PRIVACY CONTROL

Privacy & P.A.
Regolamento UE n. 679/2016

NUOVI ADEMPIMENTI PRIVACY & CYBERSECURITY

Dott. Massimo Zampetti
Data Protection Officer

Mail: *info@privacycontrol.it*

© Tutti i diritti riservati.

Introduzione al Reg. Europeo n. 679/2016

- **Pubblicazione** nella Gazzetta Ufficiale dell'Unione Europea n. 119/2016: 4 maggio 2016 (20 giorni di *Vacatio Legis, ndr. 24 maggio 2016)*.
- Entrata in vigore: **24 maggio 2016**.
- Applicabilità in **tutti** i paesi dell'UE: 25 maggio 2018.

Tutti i soggetti interessati (STATI MEMBRI DELL'UNIONE EUROPEA) hanno avuto **DUE ANNI** di tempo per adeguarsi alla nuova normativa tramite la modifica/implementazione delle proprie politiche Nazionali di trattamento dei dati.

Il Regolamento Europeo, per sua natura, è direttamente applicabile senza necessità di recepimento.

Per quanto riguarda **l'Italia**:

- Il Regolamento sostituisce (non integralmente) il D.lgs. n. 196/2003, *Codice in materia di Protezione dei Dati Personali* (c.d. Codice Privacy) in vigore dall'1 gennaio 2004;
- Il D.lgs. n. 196/2003 è stato **INTEGRATO** dal **D.lgs n. 101/2018**, pubblicato in data 4 settembre 2018 ed entrato in vigore in data **19 settembre 2018**. Il nuovo Codice **ABROGA** tutte le disposizioni in contrasto con il Regolamento Europeo n. 679/2016, e rimanda per quasi la totalità degli Articoli ai Considerando e/o Articoli del Regolamento Europeo in materia di Privacy;
- **Il D.lgs n. 101/2018** ha reinserito le **sanzioni penali** non previste dal Regolamento UE; (vedi slides nel Capitolo «Sanzioni»)
- Il Garante Privacy ha in corso una ricognizione normativa per verificare quali provvedimenti generali del garante sopravvivranno alla riforma.

AMBITO DI APPLICABILITÀ MATERIALE

- Si applica solo al trattamento dei dati di **persone fisiche**.

- Riguarda trattamenti **interamente o parzialmente automatizzati** o non automatizzati, se i dati sono contenuti in un archivio o sono destinati a confluirvi.

- Il regolamento **NON** si applica ai trattamenti di dati personali effettuati:
  - Da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o **domestico**;
  - Per attività che non rientrano nell'ambito di applicazione del diritto UE.

Parte GENERALE

1. **NUOVE INFORMAZIONI** per gli interessati (Artt. 12 al 22);
2. **DIMOSTRAZIONE** della «*conformità al GDPR n. 679/16*» (o in inglese, c.d. «*Principio dell'Accountability*»);
3. Nomina di un **R.P.D.** (o in inglese, c.d. Data Protection Officer);
4. **OBBLIGO** di Segnalazione di una **VIOLAZIONE in materia di Dati Personali** (o in inglese c.d. «*Data Breach*»);
5. Accresciuti obblighi **di TRASPARENZA ;**
6. **SANZIONI** più rigide rispetto al «Codice Privacy» (art. 83 e 84).

Parte SPECIALE

1. **Il Garante, la Scuola e la PRIVACY**
2. **CYBERSECURITY**
3. **COVID-19: Le Informative da implementare**
3. **SENTENZE nella Scuola**

1.0 Nuove informazioni per gli interessati

❖I nuovi **Obblighi** nell'informare gli interessati e i nuovi **Diritti** per l'Interessato:

- I nuovi **Obblighi** :
  - Tempi di conservazione dei dati
  - Origine dei dati
  - Diritto alla portabilità dei dati e restrizioni
  - Diritto ad adire l'Autorità di controllo competente (Garante).

- I nuovi **Diritti** :
  - Diritto all'oblio
  - Diritto alla limitazione del trattamento
  - Diritto alla portabilità dei dati (a certe condizioni)
  - Diritto di opporsi a processi di trattamento automatizzati.

1.1 Organigramma – I SOGGETTI (ART. 4)

Il Titolare del trattamento:

- La persona fisica o giuridica che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento di dati personali.

Il Responsabile del trattamento:

- La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta, archivia e conserva **dati personali** per conto del titolare del trattamento:
  - ✓ responsabile interno, solo per le Imprese con settori amministrativi distaccati;
  - ✓ qualsiasi **outsourcers** a cui sono trasferiti i dati (es. Segreteria Digitale, Registro Elettronico, Mensa, Amministratore di sistema, Enti o Associazioni, Agenzie Viaggi, ecc..).

Gli Incaricati del trattamento:

- Tutti coloro che hanno accesso ai dati (es. Ufficio personale, Ufficio alunni, protocollo, Docenti, Coll. Scolastici, ecc..).

Il DATA PROTECTION OFFICER, o Responsabile per la Protezione dei Dati:

- Il DPO (Data Protection Officer) è colui che, in una posizione di indipendenza dal Titolare e dal Responsabile del trattamento, sorveglia il rispetto del Regolamento.
- Potrebbe essere nominato un unico DPO anche da un gruppo di Enti.
- La nomina del DPO deve essere comunicata all'Autorità di controllo (Garante).

Gli Interessati:

- Coloro i cui dati vengono trattati dal titolare e dai responsabili del trattamento.

N.B.: la nuova figura del «**Responsabile per la Protezione dei Dati» personali** (ndr. *Data Protection Officer,* in inglese) è approfondita nel Cap. 3, rispettivamente dalla pag. 20.

1.2 Principali Definizioni Modificate

- **Dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («*interessato*»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
- **Dati personali**:
  - **Comuni**: sono tutti i dati personali diversi da quelli particolari e giudiziari;
  - **Particolari**: sesso, salute, razza, dati biometrici, orientamento politico, filosofico, religioso, sessuale;
  - **Giudiziari**: condanne penali o connesse a delle misure di sicurezza.

1.3 LA PROFILAZIONE

Per Profilazione si intende l'insieme delle **attività di raccolta ed elaborazione dei dati** inerenti agli utenti di un servizio, al fine di suddividerli in gruppi a seconda del loro comportamento (segmentazione).

Art. 4 Reg. UE

*[...] «qualsiasi forma di **trattamento automatizzato** di dati personali consistente nell'utilizzo di tali dati personali per **valutare determinati aspetti personali relativi a una persona fisica**, in particolare per **analizzare o prevedere aspetti** riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica"»[…]*

In linea generale è **vietata**.
L'interessato ha il diritto di NON essere sottoposto una decisione basata unicamente sul trattamento automatizzato, a meno che non vi siano circostanze specifiche, tra le quali il **chiaro consenso informato dell'interessato**.

2. La Responsabilizzazione del Titolare del Trattamento – NUOVI OBBLIGHI – Art. 24 e ss.

Il Regolamento introduce degli **OBBLIGHI** organizzativi nuovi con riferimento ai loro ruoli e funzioni, in particolare per il **Titolare del trattamento**, il quale:

- deve attuare **misure TECNICHE ED ORGANIZZATIVE** (Art. 32 e ss. del GDPR) **ADEGUATE** per «*garantire e dimostrare che il trattamento è effettuato conformemente al Regolamento*». Le misure devono essere riesaminate periodicamente e aggiornate ove necessario.

L'adesione a Codici di condotta o a meccanismi di certificazione, può essere utilizzata come elemento per dimostrare il rispetto degli obblighi imposti al Titolare del trattamento.

MISURE TECNICHE

a. autenticazione/tracciabilità
b. autorizzazione univoca/profilazione
c. cifratura dei dati (es. *sito web e allegati Mail, vedi slides succes.*)
d. separazione dei dati personali
e. firewall/controllo degli accessi/black list/anti spam
f. antivirus
g. sicurezza dei dati cartacei
h. disaster recovery
i. intrusion detection
j. vulnerability assessment/penetration test/monitoraggio delle attività di rete
k. pseudonimizzazione/anonimizzazione dei dati (es. *Password*)
l. backup ridondante
m. politica di archiviazione sostitutiva

Come criptare un file

La crittografia dei file di Windows è disponibile solo nelle edizioni di Microsoft Windows 10 Pro, Education e Enterprise, ma non per Microsoft Windows 10 Home.

