EUSERVICE

PRESENTA

PROTOCOLLO 2023

COME GESTIRE L'INVIO DI DATI IN USA

Redatto da:
DPO Coordinator Avv. Diego Dimalta
In collaborazione con:
DPO dott. Giovanni Gobbi
DPO Avv. Bruno Cantarone
DPO Avv. Chiara Giannessi
DPO dott. Ignazio La Rosa

SOMMARIO

PREMESSA

EUservice, sin dalle ore successive all'annullamento del Privacy Shield, è stata tra i principali attori in Italia che si sono occupati delle conseguenze del vuoto normativo creatosi con la decisione Schrems II. Non a caso, **già nell'ottobre 2020**, poco dopo la riapertura delle scuole, abbiamo divulgato una prima versione del presente protocollo, con indicazioni e spiegazioni di sintesi sull'accaduto. La speranza, al tempo, era quella di doverci limitare a "tamponare" eventuali problemi nell'attesa di indicazioni da parte delle autorità competenti che, purtroppo, non sono mai arrivate. Oggi, a 3 anni di distanza, a seguito di numerose richieste provenienti da associazioni e da interessati, abbiamo pensato fosse opportuno smettere di inseguire le varie segnalazioni oramai costanti, scegliendo invece un approccio più autorevole, basato su valutazioni e sul principio di *accountability*. Questo Protocollo, quindi, è volto ad aiutare i Dirigenti Scolastici, in qualità di Titolari del trattamento, a capire quali sono gli elementi in gioco, per consentire loro di prendere, consapevolmente, una decisione "ufficiale" in merito al trasferimento dati in USA, così che la posizione assunta non vari, in caso di ulteriori richieste e/o segnalazioni.

DEFINIZIONI

I recenti avvenimenti, che approfondiremo nel prosieguo, hanno reso molto difficile la scelta di fornitori di piattaforme nonché di servizi web in quanto, come è facile immaginare, la maggioranza di questi prevede l'invio di dati negli Stati Uniti d'America. Prima di procedere oltre, al fine di meglio comprendere le vicende di cui parleremo, è utile però effettuare una premessa che fornisca le definizioni di alcuni termini a cui faremo frequente riferimento nelle prossime pagine.

In primo luogo, è utile evidenziare come, in base al GDPR, il trasferimento di dati al di fuori dello spazio UE è tendenzialmente vietato salvo il ricorrere di alcune condizioni. Le soluzioni adottate più frequentemente sono:

- **DECISIONE DI ADEGUATEZZA (ex art. 45 GDPR)**: il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo in questione garantisce un livello di protezione adeguato.
- **CLAUSOLE CONTRATTUALI STANDARD (ex art. 46 GDPR)**: la Commissione Europea o l'Autorità di controllo competente, previa approvazione della Commissione, può stabilire che determinati strumenti contrattuali consentano di trasferire dati personali verso Paesi terzi o organizzazioni internazionali.

Una soluzione che si poneva come via di mezzo tra le due citate era il **PRIVACY SHIELD**: accordo che regolamentava il trasferimento di dati tra Unione Europea e USA. L'accordo mirava a proteggere i diritti fondamentali delle persone nell'UE i cui dati personali venivano trasferiti negli Stati Uniti, stabilendo regole certe per le imprese che effettuavano trasferimenti di dati al di là dell'Atlantico.

Il Privacy Shield è stato annullato il 16 luglio 2020 a seguito della sentenza Schrems II.

PERCHÉ CI INTERESSA?

Perché la maggior parte delle grandi società che operano in Internet (le c.d. "Big Tech", ossia Google Inc., Microsoft, Facebook, Amazon etc.) inviavano dati in USA in forza del Privacy Shield o di clausole contrattuali standard (CCS).

LA STORIA SINO AD OGGI

In breve, il 16 luglio del 2020 la Corte di Giustizia dell'Unione europea (CGUE), con la c.d. "sentenza Schrems II", affrontò il tema del trasferimento dei dati tra l'Unione Europea e gli Stati Uniti d'America, invalidando il Privacy Shield e rendendo quindi illegittimo l'invio di dati in USA basato su questa "modalità semplificata". Non solo, la Corte si pronunciò anche sulle **clausole contrattuali standard,** precisando che le stesse avrebbero potuto essere ancora utilizzate, **ma solo in presenza di garanzie ulteriori.** Questa decisione ebbe delle notevoli conseguenze visto che le cosiddette "Big Tech", dovendosi adeguare alla sentenza della Corte, non avrebbero più potuto fare affidamento sul Privacy Shield. Tuttavia, il problema venutosi poi a creare è che molte di queste società, anziché spostare i server in UE (come invece avrebbe voluto la Corte) hanno preferito restare in USA, fondando il trasferimento dati sulle clausole contrattuali standard. Così facendo, sistemi che erano prima considerati sicuri, anche da AGID, sono diventati rischiosi pure per la scuola, che potrebbe infatti essere anche chiamata a rispondere per il loro utilizzo.

