e seguendo scrupolosamente il principio della proporzionalità, essa può comunque informarli.

Dal canto suo, la polizia è tenuta a informare la direzione scolastica su azioni o situazioni che si producono al di fuori dell'ambito scolastico e che hanno come autore uno scolaro, nel caso potesse essere compromessa pure la sicurezza a scuola. Dal canto loro, le autorità giudiziarie possono informare in singoli casi la direzione scolastica sull'avvio, esecuzione e conclusione di una procedura penale a carico di un allievo o impiegato scolastico se interessi legittimi e preponderanti lo giustificano. La direzione scolastica è informata dalle autorità competenti pure su tempi e luogo d'esecuzione di una pena. La scuola può documentare adeguatamente i casi di reato, se ciò è necessario per lo svolgimento dei suoi compiti. L'elaborazione di dati concernenti i reati commessi, inserita in uno specifico archivio gestito separatamente dagli incarti degli allievi e da quelli del personale scolastico, può giustificarsi per l'interesse della scuola all'accompagnamento pedagogico e/o disciplinare e lavorativo. Una nota sull'esistenza di un incarto penale può essere deposta nel rispettivo incarto dell'allievo.

La scuola distrugge i dati una volta decorso il termine di conservazione, che va commisurato allo scopo della loro elaborazione. Può essere ragionevole una conservazione durante l'intero periodo di formazione presso l'istituto scolastico in questione, nel caso di reati gravi. In generale, la durata di conservazione va valutata e commisurata al singolo caso e alla gravità del reato.

*Alle autorità di tutela*

L'obbligo della scuola di informare l'autorità di tutela in caso di constatazione di disturbi del comportamento dell'allievo o di rischi cui è esposto (p.es. maltrattamenti) sussiste quando i genitori non sovvengono ai propri doveri nei confronti del figlio.
È possibile che una simile situazione concorra con l'obbligo di informare l'autorità d'istruzione penale. Al fine di raccogliere tutte le informazioni necessarie all'autorità tutoria, è lecito che dati personali sull'allievo in questione circolino tra i membri del corpo insegnanti, la direzione scolastica ed eventuali altri organi scolastici implicati.

Anche al medico scolastico incombe il dovere di informare l'autorità di tutela in caso di necessità. Esiste, nel caso di commissione di fatti reprensibili nei confronti di uno scolaro minorenne, la facoltà (ma non il dovere) dei membri del corpo insegnanti, di informare l'autorità di tutela, indipendentemente dalla gravità dei fatti.

*Trasmissione di dati a terzi*

*In generale*

I dati contenuti nella pagella scolastica, quelli concernenti eventuali misure disciplinari (p. es. una sospensione), oppure altre informazioni a carattere sensibile relative ad un allievo, possono rappresentare un profilo della personalità e sono da considerare alla stessa stregua dei dati personali degni di particolare protezione. Non possono di conseguenza essere oggetto di pubblicazione o trasmissione a terzi non coinvolti nel rapporto d'insegnamento, salvo che lo scolaro e/o i suoi rappresentanti legali vi abbiano acconsentito in modo libero, esplicito e informato. Lo stesso vale, ovviamente, anche per altre informazioni a carattere personale riguardanti gli allievi, i docenti e il personale amministrativo.

*Ai compagni di classe*

Nella misura del possibile, dati personali (soprattutto le note degli esami, le pagelle o i rapporti psicologici), non possono essere comunicati ai compagni di classe di un allievo.

Se lo svolgimento dei compiti della scuola lo esige, dati personali possono essere oggetto di trasmissione ai compagni di classe (ad esempio, il numero di telefono per l'organizzazione di una catena telefonica).

*Tramite Internet*

Innanzitutto, come già segnalato precedentemente, la pubblicazione di dati personali in internet presuppone in ogni caso, oltre alle condizioni previste qui di seguito, l'esistenza di una rispettiva base legale.

Ciò premesso, chiunque rende accessibili a terzi dati sugli scolari o dei membri del corpo insegnanti su Internet deve rispettare gli ulteriori principi della protezione dei dati.

Possono essere trasmessi senza restrizioni particolari le informazioni senza un rapporto diretto con le persone, come ad esempio l'organigramma della scuola, gli indirizzi d'istituzioni legate alla scuola, i regolamenti scolastici, il calendario scolastico, i rendiconti anonimi su manifestazioni e spettacoli scolastici, escursioni e simili.