1. Come criptare un file PDF

Windows: Acrobat Acrobat PRO oppure si consiglia di utilizzare Libre office (o ancora online Smallpdf.com)

MacOS: cliccare **File** collocato in alto a sinistra e scegli la voce **Stampa**. Dopodiché fai clic sul **menu tendina PDF** che si trova in basso a sinistra, seleziona l'opzione **Salva come PDF** da quest'ultimo e premi sul bottone **Opzioni di sicurezza**, nella nuova finestra che si apre. Per concludere, seleziona l'opzione **Richiedi password** per aprire il documento, digita la **password** che vuoi usare nei campi appositi e **clicca** sui pulsanti **OK** e **Salva**.

2. Come criptare un file/cartella winRAR

Windows: fai clic **destro** sui **file** che desideri includere **nell'archivio RAR** protetto che stai per creare, seleziona la voce **Aggiungi a un archivio** dal menu che compare, clicca sul pulsante **Imposta Parola chiave** nella finestra che ti viene mostrata e **digita**, nei due campi appositi, la **password** con cui vuoi proteggere l'archivio. Premi poi sul bottone **OK**, su quello con su scritto **Sfoglia** per indicare la posizione in cui salvare il file e, per concludere, sul pulsante **Salva**.

Come criptare un file

1. Crittografare file e cartella su Windows

- Con il tasto destro del mouse clicca sul file o sulla cartella che crittografare.
- Seleziona **Proprietà** dal menu di scelta rapida.
- Ora qui nella scheda **Generale** clicca su **Avanzate**.
- Attiva l'opzione **Cripta contenuto per la protezione dei dati**.
- Aspetta che finisca l'elaborazione.

2. Come criptare un file WinZip

Windows: cliccate con il **tasto destro** del **mouse** sul file **ZIP** che desiderate crittografare, selezionate il pulsante "**Proprietà**" dal menu contestuale per aprire le proprietà del file. Nella scheda "**Generale**", fare clic su "**Avanzate**" per aprire la finestra di dialogo "**Attributi avanzati**". Nella finestra di dialogo "**Attributi avanzati**," selezionate la casella di controllo "**Crittografia del contenuto per la protezione dei dati**" e chiudete la finestra di dialogo "Attributi avanzati" cliccando su "**OK**" , **salvate** la modifica delle proprietà del file con "**Applica**" e poi "**OK**". Il file viene visualizzato con un **lucchetto** che indica che il file corrispondente è criptato. Finché **rimanete connessi** con il vostro account utente, **avrete dunque accesso al file**. Agli altri utenti, invece, l'accesso viene negato.

La crittografia dei file di Windows è disponibile solo nelle edizioni di Microsoft Windows 10 Pro, Education e Enterprise, ma non per Microsoft Windows 10 Home.

3. Come criptare un file Word

Windows: apri il file **Word** su cui è tua intenzione intervenire, **Clicca File** situato in alto a sinistra e poi sulla voce **Proteggi documento** presente nel menu che compare. Successivamente, seleziona la voce **Crittografa con password** dal menu per la protezione dei documenti, immetti la **password** che vuoi usare per bloccare il file nella finestra che si apre e **clicca** sul bottone **OK**. Per concludere, **conferma** la **password** scelta digitandola nuovamente.

4. Come criptare un file Excel

Windows: apri il file **Excel** su cui è tua intenzione intervenire, facendo doppio clic su di esso, e, se stai usando Windows, clicca sul pulsante **File** situato in alto a sinistra, dopodiché recati nel menu **Proteggi cartella** di lavoro presente nella schermata successiva e seleziona la voce **Crittografa** con password dal menu che compare. Se non riesci a visualizzare il menu **Proteggi cartella di lavoro**, seleziona la voce **Informazioni** dalla barra laterale di sinistra. Nella finestra che si apre, digita la **password** che vuoi utilizzare per proteggere il tuo file di Excel e **clicca** sul pulsante **OK.** Ripeti la stessa operazione per confermare le impostazioni e il gioco è fatto.

MALWARE

Con il termine **MALWARE** (dalla contrazione delle due parole inglesi “malicious” e “software”, letteralmente “programma maligno” o “codice maligno”) si indica genericamente un qualsiasi software, ovvero un qualsiasi programma, creato con lo scopo di causare danni più o meno gravi ad un computer o a un qualsiasi sistema informatico su cui viene eseguito ed ai dati degli utenti in esso contenuti.

All’interno della **categoria dei malware** esistono una serie di programmi ognuno dei quali agisce con modalità differenti e con obiettivi specifici particolari.

- Virus, **worm** (“vermi” informatici) o **trojan** (“cavalli di Troia”) nonché **spyware**, possono causare la perdita di dati con gravi pregiudizi alla sfera privata;
- **Hoax** o **spam** sono spesso solo fastidiosi, qualora si adottino le appropriate contromisure comportamentali;
- La tecnica del **phishing** può portare alla perdita di informazioni personali estremamente delicate.

VIRUS

Un virus è un programma informatico composto da un numero molto ridotto di istruzioni elementari, specializzato per eseguire soltanto poche e semplici operazioni ed ottimizzato per impiegare il minor numero di risorse, in modo da rendersi il più possibile **invisibile**.

Caratteristica principale di un virus è quella di riprodursi e quindi diffondersi nel computer **ogni volta che viene aperto un file infetto**.

Lo scopo dei virus è quello di creare danni, **fastidi** e **disagi** a chi lo riceve, non ultimo quello della **perdita** totale dei dati o il **furto** di importanti informazioni.

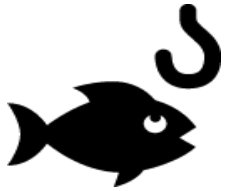
TROJAN (CAVALLI DI TROIA)

I trojan (letteralmente “cavalli di Troia”) sono programmi che eseguono di nascosto operazioni nocive, celandosi all’interno di applicazioni e documenti utili per l'utente.

I trojan sfruttano **lacune di sicurezza** dei programmi utilizzati per aprire i file infetti e installarsi nel sistema ad insaputa dell’utente. Per esempio, potrebbero trovarsi all’interno di brani musicali .mp3 o programmi eseguibili .exe, e sfruttare una qualche vulnerabilità del programma di riproduzione, soprattutto qualora questo non fosse aggiornato all’ultima versione.

Spesso i trojan sono programmi scaricati da internet, altre volte vengono propagati per il tramite di allegati alle email.

PHISHING



La parola phishing deriva dalla contrazione delle parole inglesi "password", "harvesting" (raccolta) e "fishing" (pesca).

Il *phishing* è un **tentativo di truffa**, realizzato solitamente sfruttando la posta elettronica, che ha per scopo il furto di informazioni e dati personali degli utenti.

I mittenti delle **email di** *phishing* sono (o meglio, sembrano essere) organizzazioni conosciute, come banche o portali di servizi web, e hanno apparentemente uno scopo informativo: avvisano di problemi riscontrati con account personali dell'utente (***home banking***, portali di aste online, provider di posta elettronica, social network e altro) e forniscono suggerimenti su come risolvere le problematiche.

Nella stragrande maggioranza dei casi, sarà suggerito di cliccare su qualche link e fornire informazioni e dati personali per ripristinare l'account o metterlo al sicuro. **Nel caso in cui si cliccasse sul collegamento e si fornissero le informazioni richieste, si finirebbe diritti nella *rete* dell'*hacker*-pescatore.**

SPAM

Con “spam” si indicano generalmente tutte le email indesiderate, con un contenuto di vario genere, da quello pubblicitario, a quello più o meno fantasioso ed assurdo, tipico delle catene di sant'Antonio.

Lo “spammer” è il mittente di queste comunicazioni, mentre il fenomeno del loro invio è denominato “spamming”.

Lo spammig porta ad una notevole perdita di tempo da parte di chi riceve il messaggio, anche semplicemente per la sua cancellazione.

MISURE ORGANIZZATIVE

a. nomina per iscritto degli incaricati del trattamento/personale
b. istruzioni/disciplinare tecnico/politiche per il trattamento dei dati personali a tutto il personale
c. accesso controllato
d. armadi chiusi
e. procedura modifica credenziali
f. documentazione/Policy aggiornate
g. formazione di tutto il personale
h. nomina per iscritto dei responsabili esterni
i. gestione delle postazioni da lavoro

3. La nuova figura del Responsabile della Protezione dei Dati personali (R.P.D.)

3.1 Nomina ex artt. 37 – 39 del Reg. UE 679/16

✓ Obbligatorietà

Il R.P.D. (in lingua inglese, *Data Protection Officer, D.P.O.*) dovrà essere **obbligatoriamente** nominato da **tutte le Autorità Pubbliche** od assimilate.

✓ Requisiti

I requisiti del R.P.D. consistono nella **conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati**. Può essere un libero professionista o una società, e può essere nominato un singolo R.P.D. anche da più Enti.

✓ «Indipendenza» e mancanza di «Conflitti di Interesse»

Il R.P.D. dovrà riferire direttamente al **Titolare del Trattamento** o comunque ai vertici gerarchici, senza intermediazioni, con grande **autonomia e indipendenza** rispetto agli altri dirigenti interessati.

