GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

LA SCUOLA A PROVA DI PRIVACY: ISTRUZIONI PER L'USO

10 marzo 2023
Firenze

Claudio Filippi
Vice Segretario generale
Dirigente del Dipartimento realtà pubbliche
Dirigente del Dipartimento sanità e ricerca

PREMESSA

“Se proteggi i tuoi dati proteggi stesso”
essere consapevoli del “valore privacy”.

Il fenomeno del revenge porn è in forte espansione. Si sostanzia nella diffusione illecita, non consensuale, attraverso i social media, di foto e video sessualmente o pornograficamente rilevanti, scattati nell’intimità di una esperienza relazionale e destinati a rimanere privati.

La vittima sottoposta a una gogna mediatica può essere condotta, a fronte di una sofferenza psichica, in alcuni casi ingestibile, anche a scelte estreme.

Il Revenge porn è diventato in Italia r**eato punibile con la reclusione da uno a sei anni e con la multa da euro 5mila a euro 15mila**. Resta però, purtroppo, ancora abbastanza nebuloso il panorama degli specifici strumenti di tutela a favore della vittima.

Oggi, chi teme di essere vittima di revenge porn può rivolgersi al Garante.

La tutela emergenziale a carattere preventivo per il revenge porn

Il Garante ha messo a disposizione una procedura di segnalazione quale forma di **tutela emergenziale a carattere preventivo**.

Le persone maggiorenni che temono che le loro foto o i loro video intimi possano essere diffusi senza il loro consenso **su Facebook o Instagram**, potranno segnalare al Garante tale rischio e ottenere che le immagini vengano bloccate.

La procedura è semplice e strettamente confidenziale con un form sulla pagina www.gpdp.it/temi/revengeporn.

Il Garante, raccolti gli elementi necessari, indicherà alla persona interessata il link per caricare direttamente le immagini di cui essa teme la diffusione proprio al fine di interdirne la diffusione.

Una volta caricate, le immagini verranno cifrate tramite un codice, cosiddetto "hash", in modo da diventare irriconoscibili prima di essere distrutte e, attraverso una tecnologia di comparazione, bloccate da possibili tentativi di una loro pubblicazione sulle due piattaforme.