In linea di massima, il sito Internet della scuola non deve contenere nessun riferimento personale (in particolare nomi, indirizzi, fotografie, numeri di telefono, indirizzi e-mail) riconducibile agli allievi. È, di principio, immaginabile la pubblicazione delle composizioni delle classi, indicando unicamente il nome e la prima lettera del cognome di ogni singolo allievo. Tuttavia, anche in questo caso la pubblicazione di singoli nomi non è ammissibile nella misura in cui l'allievo, rispettivamente i suoi genitori o il suo rappresentante legale, non hanno precedentemente dato il loro consenso.

Un riferimento agli insegnanti è possibile per quanto riguarda il loro nome, cognome, materie insegnate e, eventualmente, indirizzo di posta elettronica professionale.

L’accordo è indispensabile anche per la pubblicazione di dati di altre persone, ad esempio di terapeuti scolastici.
Per quanto riguarda, ad esempio, la pubblicazione di foto (di classe, della recita scolastica, di escursioni, ecc.) in Internet, ciò è possibile previo accordo (anche implicito) di tutti gli allievi e di eventuali altre persone interessate (insegnanti, genitori, accompagnatori). È riservato il diritto di blocco della pubblicazione da parte di singole persone interessate secondo l’art. 25a LPDP.

*Ad aziende private*
La scuola, nell’adempimento del suo dovere di tutela e formazione della personalità dello scolaro e nel rispetto del principio della finalità del trattamento dei dati personali, è tenuta a un’elaborazione confidenziale dei dati. In particolare, non è ammesso utilizzare o trasmettere dati personali degli scolari a terzi a fini pubblicitari senza l’accordo degli interessati.

## 5. Glossario

*Definizioni riguardanti la scuola*

ART. 2 CPV. 2 LPDP

**Scuola:** istituzione cui è demandato il compito pubblico dell’insegnamento scolastico. La scuola è composta di vari organismi quali la direzione, l’amministrazione e il corpo insegnanti. È soggetta alla direzione delle autorità scolastiche secondo la legge sulla scuola. Geograficamente, la scuola ha un’accezione larga e variabile e comprende, oltre ai siti predisposti per l’insegnamento e l’educazione in senso stretto (aule scolastiche), anche tutti gli altri posti dove s’insegna e/o dove la scuola esercita la sua funzione e giurisdizione (essenzialmente, tramite regolamenti scolastici), come la palestra, la piscina, le piste da sci, i siti esterni di workshop, le aree adibite alla ricreazione (piazzale scolastico) e la mensa.

*Definizioni giuridiche*

**Scopo della protezione dei dati personali**: tutelare i diritti fondamentali, in particolare la personalità e la sfera privata, delle persone i cui dati sono elaborati.

ART. 4 CPV. 6 LPDP

**Organi partecipanti**: unità amministrative che possono elaborare i dati, ma che non hanno la facoltà di definire lo scopo e la struttura dell'archivio.

ART. 4 CPV. 3 LPDP

**Elaborazione di dati personali**: tutte le operazioni intese segnatamente alla raccolta, conservazione, utilizzazione, modifica, trasmissione, archiviazione e distruzione di dati personali.

ART. 4 CPV. 4 LPDP

**Archivio di dati** (o banca dati): raccolta di dati personali predisposta all'identificazione delle persone interessate[vi].

ART. 4 CPV. 5 LPDP

**Organo responsabile**: autorità o persona che decide lo scopo di un archivio di dati, la sua struttura e il suo contenuto, assicurandone il controllo come pure la gestione[vii].

ART. 4 CPV. 1 LPDP

**Dati personali**: indicazioni o informazioni che direttamente (p. es. tramite il nome e l'indirizzo) o indirettamente (p. es. tramite la sola fotografia o l'indirizzo IP del suo computer, il numero AVS, i dati biometrici, ecc.) permettono di identificare e caratterizzare una persona.

ART. 4 CPV. 2 LPDP

**Dati personali meritevoli di particolare protezione (o dati sensibili)**: informazioni che possono essere fonte di discriminazione, come le opinioni o le attività religiose, filosofiche o politiche, la sfera intima, lo stato psichico, mentale o fisico, come pure quelle sui reati commessi, le relative pene inflitte e i provvedimenti adottati. Questa categoria di dati personali è soggetta a condizioni di protezione e sicurezza qualificate rispetto ai dati standard.