3.2 CARATTERISTICHE PRINCIPALI DEL DPO

Il DPO deve essere **AUTONOMO ed INDIPENDENTE:**

- **NON** deve ricevere dal Titolare o dal Responsabile alcuna istruzione per quanto riguarda l'esecuzione dei compiti affidati **né è soggetto a potere disciplinare o sanzionatorio** per l'adempimento dei propri compiti.
- deve avere le risorse necessarie e il **potere di spesa** per assolvere ai compiti assegnati, accedere ai dati personali e ai trattamenti e per mantenere le proprie conoscenze specialistiche (es. aggiornamento professionale).
- Deve fungere da punto di contatto con il **Garante** italiano per la protezione dei dati personali e con gli **interessati**.

3.3 Quali sono i principali compiti del R.P.D.?

Compiti Generali ai sensi dell'Art. 39 del Regolamento UE n. 679/16:

- **Informare, consigliare e FORMARE** il titolare o il responsabile del trattamento, i dipendenti e i quadri, in merito agli obblighi derivanti dal Regolamento (Art. 39 Reg UE);
- **Verificare** l'attuazione e l'applicazione della normativa;
- **Fornire** pareri e consulenza in merito alla valutazione d'impatto (Art. 35) sulla protezione dei dati;
- **Fungere da punto di contatto** per gli "**interessati**", in merito a qualunque problematica connessa al trattamento dei loro dati;
- **Fungere da punto di contatto** per il **Garante** per la Protezione dei Dati Personali.

4. VIOLAZIONE DEI DATI PERSONALI - Data breach (artt. 33 e 34)

Attualmente il Regolamento UE prevede per l'Autorità Pubblica **l'obbligo** di comunicare **l'avvenuta violazione** di dati personali:

- al **Garante** per la protezione dei dati personali;
- in determinati casi, anche al contraente/cliente.

Il Nuovo Regolamento estende tale **OBBLIGO** di comunicazione a **TUTTI i Titolari e Responsabili.**

4.1 Nello specifico, quali sono i compiti e i doveri del Titolare e del Responsabile del Trattamento?

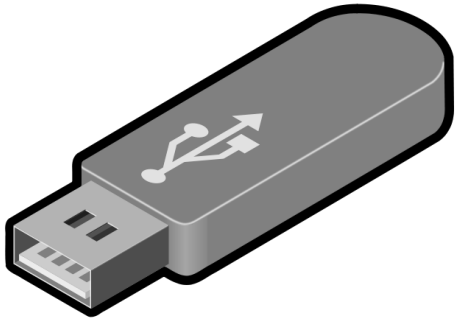
- il **Responsabile/Incaricato** deve informare il Titolare senza ingiustificato ritardo della violazione;
- **Il Titolare** deve notificare «*la violazione*», a sua volta senza ingiustificato ritardo, all'autorità di controllo (i.e., al Garante) e, ove possibile, **entro 72 ore** dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la suesposta violazione presenti un rischio per i diritti e le libertà delle persone.

❖**Domanda:** Quali Sanzioni comporta la mancata segnalazione della violazione?

- **Sanzioni amministrative** fino a **10 milioni di Euro** o fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore.

Esempio di potenziale Data Breach nella Scuola

Una prassi consolidata nella Scuola è utilizzare, per i doveri d'ufficio, **dispositivi d'archiviazione mobili personali**.
Al netto del fatto che difficilmente i dirigenti scolastici hanno **espressamente vietato tale pratica mediante regolamento**, è evidente che **in caso di perdita o furto del dispositivo** o addirittura di danno causato dalla **divulgazione non autorizzata** di quelle immagini, ci si troverebbe in presenza di un data breach.
Se il dispositivo contiene dati **crittografati**, la chiave crittografica è nella **disponibilità** del titolare e questi possiede un **backup**, il data breach **non è lesivo** nei confronti degli interessati e quindi **non notificabile**.
In caso invece la chiave crittografica non sia sicura o non esista un backup dei dati smarriti, **sarà necessario attivare le procedure di notifica e comunicazione individuate**.



Esempio di potenziale Data Breach nella Scuola

Un secondo esempio è connesso alla **creazione di gruppi WhatsApp con i genitori, da parte dei docenti**, per le comunicazioni con le famiglie, in quanto prassi sicuramente funzionale, che tuttavia **non tiene conto di alcuni aspetti**, come il fatto che creare un gruppo significa **condividere numeri telefonici, informazioni di varia natura e spesso immagini dei partecipanti.**

Per via di tutte queste problematiche è sempre indicato usare **strumenti istituzionali per le comunicazioni**, evitando, salvo casi eccezionali, l'utilizzo di strumenti personali e comunque preferendo sempre comunicazioni dirette esclusivamente alla singola persona interessata.

5. ACCRESCIUTI OBBLIGHI DI TRASPARENZA (artt. 5 e 12 Reg. UE)

Il Legislatore europeo dedica una sezione del Nuovo Regolamento alla "**Trasparenza**" (Sezione 1 del Capo III) e **richiede** che le informazioni all'interessato:

- siano rese con un **linguaggio semplice** e chiaro, soprattutto nel caso di minori;
- abbiano sempre **forma scritta**;
- **prevedano:**
  - il **periodo di conservazione** dei dati personali;
  - il diritto di **proporre reclamo** ad un'autorità di controllo;
  - **l'intenzione** del titolare di **trasferire** dati personali a un paese terzo.

5.1 L'informativa

Con l'informativa il responsabile del trattamento deve fornire all'interessato tutte le informazioni e le comunicazioni relative al trattamento dei dati personali in **forma intelligibile**, utilizzando un **linguaggio semplice**, **chiaro** e **adeguato** con riferimento alla condizione dell'interessato, con la particolare attenzione se le informazioni sono destinate ai minori.

Nell'informativa **si deve INDICARE specificamente il diritto di proporre reclamo all'Autorità di controllo**, fornendo le coordinate di contatto della predetta Autorità.

Si dovrà inoltre FORNIRE ogni eventuale informazione ritenuta necessaria al fine di garantire un trattamento equo nei confronti dell'interessato, in relazione alle peculiari circostanze in cui viene effettuata la raccolta dei dati personali.

Domanda: Sono previste Sanzioni in caso di **omessa o inidonea** informativa all'Interessato?

Omessa o inidonea informativa all'interessato:

- **Fino a 20.000.000,00 euro** (rispetto alle condizioni economiche del contravventore).

5.2 Il consenso

Domanda: Quali sono le novità introdotte dal Nuovo Regolamento Europeo?

- Criterio principale di liceità rimane il consenso dell'interessato.
- Il consenso, inteso (art. 4, n. 11) come qualsiasi manifestazione di assenso dell'interessato, **deve** essere **libero, specifico, informato e inequivocabile,** cioè espresso mediante dichiarazione o azione positiva inequivocabile (non può mai essere desunto dal silenzio o da un comportamento inattivo: v. considerando 32).
- Il consenso non dovrebbe costituire il presupposto per un valido trattamento qualora vi sia un "*evidente squilibrio tra interessato e titolare del trattamento*", **soprattutto nei casi in cui quest'ultima sia un'autorità pubblica** o comunque si possa presumere che il consenso non si sia liberamente formato (Considerando 43).
- Il consenso è liberamente revocabile (art. 7, par. 3).

5.3 Consenso Del Minore

Se un trattamento di dati nell'ambito **della fornitura ad un minore di un servizio della società dell'informazione** (es. l'accesso a Internet, l'iscrizione a un social network, etc.) prevede l'acquisizione del consenso preventivo, la **raccolta del consenso e il trattamento dei dati del minore sono leciti se egli abbia compiuto almeno 16 anni** (salvo il diritto degli Stati membri di stabilire anche un'età inferiore a tali fini, purché non inferiore ai 13 anni).

Il Titolare deve adottare **misure ragionevoli per verificare che il consenso sia prestato** o autorizzato dal titolare della potestà genitoriale sul minore.

5.4 La prova del consenso

- È **innovativa** la previsione introdotta dall'art. 7, par. 1:
  - "*qualora il trattamento sia basato sul consenso,* ***il titolare del trattamento DEVE essere in grado di dimostrare che l'interessato ha prestato il proprio consenso*** *al trattamento dei propri dati personali*";
- si pone in capo al **TITOLARE** un vero e proprio **onere della prova** sulla raccolta del consenso;
- AL CONTRARIO nel CODICE PRIVACY D. Lgs. 196/03 non era necessario che il consenso sia documentato per iscritto (v. art. 23, co. 3).