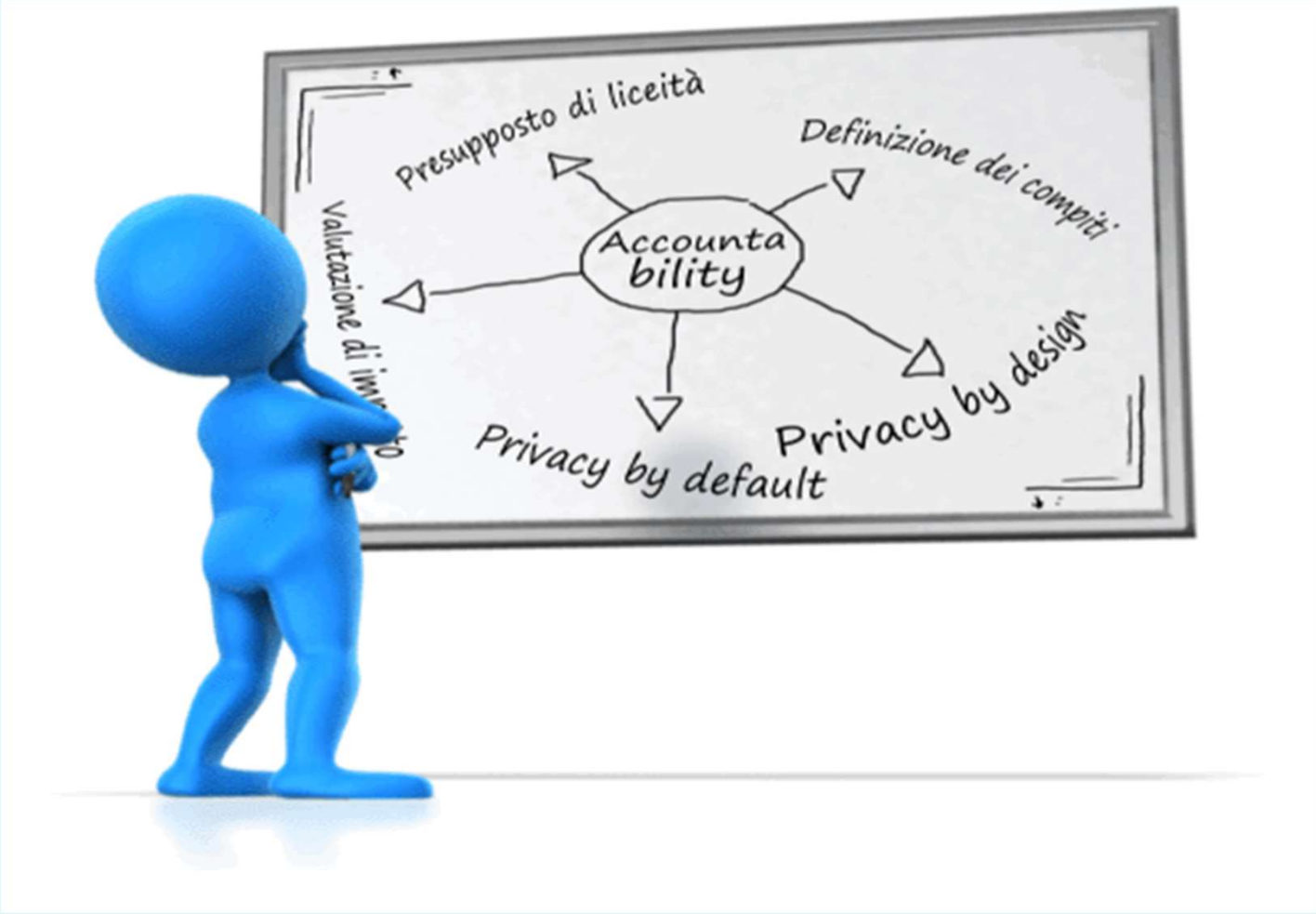
QUESTIONE DI ACCOUNTABILITY

LA «RESPONSABILIZZAZIONE» DEL TITOLARE

La principale novità introdotta dal regolamento europeo è il principio di "***responsabilizzazione***" (cd. ***accountability***)

Si **attribuisce direttamente ai titolari** del trattamento il compito di **assicurare**, ed essere in grado di **comprovare**, il rispetto dei principi applicabili al trattamento dei dati personali (art. 5).

Necessità di un approccio sistemico

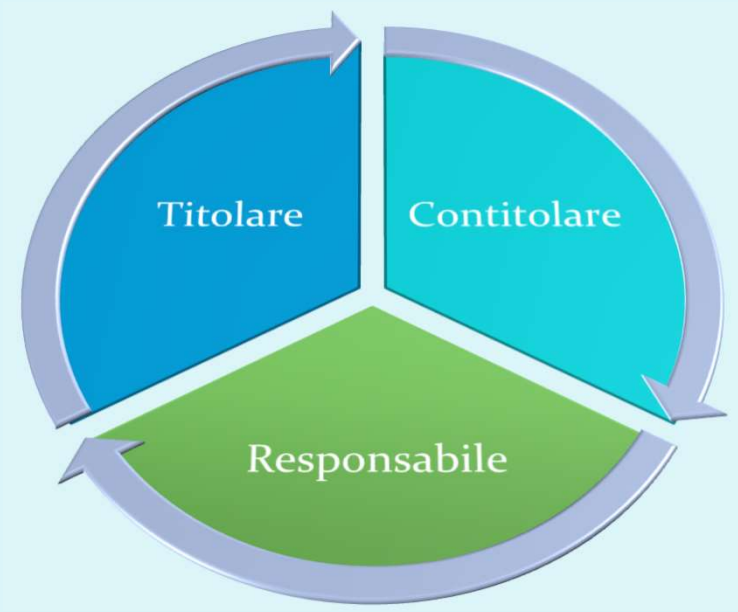


I PRINCIPI ALLA BASE DELLA RESPONSABILIZZAZIONE (art. 5 Gdpr)