ART. 3 LETT. D E 37 LPD COMBINATI

**Profilo della personalità**: insieme di dati che permette di valutare caratteristiche essenziali della personalità di una persona fisica. Per quanto riguarda la sua protezione e sicurezza, il profilo della personalità va considerato alla stessa stregua dei dati personali meritevoli di particolare protezione.

*Definizioni tecniche*

**Procedura di richiamo**: modo di consultazione automatizzato di dati, tramite il quale l'organo o l'autorità che richiede l'informazione decide di propria iniziativa il momento, il modo e l'estensione dell'accesso nel caso specifico. Ciò avviene senza l'accordo preventivo dell'autorità che detiene i dati, ossia senza che questa esamini la liceità della consultazione e la sua motivazione ad ogni singola richiesta. La procedura di richiamo presuppone una base legale specifica.

**Logfiles (o giornalizzazioni):** archivi di dati generati automaticamente che permettono di ricostruire, in modo sistematico, le attività d'uso dell'infrastruttura informatica, ad esempio quelle in rete. Generalmente, le informazioni contenute nei logfiles concernono l'autore, l'oggetto e la cronistoria di un'attività[viii].

**Indirizzo IP**: identificatore univoco di un computer che ne permette l'allacciamento e la comunicazione in rete.

**Virus informatico**: programma che, una volta eseguito, è in grado di infettare dei file e di propagarsi verso altri file e/o computer.

**Spyware**: programma informatico in grado di raccogliere dati personali (indirizzi di siti visitati, password, numeri di carte di credito, ecc.) dell'utente a sua insaputa e senza il suo consenso. Questi dati possono essere trasmessi agli autori dello spyware, i quali li possono elaborare a scopi differenti da quelli originariamente previsti.

**Keylogger**: programma o apparecchiatura in grado di intercettare, memorizzare e trasmettere a terzi le sequenze di tasti attivati dall'utente. Queste informazioni (che possono concernere anche le password o i numeri di carte di credito) possono essere ulteriormente elaborate a scopi non conformi a quelli originari.

**Sniffer**: programma o apparecchiatura che intercetta, analizza e

memorizza ciò che transita su una rete informatica.

**PKI**: infrastruttura a chiave pubblica (*Public Key Infrastructure*) che consente di identificare gli utenti in maniera sicura. Grazie ad essa, gli utenti possono avere la garanzia che i messaggi scambiati non saranno intercettati e/o modificati da terzi.

**Cifratura**: tecnica che permette di rendere indecifrabili a terzi dati personali e/o documenti di ogni genere. Si distinguono due tipi di cifrature: quella simmetrica, basata sulla precedente condivisione di una chiave segreta tra gli interlocutori, e quella asimmetrica, basata su una PKI.

**Firma elettronica**: procedimento informatico, basato su PKI, che permette di certificare l'originalità di un documento e di verificare se quest'ultimo è stato modificato dopo essere stato firmato (a due documenti diversi, corrispondono due firme diverse).

**http/https**: principale protocollo di comunicazione usato per comunicare in Internet. La sua variante "https" comprende una cifratura robusta.

**Cloud computing**: insieme di tecnologie che permettono, di norma sotto forma di un servizio, di memorizzare, archiviare e/o elaborare dati sfruttando risorse informatiche distribuite e virtualizzate in rete.

**Account personale:** insieme delle funzionalità e dei contenuti attribuiti a un utente.

# 6. Documentazione utile e abbreviazioni

## 6.1 Guide e pareri

- Direttive di *privatim,* l'associazione dei Garanti svizzeri della privacy, del 31 ottobre 2013 sul Cloud computing nell'ambito scolastico, http://www.privatim.ch/files/layout/downloads_de/privatim_Cloud_Computing_scuol

e_2013_i_V1.0.pdf ;