6. IL NUOVO APPARATO SANZIONATORIO

6.1 La tutela dell'interessato e le sanzioni Penali

Art. 167 - Trattamento illecito dei dati personali:

- ⌜ … ⌝ Chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato ⌜ … ⌝ è punito da sei mesi a tre anni

Art. 167 bis - Comunicazione e diffusione illecita di dati oggetto di trattamento su larga scala

- ⌜ … ⌝ Chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso ⌜ … ⌝ è punito con la reclusione da uno a sei anni

Art. 167-ter. Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala

- ⌜ … ⌝ Chiunque acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala ⌜ … ⌝ è punito con la reclusione da uno a quattro anni.

Art. 168 - Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio di poteri del Garante

- ⌜ … ⌝ Chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, ⌜ … ⌝ è punito con la reclusione da sei mesi a tre anni.

Art. 170 - Inosservanza dei provvedimenti del Garante

- ⌜ … ⌝ Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ⌜ … ⌝ è punito con la reclusione da tre mesi a due anni.

6.2 RESPONSABILITÀ CIVILE

Dal punto di vista **civilistico**, confermata la responsabilità risarcitoria per il c.d. "*danno da trattamento*".

L'art. 82 prescrive difatti che "*Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento*".

Chiariti i **meccanismi di ripartizione della responsabilità risarcitoria** tra Titolare e Responsabile del trattamento, e tra contitolari del trattamento (con la previsione specifica di azioni di regresso reciproche), così come i meccanismi di esonero.

6.3 SANZIONI AMMINISTRATIVE

Il Regolamento Europeo ha inasprito l'ammontare delle **sanzioni:**

- **Sanzioni amministrative** fino a **10 milioni di Euro** o fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore;

  (Es. Violazione obblighi in materia di consenso dei minori, misure di sicurezza; Violazione obblighi impartiti dal Titolare; Violazione obblighi di comunicazione per Data Breach);

- **Sanzioni amministrative** fino a **20 milioni di Euro** o fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

  (Es. Violazioni concernenti i diritti degli interessati, i principi cardine del trattamento (es. consenso; trasferimenti dei dati; Violazioni di ordini o misure imposte dall'Autorità).

Le sanzioni amministrative pecuniarie sono inflitte **in aggiunta o in luogo alle sanzioni di cui all'art. 58, par. 2, lett. da a) a h) e j) del Regolamento** (avvertimenti, ammonimenti, ingiunzioni, limitazioni ai trattamenti, ordine di cancellazione, rettifica o limitazioni del trattamento, revoca della certificazione o ingiunzione all'Organismo certificatore di ritirare o non emettere la certificazione, ordine di sospensione dei flussi di dati verso un destinatario).

SANZIONE AMMINISTRATIVA PECUNIARIA	DISPOSIZIONE VIOLATA	OBBLIGO VIOLATO (in sintesi)
Fino a **10.000.000 EUR** o, per le imprese, fino al **2%** del fatturato mondiale totale Annuo dell'esercizio precedente, se superiore.	Art. 8	Verifica che il consenso al trattamento sia prestato o autorizzato dal titolare della responsabilità genitoriale nel caso di offerta diretta di servizi della società dell'informazione a minori di età inferiore a 16 anni.
	Art. 11	Obbligo di non conservazione, acquisizione o trattamento di informazioni per identificare l'interessato se le finalità del trattamento non richiedono più l'identificazione dell'interessato non richiedono o non richiedono più l'identificazione dell'interessato.
	Art. 25	Adozione di misure tecniche e organizzative atte ad attuare i principi di protezione dei dati, la tutela dei diritti degli interessati e la garanzia che siano trattati, per impostazione predefinita, solo i dati necessari per ogni specifica finalità di trattamento (c.d. *privacy by design* e *by default*).
	Art. 28	Designazione del Responsabile del trattamento e rispetto degli obblighi e compiti posti a carico del Responsabile.
	Art. 30	Tenuta dei Registri delle attività di trattamento.
	Art. 32	Adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio.
	Art. 33	Notifica di una violazione dei dati personali all'autorità di controllo.
	Artt. 35 e 36	Svolgimento di una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali e conseguente consultazione preventiva dell'Autorità di controllo.
	Artt. 37 e 39	Prescrizioni in tema di designazione del Responsabile della protezione dei dati (Data Protection Officer).

SANZIONE AMMINISTRATIVA PECUNIARIA	DISPOSIZIONE VIOLATA	OBBLIGO VIOLATO (in sintesi)
Fino a **20.000.000 EUR** o, per le imprese, fino al 4% del fatturato mondiale totale Annuo dell'esercizio precedente, se superiore.	Art. 5	Rispetto dei principi applicabili al trattamento trasparenza; liceità, correttezza e limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
	Art. 6	Rispetto delle condizioni di liceità del trattamento.
	Art. 7	Dimostrazione della prestazione del consenso e del rispetto delle condizioni per il consenso. Tutela del dritto dell'interessato di revoca del consenso.
	Art. 9	Rispetto delle condizioni di liceità del trattamento di categorie particolari di dati personali.
	Artt. da 12 a 22	Obblighi informativi nei confronti dell'interessato. Tutela dei diritti dell'interessato (diritto d'accesso; di rettifica; all'oblio; di limitazione del trattamento; di notifica in caso di rettifica o cancellazione dei dati o limitazione del trattamento; alla portabilità dei dati; di opposizione; alla profilazione consenziente)
	Artt. da 44 a 49	Obblighi connessi al trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali.
	Capo IX	Qualsiasi obbligo previsto dalle legislazioni degli Stati membri per specifiche situazioni di trattamento a norma del Capo IX del Regolamento.
	Art. 58	Rispetto di un ordine, di una limitazione di trattamento o di un ordine di sospensione di flussi di dati dell'Autorità di controllo o di un negato accesso ai sensi dell'art. 58, par. I

PARTE SPECIALE

- IL GARANTE, LA SCUOLA E LA PRIVACY
- CYBERSECURITY
- COVID-19: Le nuove Policy
- SENTENZE nella Scuola

Le Indicazioni del Garante

ISCRIZIONI:
Nell'ambito della scuola pubblica **non è necessario acquisire il consenso** per trattare i dati personali ai fini dell'iscrizione o di altre attività scolastiche. I dati richiesti non possono riguardare informazioni eccedenti e non rilevanti (es. professione dei genitori o stato di salute dei nonni)

TEMI IN CLASSE:
Non lede la normativa privacy l'assegnazione di temi in classe aventi ad oggetto il mondo personale o familiare dell'alunno.
In caso di lettura in classe l'insegnante dovrà trovare il **giusto equilibrio** tra esigenze didattiche e tutela dei dati personali
Restano comunque fermi gli obblighi di **segreto professionale** o d'ufficio e quelli relativi alla conservazione dei dati personali degli alunni contenuti nei temi.

VOTI ED ESAMI:
I voti e gli esiti degli esami sono pubblici. **Tuttavia non possono essere pubblicate informazioni sullo stato di salute degli alunni (per esempio affetti da dsa).** Il riferimento a prove differenziate sostenute da studenti portatori di handicap o con disturbi specifici di apprendimento non va inserito nei tabelloni ma solo nell'attestazione da rilasciare allo studente

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 esempio, gli alunni coinvolti in casi di bullismo o in altre vicende particolarmente delicate

PUBBLICAZIONI:
Gli avvisi messi on line devono avere carattere generale, mentre alle singole persone ci si deve rivolgere con comunicazioni di carattere individuale.
Gli istituti scolastici non possono pubblicare on line, in forma accessibile a chiunque, ad esempio 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 affermando che si sta procedendo per garantire la trasparenza del procedimento.

N.B.: Tale diffusione dei contatti personali incrementa, tra l'altro, il rischio di esporre i lavoratori interessati a forme di stalking o a eventuali furti di identità.

Esempio di Pubblicazione nella Scuola

Un esempio riguarda l'applicazione del D. Lgs. 33/2013 (**Amministrazione Trasparente**) e, in particolare, la **gestione dei CV** degli esperti esterni.
Prima di pubblicare (e quindi diffondere) i CV, il Titolare del trattamento **deve operare un'attenta selezione dei dati in essi contenuti**.

AMMINISTRAZIONE TRASPARENTE
Dlsg. n. 33 del 14 Marzo 2013

Sono **pertinenti** le informazioni riguardanti i titoli di studio e professionali, le esperienze lavorative, nonché ulteriori informazioni di carattere professionale come le conoscenze linguistiche oppure la partecipazione a convegni e seminari, o la redazione di pubblicazioni.
Quello che, invece, **non deve essere pubblicato** sono i **dati eccedenti rispetto alla finalità** quali, ad esempio, i recapiti telefonici o personali, come anche il codice fiscale, in quanto dati forieri di potenziali furti di identità.