I dati devono essere:

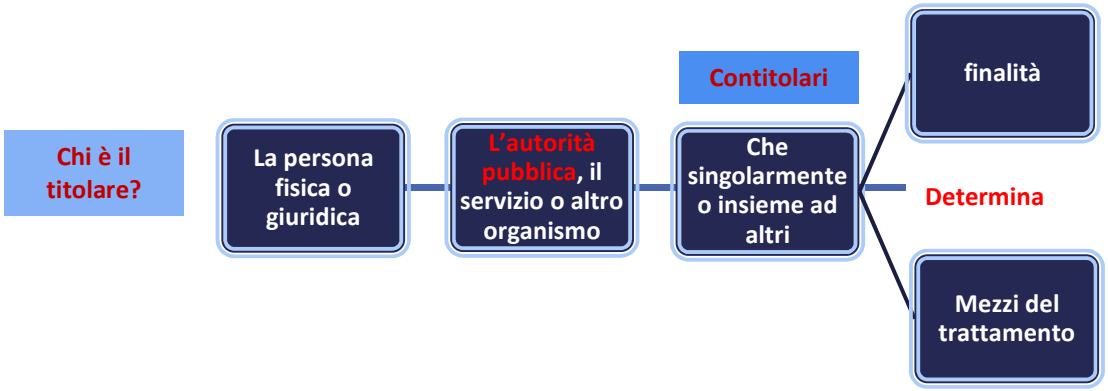
- trattati secondo "**liceità, correttezza e trasparenza**";
- raccolti per "**finalità determinate, esplicite e legittime**";
- adeguati, pertinenti e limitati rispetto alle finalità;
- Esatti;
- limitati nella conservazione;
- **trattati garantendo sicurezza e integrità**.

Gli attori e i ruoli



Comitato europeo per la protezione dei dati Guidelines 7/2020 on the concepts of controller and processor in the GDPR (7.7 2021)

artt. 4, p.7), 24 e 26 e cons da 74 a 79



L'Istituto scolastico titolare del trattamento in ragione della sua **autonomia organizzativa rispetto al Ministero dell'Istruzione**

Il **dirigente scolastico** è colui che – in quanto legale rappresentante - in concreto a prendere decisioni sulle attività di trattamento da intraprendere e sulle modalità attraverso cui queste verranno svolte mediante il personale amministrativo e/o docente

Responsabilità del titolare

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, **il titolare del trattamento mette in atto misure tecniche e organizzative adeguate** per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento (art. 24).

GDPR: artt. 4, par. 7, 24 e 26 e considerando da 74 a 79

Soggetti: compiti del titolare

GDPR: artt. 4, par. 7, 24 e 26 e considerando da 74 a 79

Il titolare:

- **Individua il rischio connesso al trattamento;**
- **Pone in sicurezza l'attività di trattamento dei dati;**
- **Rilascia l'informativa all'interessato;**
- **Attende all'esercizio dei diritti dell'interessato;**
- **Nomina il Responsabile del trattamento dei dati;**
- **Vigila sull'osservanza del contratto di nomina del Responsabile del trattamento dei dati**

Soggetti: compiti del titolare

GDPR: artt. 4, par. 7, 24 e 26 e considerando da 74 a 79

- **Compila il registro del trattamento dei dati;**
- **Nomina il Responsabile della Protezione dei dati (DPO/RPD);**
- **Coopera con l'Autorità di controllo;**
- **Effettua la «valutazione d'impatto» (DPIA);**
- **Effettua la «consultazione preventiva».**

- **Notifica l'eventuale violazione dei dati personali (*data breach*);**
- **Documenta la violazione dei dati personali (*data breach*);**
- **Comunica la violazione dei dati personali (*data breach*);**

IL RESPONSABILE

la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali **per conto** del titolare del trattamento (art. 4, § 8;)

Responsabilità del «responsabile»

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che **presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate** in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato (art. 28).