- Parere dell'11 febbraio 2009 del Gruppo di lavoro articolo 29 (UE) per la protezione dei dati (n. 2/2009) sulla protezione dei dati personali dei minori, (http://ec.europa.eu/justice home/fsj/privacy/docs/wpdocs/2009/wp160_it.pdf);
- Guida del Garante italiano per la protezione dei dati personali "La privacy tra i banchi di scuola", (Roma, 2010) http://www.garanteprivacy.it/garante/ document? ID=1721480;
- Guida dell'Ufficio federale della salute pubblica e dell'Istituto svizzero di prevenzione dell'alcolismo e altre tossicomanie (ISPA) "École et Cannabis", http://www.sfa-ispa.ch/DocUpload/ecole_cannabis.pdf (Berna, 2004);
- Leitfaden Datenschutz für Kindergärten, Schulen und spezielle Schuldienste des Kantons Baselland (Basilea, 2010) www.baselland.ch/fileadmin/baselland/ files/ docs/ jpd/ds/prak/prak-022.pdf;
- Protection des données personnelles dans les écoles du canton de Berne – Lignes directrices (Berna 2009), http://www.jgk.be.ch/jgk/fr/index/aufsicht/datenschutz/ schulen.assetref/content/dam/documents/JGK/DS/fr/DS_Leitfaden-fuer-Datenschutz_fr.pdf;
- Incaricato cantonale della protezione dei dati, Comunicazione di dati personali concernenti allievi e docenti - Criteri generali e raccomandazioni, http://www4.ti.ch/fileadmin/CAN/ICPD/PDF/TEMI/Allievi%20e%20docenti.pdf (Bellinzona, 2002);
- Guida della Cancelleria di Stato "Pubblicare e scaricare da Internet – Qualche riflessione", http://www4.ti.ch/fileadmin/CAN/ICPD/PDF/TEMI/ Pubblicare_e_scaricare da_Internet.pdf;

## 6.2 Basi legali e direttive

- Direttiva del Consiglio informatico della Confederazione (CIC) sulla sicurezza dell'informazione, http://www.isb.admin.ch/themen/sicherheit/00150/00836/index.html? lang=it;
- Direttiva del Consiglio di Stato del 24 ottobre 2006 (n. 5133) per la sicurezza e l'uso di risorse informatiche nell'Amministrazione Cantonale, http://intranet.ti.ch/dipartimenti/

DFE/CSI/SICUREZZA_INFORMATICA/documenti/RG_5133_sicurezza.pdf.

- Legge sulla protezione dei dati personali del 9 marzo 1987 (LPDP; RL 1.6.1.1)
- Legge sulla scuola del 1 febbraio 1990 (Legge scuola; RL 5.1.1.1)
- Legge cantonale sull'ordinamento degli impiegati e dei docenti del 15 marzo 1995 (LORD; RL 2.5.4.1)
- Codice Penale Svizzero (CP; RS 311.0

## 6.3 Abbreviazioni

- Legge sulla scuola: legge sulla scuola del 1° febbraio 1990 (RL 5.1.1.1);
- LPDP: legge sulla protezione dei dati personali del 9 marzo 1987 (RL 1.6.1.1);
- LPD: legge federale sulla protezione dei dati del 19 giugno 1992 (RS 235.1);
- LArch: legge sull'archiviazione e sugli archivi pubblici del 15 marzo 2011 (RL 1.6.2.1);
- LIT: legge sull'informazione e sulla trasparenza dello Stato del 15 marzo (RL 1.6.3.1);
- LORD: Legge cantonale sull'ordinamento degli impiegati e dei docenti del 15 marzo 1995 (RL 2.5.4.1);
- CP: Codice Penale Svizzero del 21 dicembre 1937 (RS 311.0).

## 6.4 Note

[i] www.edoeb.admin.ch

[ii] L'ultima revisione della LPDP prevede ancora soltanto la base legale quale motivo giustificativo per l'elaborazione sistematica di dati (vedi Messaggio governativo n. 7061 del 18 marzo 2005), cioè per elaborazioni effettuate su un periodo prolungato di tempo e tramite un archivio o sistema di gestione di dati personali (banca dati, videosorveglianza, ecc.).

[iii] Ad esempio, presso la Commissione cantonale protezione dei dati.

iv Ogni utente è confrontato con l'uso di più password (posta elettronica, computer, e-banking, tessere bancarie, ecc.). Considerate le oggettive difficoltà di ricordare tutte le password, alcune usate molto raramente, è consigliabile l'uso di appositi programmi che permettano di memorizzarle e proteggerle, ricordando soltanto quella di accesso a tale programma. Lo scopo di un simile accorgimento è quello di evitare che una stessa password venga utilizzata da un utente per diversi servizi compromettendone la confidenzialità.

[v] Gli archivi cartacei sono paragonabili ai server e valgono, di principio, le stesse regole.

[vi] Il sistema elettronico di gestione dei dati sugli scolari è un archivio di dati.

[vii] L'organo scolastico che decide questi parametri del sistema di gestione dei dati personali degli scolari è organo responsabile.

[viii] Gli esempi più classici sono i logfiles degli accessi ad Internet o della posta elettronica.