DISABILITA' E DISTURBI SPECIFICI DELL'APPRENDIMENTO:

Le istituzioni scolastiche devono prestare particolare attenzione a **NON diffondere**, anche per mero errore materiale, dati idonei a rivelare lo stato di salute degli studenti, così da non incorrere in **sanzioni amministrative o penali**.
Non è consentito, ad esempio, pubblicare on line una **circolare** contenente i **nomi** degli studenti portatori di handicap. Occorre fare attenzione anche a chi ha accesso ai nominativi degli allievi con disturbi specifici dell'apprendimento (DSA), limitandone la conoscenza ai soli soggetti legittimati previsti dalla normativa, ad esempio i professori che devono predisporre il piano didattico personalizzato.

DALLA SCUOLA AL LAVORO:

Su esplicita richiesta degli studenti interessati, le scuole **secondarie** possono comunicare o diffondere, anche a privati e per via telematica, i dati relativi ai loro risultati scolastici e altri dati personali (esclusi quelli sensibili e giudiziari) utili ad 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**.

L'UTILIZZO DELLE IMMAGINI

LE RECITE, LABORATORI didattici e VIAGGI di istruzione:
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 caso di comunicazione sistematica o diffusione diventa infatti necessario, di regola, **ottenere il consenso** informato delle persone presenti nelle fotografie e nei video.

UTILIZZO DELLO SMARTPHONE:
L'utilizzo di telefoni cellulari, di apparecchi per la registrazione di suoni 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 o professori) in particolare della loro immagine e dignità.
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** o comunicare sistematicamente i dati di altre persone (ad esempio pubblicandoli su Internet) senza averle prima informate adeguatamente e averne ottenuto l'esplicito **consenso**.

CYBERSECURITY

-

IL RUOLO DELL'UTENTE

COME PARTE ATTIVA DELL'INSECURITY

Gli attacchi cyber in Italia e nel mondo

Secondo i dati del Rapporto Clusit 2019, presentati al Cyber Security 360 Summit, sono 571 a livello globale gli attacchi di dominio pubblico avvenuti da gennaio a giugno 2019, con un impatto significativo per le vittime, in termini di danno economico, reputazione e diffusione di dati sensibili: il peggiore semestre di sempre, con una crescita costante dal 2011 ad oggi.

- Oltre il 50% delle organizzazioni nel mondo **ha subito almeno un'offensiva grave nell'ultimo anno**. La maggior parte degli attacchi (il 36%) è stata sferrata con **malware** (+86% rispetto al secondo semestre 2016), ma crescono (+85%) anche gli attacchi via **Phishing** e Social Engineering (manipolazione psicologica delle persone che le induce a compiere determinate azioni o a divulgare informazioni riservate).

- In riferimento al mondo Scuola il **MIUR** ha pubblicato un documento nel maggio 2018 in cui si evidenzia come l'azione amministrativa sia caratterizzata da una gestione che in alcuni casi **digitale in ogni suo passaggio**. Per tale motivo il tema della **sicurezza informatica** riveste un'importanza **fondamentale e strategica**. La perdita di dati e di informazioni, l'aumento costante di violazioni ai sistemi informatici rende necessaria una RINNOVATA RESPONSABILIZZAZIONE degli attori principali del trattamento dei dati personali.

La situazione in tempo reale -> https://livethreatmap.radware.com

La sicurezza informatica in Italia e l'obbligo per la PA, di consultare il Cert-PA

AgID e il CERT-PA (**Computer Emercency Response Team**)

- **AgID** ha il compito di definire raccomandazioni, strategie, norme tecniche per sensibilizzare e informare le amministrazioni sui temi della sicurezza e delle emergenze ad essa collegate.
- **AgID** svolge un ruolo significativo nella tutela della sicurezza nazionale in ambito sicurezza cibernetica e nella prevenzione e gestione degli incidenti di sicurezza informatica nella pubblica amministrazione.
- **CERT-PA** opera all'interno di AgID e ha il compito di supportare le amministrazioni nella **prevenzione** e nella **risposta** agli incidenti di sicurezza informatica:

  - Servizi di **analisi e di indirizzo**, finalizzati a supportare la gestione della sicurezza
  - Servizi **proattivi**, relativi alla raccolta e all'elaborazione di dati significativi
  - Servizi **reattivi**, per poter gestire gli allarmi di sicurezza
  - Servizi di **formazione** e comunicazione per promuovere la cultura della sicurezza cibernetica

Il pericolo oggi si chiama RANSOMWARE

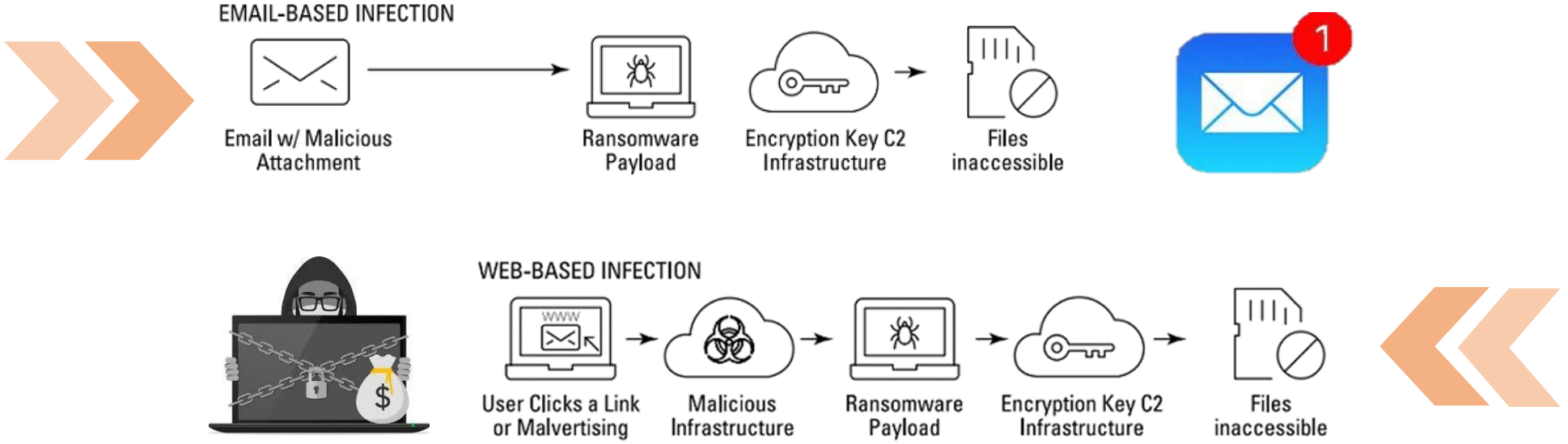
Ransomware: è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un **RISCATTO** (ransom in inglese) da pagare per rimuovere la limitazione.

E' in grado di **BLOCCARE** il funzionamento del computer, facendo sì che l'utente NON riesca a effettuare il login nel suo profilo utente (mostrando, solitamente, un AVVISO dell'FBI o della Polizia di Stato) o utilizzando la **crittografia** per rendere **illeggibili** i file presenti all'interno del disco rigido (questi ransomware sono chiamati cryptolocker). **WannaCry** per esempio, appartiene proprio a questa seconda categoria.

(WannaCry)

I Ransomware preferiscono le email pur essendo presenti anche nel web

Al primo posto, tra le tipologie di malware trasmesse per email, si trovano i ransomware. Secondo l'azienda di cybersecurity Proofpoint, il virus del riscatto è stato trovato nel **68% dei messaggi di posta elettronica** contenenti una qualsiasi forma di programma malevolo.



I punti deboli sfruttati da Malware e Ransomware

- **Vulnerabilità software dei sistemi**: aspetti del sistema per i quali le misure di sicurezza non sono adeguate o sono compromesse e di conseguenza più facilmente attaccabili.
- **Formazione degli utenti**: Virus e truffe online Il 74% degli utenti non ha le competenze necessarie per riconoscere i pericoli online. A rivelarlo è un test realizzato da Kaspersky Lab sulle abitudini di 18.000 utenti.
- **Comportamenti non appropriati** degli utenti: ad esempio apertura di allegati sospetti per disattenzione e/o curiosità.

Come difendersi?

- **Leggere sempre con attenzione** i messaggi visualizzati nel PC e in particolare durante la navigazione, prima di cliccare su SI.
- È fondamentale ai fini della sicurezza scaricare gli **aggiornamenti** del **software** (software update, chiamate anche "patch"), perché consentono di colmare le falle di sicurezza che vengono scoperte quasi quotidianamente, le cosiddette vulnerabilità del Sistema; è consigliabile programmare gli aggiornamenti in automatico.
- In caso di problemi o difficoltà, è consigliabile rivolgersi a ditte specializzate.