UN RESPONSABILE CON TANTE «RESPONSABILITA'»

ESCLUSIVAMENTE CON UN CONTRATTO (o altro atto giuridico) E' DISCIPLINATA:

- Materia, durata, natura e finalità del trattamento;
- tipo di dati personali e categorie di interessati;
- **obblighi e diritti** del titolare del trattamento.

IN BASE AL CONTRATTO IL RESPONSABILE SI IMPEGNA A:

- trattare dati soltanto **su istruzione documentata del titolare**;
- consentire i trattamenti **solo a persone autorizzate** con impegno alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza;
- adottare tutte le **misure di sicurezza** (es. cifratura; pseudonimizzazione; recupero da backup);
- rispettare le **condizioni per ricorrere a un sub-responsabile** del trattamento;
- assistere il titolare per dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- **cancellare o restituire** tutti i dati e cancellare le copie esistenti;
- mettere a disposizione del titolare le informazioni per dimostrare il rispetto dei suddetti obblighi e consentire le ispezioni.

Personale autorizzato direttamente coinvolto nel processo formativo ed educativo o nelle attività amministrative della scuola

le persone autorizzate al trattamento dei dati personali operano sotto l'autorità diretta del titolare o del responsabile

Le persone autorizzate al trattamento dei dati personali non possono trattare tali dati se non sono istruite in tal senso dal titolare o dal responsabile

2-quaterdecies del Codice, titolare e responsabile possono prevedere sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo che specifiche funzioni siano attribuite **a persone fisiche espressamente designate**

Individuano le modalità più opportune per autorizzare al trattamento le persone che operano sotto la loro autorità diretta

Istruzioni mirate al contesto (trattamento dati minori, rendimento scolastico)

I PRINCIPI ALLA BASE DELLA RESPONSABILIZZAZIONE (art. 5 Gdpr)

I dati devono essere:

- trattati secondo "**liceità, correttezza e trasparenza**";
- raccolti per "**finalità determinate, esplicite e legittime**";
- adeguati, pertinenti e limitati rispetto alle finalità;
- Esatti;
- limitati nella conservazione;
- **trattati garantendo sicurezza e integrità**.

Accountability e approccio basato sul rischio: valutazione di impatto

GDPR: art. 35 e considerando 84, da 89 a 93 e 95

La valutazione di impatto è prevista per i **trattamenti che presentano un rischio elevato per i diritti e le libertà delle persone fisiche. effettuati con l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità.**

Il registro dei trattamenti: perchè è così importante

GDPR: art. 30 e considerando 82

Il titolare deve avere un **documento di censimento dei trattamenti effettuati** per **disporre di un quadro aggiornato indispensabile per ogni valutazione e analisi del rischio**.

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali e si configura come strumento di compliance alla normativa poiché deve essere esibito in caso di verifiche da parte dell'Autorità.

Quali elementi deve contenere

a) il nome e i **dati di contatto del titolare** del trattamento;

b) le **finalità** del trattamento;

c) una descrizione delle **categorie di interessati** e delle categorie di dati personali;

d) le categorie di **destinatari** a cui i dati personali sono comunicati;

e) i **trasferimenti verso un paese terzo** o un'organizzazione internazionale (indicando il paese terzo o l'organizzazione , la documentazione delle garanzie adeguate;

f) **i termini previsti per la cancellazione** delle diverse categorie di dati (durata conservazione);

g) una descrizione delle **misure di sicurezza** tecniche e organizzative.

Niente vieta di inserire **ulteriori informazioni nell'ottica della complessiva valutazione di impatto** dei trattamenti svolti.

Ma per i responsabili….