Verificare l'installazione del programma antivirus e tenerlo aggiornato

- Un **software antivirus** aggiornato è assolutamente indispensabile.
- Dato che giornalmente nascono numerosi nuovi malware, è tassativamente indispensabile anche un **aggiornamento frequente** del software antivirus.
- La maggior parte dei prodotti dispongono di funzioni automatiche di aggiornamento che devono essere assolutamente attivate.

Cosa non fare

- NON aprire **chiavette USB** sulla propria postazione di lavoro, magari per caricare il file di un collega.
- NON scaricare **programmi da internet** se non con l'assistenza di una persona esperta e solo dopo aver verificato l'attivazione dell'antivirus e il suo aggiornamento; accertarsi di essere sul sito del produttore del software.
- NON scaricare programmi **sconosciuti**.
- NON scaricare musica, film, file con estensioni: **zip, exe**, bat, dll o non conosciute.
- NON navigare sui social e/o su siti **non conosciuti**.

Attenzione alle email

- Usare **prudenza nella apertura di email con mittente ignoto;**
- **Diffidare delle email di cui non si conosce l'indirizzo del mittente**; in questo caso non aprire mai gli allegati o i programmi ivi contenuti, né selezionare i link indicati;
- Aprire unicamente i file o i programmi provenienti da **fonti affidabili** e solo previa verifica con un programma antivirus aggiornato;
- **Diffidare dei file con due estensioni:** non aprire mai gli allegati di email provvisti di due estensioni (ad es. picture.bmp.vbs o pdf.exe) e non lasciarsi ingannare dall'icona di simili file; disattivare nelle opzioni del browser, dove presente, l'opzione "nascondi le estensioni per i tipi di file conosciuti; i file firmati possono presentare due estensioni, ad es. .pdf.p7m, accertarsi comunque della fonte prima di aprirli.

Attenzione alle email

- **Non rispondere alle spam**: rispondere ad un messaggio di spam equivale ad informare lo spammer che **l'indirizzo email è valido e quindi questi invierà ulteriori spam** oppure metterà il vostro indirizzo a disposizione di altri spammer; particolare attenzione va portata agli spam con l'opzione di "cancellazione dall'elenco" in cui si promette la cancellazione dall'elenco di distribuzione tramite l'invio di un'email con un determinato contenuto.
- **Controllare l'indirizzo del mittente**: passare sempre il mouse sopra l'indirizzo: apparirà un collegamento ipertestuale; è importante che il link visualizzato dopo il passaggio con il mouse resti identico, altrimenti molto probabilmente si tratta di un tentativo di truffa con un indirizzo fasullo.
- **Verificare sempre la validità di un indirizzo o di un link ricevuto via e-mail**: a volte gli indirizzi cambiano di poco (anche per una sola una vocale o consonante diversa); altre volte vengono aggiunte delle parti all'apparenza non dubbie, ma che poi rimandano a siti ingannevoli.

Attenzione alle email

- **Prestare attenzione alla grammatica e all'ortografia**: spesso chi crea una campagna di phishing non proviene dall'Italia; è probabile che il messaggio ricevuto presenti una URL all'apparenza valida e anche il nome del mittente ricordi quello della nostra banca, di un'azienda o di un amico ma se il testo presenta errori nei tempi verbali, negli accenti, o nella costruzione della frase , è molto probabile che si tratti di una truffa, questo perché il testo è stato quasi certamente tradotto da un'altra lingua.
- **Diffidare delle email scritte in inglese** provenienti da mittenti sconosciuti.
- **Diffidare delle offerte irrifiutabili**: quando una cosa sembra troppo bella per essere vera, molto probabilmente non è vera. Se riceviamo un messaggio da un utente sconosciuto che ci promette a prezzi stracciati smartphone, tablet o accessori hi-tech, vincite alla lotteria …. si tratta di una truffa.
- **Diffidare anche delle email di offerte** che assomigliano a quelle che si ricevono solitamente da siti e-commerce.

Attenzione alle email

- **Diffidare di email apparentemente provenienti da enti governativi o pubblici**: i cyber criminali a volte fingono di essere un'istituzione; è bene ricordare, che i vari enti non utilizzano la posta elettronica per certi tipi di comunicazioni; ad esempio, è improbabile che il Comune o altre istituzioni ci scrivano via email per chiederci dei soldi o informazioni riservate e che l'Agenzia delle Entrate mandi alla scuola un accertamento fiscale via email.
- **Non aprire mai allegati tipo fattura elettronica**: la scuola riceve solo fatture elettroniche via SIDI; se si consce il fornitore contattarlo al telefono.

Come intervenire?

La sicurezza dei dati personali degli utenti dipende principalmente **dall'attenzione degli operatori**.

In caso di infezione:

1. spegnere il PC;
2. staccarlo dalla rete, e
3. se connesso via cavo, rivolgersi al personale tecnico della scuola o chiamare l'assistenza.

Trattamento dati nel contesto SCOLASTICO nell'ambito dell'emergenza sanitaria

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

COVID-19
e protezione
dei dati personali

FAQ

1) Gli Istituti scolastici devono INFORMARE gli interessati in merito ai trattamenti dei dati personali effettuati nelle attività di didattica a distanza?

Sì. Gli istituti scolastici sono tenuti ad assicurare la **trasparenza** del trattamento informando, con un linguaggio facilmente comprensibile anche dai minori, gli interessati (alunni, studenti, genitori e docenti) in merito, in particolare, ai:

- tipi di dati e alle modalità di trattamento degli stessi,
- ai tempi di conservazione e
- alle altre operazioni di trattamento,

specificando che le **finalità perseguite sono limitate esclusivamente all'erogazione della didattica a distanza**, sulla base dei medesimi presupposti e con garanzie analoghe a quelli della didattica tradizionale.

Nota 17 marzo 2020 – M.I.U.R.
«Prime indicazioni operative per le attività didattiche a distanza»

Ministero dell'Istruzione

Dipartimento per il sistema educativo di istruzione e di formazione

La questione *privacy*

Occorre subito precisare che le istituzioni scolastiche non devono richiedere il consenso per effettuare il trattamento dei dati personali (già rilasciato al momento dell'iscrizione) connessi allo svolgimento del loro compito istituzionale, quale la didattica, sia pure in modalità "virtuale" e non nell'ambiente fisico della classe, è.

Le istituzioni scolastiche sono invece tenute, qualora non lo abbiano già fatto, ad informare gli interessati del trattamento secondo quanto previsto dagli artt. 13 e 14 del Regolamento UE 2016/679 e:

- a garantire che i dati personali siano trattati in modo lecito, corretto e trasparente, che siano raccolti per finalità determinate, esplicite e legittime, che siano trattati in modo non incompatibile con tali finalità, evitando qualsiasi forma di profilazione, nonché di diffusione e comunicazione dei dati personali raccolti a tal fine, che essi siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati, e trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
- a stipulare contratti o atti di individuazione del responsabile del trattamento ai sensi dell'articolo 28 del Regolamento, che per conto delle stesse tratta i dati personali necessari per l'attivazione della modalità didattica a distanza;
- a sottoporre i trattamenti dei dati personali coinvolti a valutazione di impatto ai sensi dell'articolo 35 del regolamento.

Individuazione della base giuridica del trattamento: svolgimento del compito istituzionale, quale la didattica, sia pure in modalità "virtuale" e non nell'ambiente fisico della classe.