Ogni responsabile deve avere un registro di tutte le categorie di **attività svolte per conto di ogni titolare**, contenente:

a) il nome e i dati di contatto **di ogni titolare del trattamento per conto del quale agisce** e del responsabile della protezione dei dati (RPD/DPO);

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento.

IL SISTEMA DELLE RESPONSABILITA

I POTERI «CORRETTIVI» DEL GARANTE

Le sanzioni amministrative pecuniarie

I poteri «correttivi»

Una volta accertata la violazione del regolamento dopo aver valutato i fatti del caso, **il Garante deve individuare le «misure correttive» più appropriate per affrontare tale violazione**.

Le disposizioni di cui all'articolo 58, paragrafo 2, lettere da b) a j), indicano gli strumenti che le autorità di controllo hanno a disposizione per **far fronte a un'inadempienza da parte di un titolare o responsabile** del trattamento.

LE DISPOSIZIONI SANZIONATE DAL REGOLAMENTO
art. 83, c. 4

fino a 10 000 000 EUR, o per le imprese, **fino al 2 %** del fatturato per la violazione degli **obblighi**:

- **del titolare e del responsabile** (artt. 8, 11, da 25 a 39, 42 e 43);
- dell'organismo di certificazione (artt. 42 e 43);
- dell'organismo di controllo (art. 41, paragrafo 4)(sulla conformità con il codice di condotta).

LE DISPOSIZIONI SANZIONATE DAL REGOLAMENTO
art. 83, c. 5

fino a 20 000 000 EUR, o per le imprese, **fino al 4 %** del fatturato per la violazione dei:

- principi di base del trattamento, comprese le condizioni relative al consenso (artt. 5, 6, 7 e 9);
- diritti degli interessati (artt. da 12 a 22) es.: informativa e accesso ai propri dati;
- trasferimenti di dati personali extra UE (artt. da 44 a 49);
- obblighi previsti dagli Stati nelle materie del capo IX (artt. da 85 a 91 –) es. giornalismo, lavoro, ricerca scientifica, storica, statistica, segreto professionale;
- inosservanza di un ordine o di una limitazione del Garante o il negato accesso ai dati e ai locali (art. 58, c. 1 e 2).

Criteri per l'applicazione delle sanzioni amministrative pecuniarie

1. la **natura, la gravità e la durata della violazione** tenendo in considerazione la **natura, l'oggetto o la finalità del trattamento** in questione nonché il **numero di interessati lesi dal danno** e il **livello del danno da essi subito**;
2. il carattere **doloso** (es. contrario al parere del DPO) o **colposo** della violazione;
3. le **misure adottate** dal titolare del trattamento o dal responsabile del trattamento **per attenuare il danno subito** dagli interessati;
4. il **grado di responsabilità** del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 (by design/by default) e 32 (misure sicurezza);
5. ***eventuali*** **precedenti violazioni** pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
6. il **grado di cooperazione con l'autorità di controllo** al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
7. le **categorie di dati** personali interessate dalla violazione;
8. la **maniera in cui l'autorità di controllo ha preso conoscenza della violazione**, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione (data breach);
9. **qualora siano stati precedentemente disposti provvedimenti** di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo **stesso oggetto**, il **rispetto di tali provvedimenti**;
10. l'**adesione ai codici di condotta** approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e
11. eventuali altri **fattori aggravanti o attenuanti** applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

COSA SUCCEDE SE ……

- **In caso di mancato riscontro alla richiesta di informazioni** ai sensi dell'art. 157 del Codice (art. 83, §5 del Regolamento (art. 15 c. 1, dlgs. n. 101/2018; art. 166 Codice);
- **ovvero di negato accesso ai dati e ai locali (art. 83, §5, lett. e) del Regolamento):**

Si configura una violazione amministrativa per la quale è previsto il pagamento di una somma fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato

---

- Qualora in un procedimento o nel corso di accertamenti dinanzi al Garante, **chiunque dichiari o attesti falsamente notizie o circostanze o produce atti o documenti falsi, si configura un illecito penale punito con la reclusione da sei mesi a tre anni**