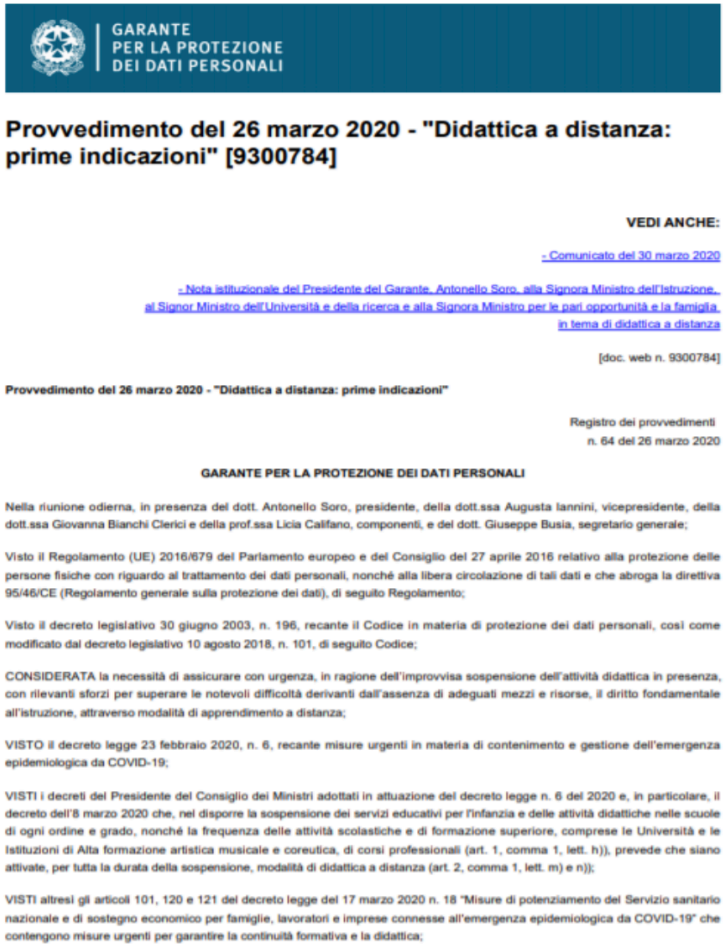
Sono escluse le richieste di consenso per la finalità didattica:

► **Obblighi di informativa** ex artt. 13 e 14 del Regolamento UE 2016/679 (GDPR);

► **Stipula di contratti o atti di individuazione** del responsabile del trattamento ex articolo 28 del GDPR, il quale tratta i dati personali necessari per l'attivazione della modalità didattica a distanza per conto delle istituzioni scolastiche;

► Sottoporre i trattamenti dei dati personali coinvolti a **Valutazione di impatto privacy** ex articolo 35 del GDPR
(Data Privacy Impact Assessment o «DPIA»)

Provvedimento Autorità Garante per la protezione dei dati personali
Provvedimento n. 64 del 26 marzo 2020 «Didattica a distanza: prime indicazioni»



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Provvedimento del 26 marzo 2020 - "Didattica a distanza: prime indicazioni" [9300784]

VEDI ANCHE:

- Comunicato del 30 marzo 2020

- Nota istituzionale del Presidente del Garante, Antonello Soro, alla Signora Ministro dell'Istruzione, al Signor Ministro dell'Università e della ricerca e alla Signora Ministro per le pari opportunità e la famiglia in tema di didattica a distanza

[doc. web n. 9300784]

Provvedimento del 26 marzo 2020 - "Didattica a distanza: prime indicazioni"

Registro dei provvedimenti
n. 64 del 26 marzo 2020

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

Visto il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati), di seguito Regolamento;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali, così come modificato dal decreto legislativo 10 agosto 2018, n. 101, di seguito Codice;

CONSIDERATA la necessità di assicurare con urgenza, in ragione dell'improvvisa sospensione dell'attività didattica in presenza, con rilevanti sforzi per superare le notevoli difficoltà derivanti dall'assenza di adeguati mezzi e risorse, il diritto fondamentale all'istruzione, attraverso modalità di apprendimento a distanza;

VISTO il decreto legge 23 febbraio 2020, n. 6, recante misure urgenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19;

VISTI i decreti del Presidente del Consiglio dei Ministri adottati in attuazione del decreto legge n. 6 del 2020 e, in particolare, il decreto dell'8 marzo 2020 che, nel disporre la sospensione dei servizi educativi per l'infanzia e delle attività didattiche nelle scuole di ogni ordine e grado, nonché la frequenza delle attività scolastiche e di formazione superiore, comprese le Università e le Istituzioni di Alta formazione artistica musicale e coreutica, di corsi professionali (art. 1, comma 1, lett. h)), prevede che siano attivate, per tutta la durata della sospensione, modalità di didattica a distanza (art. 2, comma 1, lett. m) e n));

VISTI altresì gli articoli 101, 120 e 121 del decreto legge del 17 marzo 2020 n. 18 "Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19" che contengono misure urgenti per garantire la continuità formativa e la didattica;

► **Base giuridica** del trattamento dei dati personali;
► Privacy by design e by default: **scelta e configurazione degli strumenti** da utilizzare;
► Il **ruolo dei fornitori** dei servizi on line e delle piattaforme;
► **Limitazione** delle finalità del trattamento;
► **Liceità**, **correttezza** e **trasparenza** del trattamento.

Provvedimento Autorità Garante per la protezione dei dati personali Provvedimento n. 64 del 26 marzo 2020 «Didattica a distanza: prime indicazioni»

Inoltre, nella Nota istituzionale del Presidente del Garante, Antonello Soro, alla Signora Ministro dell'Istruzione, al Signor Ministro dell'Università e della ricerca e alla Signora Ministro per le pari opportunità e la famiglia in tema di didattica a distanza

«le straordinarie potenzialità del digitale […] non devono, però, indurci a sottovalutare anche i **rischi, suscettibili di derivare dal ricorso a un uso scorretto o poco consapevole degli strumenti telematici, spesso dovuto anche alla loro oggettiva complessità di funzionamento**. […]

Molte delle piattaforme suscettibili di utilizzo a fini didattici, ad esempio, funzionano come veri e propri social network che necessitano, come tali, di una sia pur minima cognizione delle loro regole di utilizzo e delle implicazioni di ciascun "click", anche tra l'altro sui diritti della personalità di terzi. […]

La corretta gestione dei dati personali di tutti i soggetti coinvolti, a vario titolo, nell'attività didattica a distanza rappresenta, in questo senso, **il presupposto quantomai indispensabile per rendere il digitale una risorsa straordinaria per la promozione dei diritti** (quello allo studio, in particolare), al riparo da rischi di abusi o violazioni. […]»

FIGURE CHIAVE NELLA DAD

Titolare del Trattamento	La **persona fisica o giuridica**, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
Data Protection Officer	**Assicura l'applicazione del quadro normativo** vigente in materia di protezione dei dati personali, nell'ambito dei trattamenti svolti dal Titolare del trattamento.
Presidi Privacy	E' possibile **identificare Presìdi** - all'interno della struttura del Titolare del trattamento, se particolarmente articolata - per svolgimento degli adempimenti privacy relativi a ciascuna area.
Persone autorizzate al trattamento	Il personale che **effettua operazioni di trattamento** sui dati personali sotto l'autorità del Titolare del trattamento e sulla base di istruzioni fornite dallo stesso.
Responsabili del trattamento	**Soggetti terzi che trattano dati personali** per conto del Titolare, mettendo in atto misure di sicurezza adeguate di tipo tecnico ed organizzativo.

Il SUPPORTO del Data Protection Officer

► La nomina del DPO è **obbligatoria** per le Pubbliche Amministrazioni. Il rapporto con il Titolare sarà disciplinato da un **contratto di servizi**.

► Deve operare sempre in **assenza di conflitti di interesse**.

► Per eseguire i suoi compiti necessita di un **sostegno adeguato in termini di risorse finanziarie e umane**. Il DPO garantisce che tutti gli elementi del suo team siano in possesso dei requisiti professionali richiesti dalla normativa.

► Ha competenze trasversali e adeguate in ambito **privacy**, **information security** e **conoscenza dei processi della realtà del Titolare** (la Scuola).

Nel contesto DAD, quale SUPPORTO può dare il DPO al TITOLARE del trattamento (nella persona del Dirigente scolastico)?

1. **Promuove la cultura della privacy nella realtà del Titolare**: attività di sensibilizzazione e formazione del personale docente in merito alla tutela dei dati personali nel contesto della DAD.
2. **Informa e consiglia il Titolare del trattamento, nonché i dipendenti, in merito agli obblighi della normativa applicabile**: consulenza costante al Dirigente Scolastico e al personale docente.
3. **Verifica che la normativa vigente e la documentazione privacy adottata dal Titolare siano correttamente attuate e applicate**: supporto al Dirigente Scolastico in merito al monitoraggio della normativa, anche mediante attività di pareristica e consulenza.
4. **Funge da punto di contatto con l'Autorità Garante per la protezione dei dati personali e con gli interessati**: cura un dialogo aperto con il personale docente e le famiglie degli studenti.

PERCHÉ È NECESSARIO VALUTARE L'IMPATTO PRIVACY?

- **Immagini e webcam**

L'utilizzo della webcam ai fini della videoconferenza **potrebbe non essere sempre necessario**. I partecipanti dovrebbero essere in grado di autorizzare o meno il funzionamento della webcam per mostrare o meno la propria immagine. Anche il docente è libero di mostrare o meno la propria immagine.

- **Creazione di account**

La creazione di una classe virtuale con strumenti dedicati (es. **G Suite Classroom** o Microsoft Teams) consente di poter accedere a impostazioni di sicurezza, regolare gli accessi, creare o disabilitare in ogni momento le classi virtuali.

- **Si possono registrare le lezioni?**

La scuola **dovrebbe chiedersi se desidera registrare o meno le lezioni** e se metterle a disposizione degli studenti, **magari utilizzando uno storage cloud** (es. Google Drive).
In tale caso, gli interessati dovrebbero essere informati di tale eventualità e dovrebbe essere precisato per quanto tempo verranno conservate le registrazioni.

- **Utilizzo degli account aziendali da parte degli studenti**

La **creazione di account** o indirizzi di posta elettronica aziendali in capo agli studenti dovrebbe essere regolato mediante misure tecniche che **consentano di limitare alcune operazioni** (es. Impedire l'invio e ricezione di messaggi al di fuori dell'organizzazione o del gruppo classe), coinvolgendo i genitori.

QUALI SONO I PUNTI CRITICI?

- **Minimizzazione**

Si dovranno attivare, di default, i soli servizi strettamente necessari alla formazione, configurandoli in modo da minimizzare i dati personali da trattare, sia in fase di attivazione dei servizi, sia durante l'utilizzo degli stessi da parte di docenti e studenti (**evitando, ad esempio, il ricorso a dati sulla geolocalizzazione**, ovvero a sistemi di social login che, coinvolgendo soggetti terzi, comportano maggiori rischi e responsabilità).

- **Serve acquisire il consenso?**

L'erogazione di servizi di **didattica a distanza** rientra nell'esecuzione del rapporto contrattuale e delle funzioni istituzionali , ma alcune funzionalità (es. Immagine tramite webcam) possono richiedere il consenso degli interessati.
Secondo il **Garante privacy**, **NON** deve pertanto essere richiesto agli interessati (docenti, alunni, studenti, genitori) **uno specifico consenso** al trattamento dei propri dati personali funzionali allo svolgimento dell'attività didattica a distanza.

- **Contratto con le piattaforme**

L'art. 28 GDPR richiede che tali soggetti sottoscrivano un contratto per garantire standard adeguati di sicurezza nei confronti del titolare del trattamento.

2) La scuola può comunicare alle famiglie degli alunni l'identità dei parenti di studenti risultati positivi al COVID 19?

Spetta alle autorità sanitarie competenti informare i contatti stretti del contagiato, al fine di attivare le previste misure di profilassi.

L'istituto scolastico è tenuto a fornire alle istituzioni competenti, le informazioni necessarie, affinché le stesse possano ricostruire la filiera dei contatti del contagiato, nonché, sotto altro profilo, ad attivare le misure di sanificazione recentemente disposte.

3) Si devono registrare le autodichiarazioni all'ingresso?

La scuola dovrebbe chiedere all'entrata dell'edificio di consegnare un **autodichiarazione** sul modello indicato dal **Protocollo** istituito dal **Ministro dell'Istruzione**.

Per **semplificare** le procedure, gli interessati potrebbero firmare un **Registro degli accessi** firmando per presa visione l'autodichiarazione sopra citata appesa all'ingresso della scuola.

L'interessato dichiara quanto segue:
- di non presentare sintomatologia respiratoria o febbre superiore a 37.5° C in data odierna e nei tre giorni precedenti;
- di non essere stato in quarantena o isolamento domiciliare negli ultimi 14 giorni;
- di non essere stato a contatto con persone positive, per quanto di loro conoscenza, negli ultimi 14 giorni.

ALLEGATO 2

AUTODICHIARAZIONE

Il sottoscritto,

Cognome ..... Nome .....

Luogo di nascita ..... Data di nascita .....

Documento di riconoscimento .....

Ruolo..... (es. studente, docente, personale non docente, altro)

nell'accesso presso Istituto Scolastico .....
sotto la propria responsabilità (se maggiorenne) o di quella di un esercente la responsabilità genitoriale, dichiara quanto segue:

- di non presentare sintomatologia respiratoria o febbre superiore a 37.5° C in data odierna e nei tre giorni precedenti;
- di non essere stato in quarantena o isolamento domiciliare negli ultimi 14 giorni;
- di non essere stato a contatto con persone positive, per quanto di loro conoscenza, negli ultimi 14 giorni.

La presente autodichiarazione viene rilasciata quale misura di prevenzione correlata con l'emergenza pandemica del SARS CoV 2.

Luogo e data .....

Firma leggibile
(dell'interessato e/o dell'esercente la responsabilità genitoriale)

.....

4) Si deve misurare la temperatura quando visitatori, fornitori e dipendenti si presentano all'ingresso della scuola?

La febbre, se presente dovrà essere autodichiarata.

Non ci sarà la misurazione della febbre all'ingresso delle scuole anche in occasione degli esami di maturità, come invece si pensava.

In caso di temperatura superiore a 37,5 gradi o di sintomi di patologie respiratoria il candidato**, i docenti o il resto del personale dovrà segnalarlo nell'apposito modulo di autodichiarazione**.

SENTENZE nella Scuola

Corte dei conti
Sez. giurisd. per il Lazio 28/5/2019 n. 246

- La sezione giurisdizionale per il Lazio della Corte dei Conti, con la sentenza 246 del 28 maggio, ha condannato un Dirigente Scolastico per aver **autorizzato** la PUBBLICAZIONE di una **circolare sul sito della scuola, contenente dati sensibili relativi allo stato di salute di studenti con disabilità**.

- La circolare andava invece **indirizzata ai soli genitori degli studenti**. E' il Codice della privacy che contiene le norme relative al trattamento dei dati sensibili, sia riguardo alle autorizzazioni degli interessati, sia al tipo di dati da trattare, sia le operazioni che si possono eseguire con quei dati.

Corte dei conti
Sez. giurisd. per il Lazio 28/5/2019 n. 246

- E' sempre **vietato diffondere lo stato di salute** o qualsiasi informazione collegata, anche indirettamente, allo stato di malattia o l'esistenza di patologie dei soggetti interessati e alle condizioni di invalidità, disabilità, o handicap fisici e/o psichici.
- La Corte ha inoltre stabilito che **nessuna colpa può essere addossata a chi ha scritto e pubblicato manualmente la circolare**, in quanto la responsabilità di verificare la correttezza e la legittimità di una circolare è solo del dirigente scolastico e non può essere estesa ai docenti coinvolti nella stesura e nella pubblicazione.

La sentenza del 2019 della Corte dei Conti

Quest'ultima, dopo ben quattro anni con sentenza del 28 maggio 2019, ha condannato **IL DIRIGENTE** a rifondere personalmente alla scuola 7.500 euro.

I giudici hanno infatti riscontrato che egli, **non avendo prescritto alcun divieto di pubblicazione** né controllato che la circolare non venisse pubblicata sul sito web dell'istituto, ha manifestato un **comportamento gravemente negligente**.

La pubblicazione di dati personali su internet senza il consenso dei diretti interessati o altra base giuridica, **comporta** la divulgazione a soggetti terzi delle informazioni, e conseguentemente **un trattamento illecito**.

Il Garante ricorda inoltre come i **dati riguardanti la salute** vadano **trattati con estrema cautela**, rispettando specifiche norme di legge e verificando non solo la pertinenza e la completezza delle informazioni, ma anche la loro indispensabilità rispetto alle "finalità di rilevante interesse pubblico" che si intendono perseguire.

La diffusione dei dati sulle condizioni di salute dei minori si riflettono inoltre sui genitori/tutori, i quali potrebbero essere esposti a condizionamenti o discriminazioni da parte di soggetti terzi.

Foto minori nel Web, una buona notizia dal "Sole24 ore

Si legge "*Solo la liberatoria firmata dai genitori salva il DOCENTE di un liceo classico romano sanzionato per aver realizzato un calendario con gli studenti nell'ambito di un progetto promosso dalla scuola, che però aveva irrogato al prof la censura per aver raccolto i dati degli alunni minori di propria iniziativa*».

In questo caso il tribunale ha **ACCOLTO** il **ricorso del docente** che aveva appunto fatto sottoscrivere la liberatoria ai genitori insieme all'informativa privacy (Trib. di Roma, sentenza del 28/02/2019 n. 2007).

Bisogna **sempre ottenere il consenso esplicito** del genitore o dell'alunno maggiorenne. Indicazione ripresa dal GDPR (25 maggio 2018) e dal D. Lgs. n. 101/08, ad integrazione del D. Lgs. n. 196/03.

Grazie per l'attenzione!

Dott. Massimo Zampetti

Data Protection Officer

info@privacycontrol.it

© 2018 Privacycert Lombardia S.r.l. – Tutti i dritti riservati. Ferme restando le utilizzazioni libere consentite dalle leggi vigenti, in mancanza di un espressa autorizzazione scritta di Privacycert Lombardia S.r.l. è vietata qualunque riproduzione, utilizzazione o qualunque altra forma di messa a disposizione di terzi del presente documento o di una parte di essi.