- Qualora **chiunque intenzionalmente cagioni un'interruzione o turbi** la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti (art. 168 Codice) **si configura un illecito penale punito con la reclusione sino ad un anno.**

La Corte dei conti - Sezione giurisdizionale per la Regione Calabria

14 maggio 2019

La Procura regionale della Corte dei conti **ha convenuto l'ex Presidente della Regione Calabria** chiedendone la condanna al risarcimento dei danni, in favore della Regione Calabria, alla **somma di euro 66.000.**

La richiesta di risarcimento poggia sul pagamento, da parte della Regione Calabria, di complessivi euro **80.000, in forza dell'accertamento di violazioni da parte del Garante**

Le sanzioni irrogate con una ordinanza - ingiunzione, applicativa di una sanzione cumulativa per due distinte condotte: la mancata risposta a una **richiesta del *Garante*** e il mancato rispetto delle **misure minime di sicurezza**.

La Corte dei conti - Sezione giurisdizionale per la Regione Calabria, definitivamente pronunciando, in parziale accoglimento delle richieste della Procura regionale:

Condanna il convenuto ….. al pagamento, in favore della Regione Calabria, della somma di euro 66.000,00.

Le spese seguono la soccombenza e sono liquidate nella misura di euro * 688,04**seicentoottantotto/04*

…….

Così deciso in Catanzaro, nella camera di consiglio del 14 maggio 2019.

- L'ESTENSORE — IL PRESIDENTE
- f.to Andrea Luberti — f.to Rita Loreto

La pubblicazione online di una circolare con dati sensibili di alunni minorenni

La Corte dei Conti, su istanza della Procura regionale, ha riconosciuto a carico della dirigente e di alcuni docenti di un **istituto professionale** la **responsabilità** "*per asserito danno indiretto cagionato all'ente di appartenenza derivante dall'avere pubblicato sulla rete internet una circolare contente* ***dati idonei a rivelare lo stato di salute di scolari minori affetti da disabilità****, così ledendo il diritto alla riservatezza loro e delle famiglie, e, per l'effetto, causando l'irrogazione ad opera del Garante per la Protezione dei dati personali di una sanzione amministrativa, per violazione dell'art. 22, comma 8, del Codice, di* ***€ 20.000,00*** *soddisfatta con fondi appartenenti alla scuola*".

La Corte ha stabilito che «*gli obblighi normativi [...] sono stati dunque disattesi dalla Dirigente scolastica, che con la sua* ***condotta gravemente sprezzante ...*** *ha leso il diritto alla tutela della riservatezza del minore, causando per sua esclusiva colpa (personale ed in vigilando) l'irrogazione della sanzione [provvedimento del Garante n. 36127/97738 del 22.12.2015], così da* ***creare un danno, indiretto, alle casse dell'Istituto scolastico****, in quanto il pagamento di somme con denaro pubblico* ***a causa dell'inosservanza di obblighi imposti normativamente*** *costituisce un aggravio di spesa e sottrae le relative somme all'attuazione degli scopi istituzionali*».

La Corte, in applicazione del potere riduttivo dell'addebito, ha condannato la Dirigente scolastica [...] al «*pagamento, in favore dell'Istituto Professionale di Stato [...], della somma di* ***€ 7.500,00*** *[...]*», specificando altresì «*l'impossibilità di ritenere responsabili della pubblicazione della circolare in parola gli altri docenti rispetto ai quali è emerso il loro ruolo marginale, di* ***meri esecutori delle istruzioni diramate dalla Dirigente scolastica*** *[...]*».
(Sentenza n. 246 del 28 maggio 2019)

GRAZIE PER L'ATTENZIONE

Garante per la protezione dei dati personali
Piazza Venezia 11 - 00186 ROMA
Sito www.gpdp.it – www.garanteprivacy.it
Centralino telefonico: (+39) 06.696771
E-mail: garante@gpdp.it – urp@gpdp.it
Pec: protocollo@pec.gpdp.it