UN VUOTO NORMATIVO

A seguito della sentenza Schrems II gli esperti di settore si sarebbero aspettati una serie di interventi coordinati da parte delle Autorità di Controllo (*i Garanti Privacy di tutti i paesi UE*), circostanza questa, però, che non si è verificata, andando così a creare una situazione di forte **incertezza**. Tale incertezza è stata frutto di una serie di elementi che non hanno in alcun modo agevolato le scuole e le imprese di tutta Europa e, in particolare, d'Italia. Difatti, mentre da una parte il MIUR (oggi MIM) suggeriva - per ben due anni- di utilizzare le note piattaforme *educational* distribuite da società americane, dall'altra i Garanti Privacy iniziavano a inibire l'utilizzo di sistemi come Google Analytics, G-Suite e, in Danimarca, anche Google Workspace for Education. In questo contesto, inoltre, si inserivano le indicazioni fornite da **European Data Protection Board**, il Comitato di tutti i Garanti Privacy d'Europa che, nel suggerire una serie di soluzioni, fornì indicazioni inadatte al contesto scolastico, in quanto eccessivamente costose e/o macchinose.

SCENARIO ATTUALE

Il collettivo MonitoraPA si inserisce in questo scenario, evidenziando una realtà di fatto difficilmente contestabile: l'invio di dati in USA, a seguito dell'annullamento del Privacy Shield è illecita. Sotto questo punto di vista non si può che riconoscere la correttezza della posizione di MonitoraPA. Tuttavia, bisogna evidenziare alcuni aspetti:

1. Nel novembre 2022 è partito il procedimento che dovrebbe portare al nuovo Privacy Shield e che, salvo intoppi, potrebbe concludersi già entro l'estate 2023.
2. Il Garante Privacy Italiano ha di recente organizzato dei corsi di formazione diretti ai docenti, proprio in collaborazione con Google.
3. Il Ministero ed il Garante, nonostante le segnalazioni di alcune note associazioni, non hanno mai espresso alcuna opinione contraria rispetto all'utilizzo di sistemi americani che, peraltro, tutt'oggi, mantengono la certificazione del marketplace AGID la quale, tra i requisiti, prevede proprio il rispetto della normativa GDPR.

Ora, questi aspetti certamente non rendono legittimo di per sé l'invio di dati in USA, ma possono e **debbono** incidere sulla valutazione, riservata al Titolare del trattamento, circa la scelta tra **abbandonare o non abbandonare i sistemi informatici statunitensi**.

COME PROCEDERE?

Premesso quanto sopra, possiamo ritenere che sostanzialmente esistono tre opzioni che consentono il raggiungimento di livelli di conformità/prudenza diversi fra loro:

1. Abbandonare totalmente i sistemi americani
2. Mantenere i sistemi americani senza alcun ulteriore accorgimento
3. Mantenere i sistemi americani riducendo il rischio

Ognuna di queste opzioni presenta vantaggi e svantaggi, motivo per cui necessitano di essere esaminate nel dettaglio.

OPZIONE 1 - ABBANDONARE I SISTEMI AMERICANI

Questa opzione, diversamente da quanto si potrebbe pensare, è assolutamente realizzabile. Le iniziative passate di MonitoraPA, al netto di tutte le possibili critiche, hanno sicuramente dimostrato che esistono mezzi alternativi a quelli di Google&Co. Così, mentre prima si pensava che l'unico cookie analitico fosse quello di Google, ora conosciamo altri produttori (europei) che distribuiscono sistemi pressoché identici. **Scegliere questa opzione significa intraprendere un percorso di consapevolezza che, probabilmente, ripagherà nel lungo periodo** in quanto, anche il futuro Privacy Shield 2, con molta probabilità, sarà, come i suoi predecessori, soggetto a critiche e impugnazioni sino al suo annullamento. In un simile scenario, il rischio è quello di trovarsi tra due anni con un nuovo vuoto normativo e le stesse problematiche che stiamo vivendo oggi. Anche per questo, sarebbe tutt'altro che sbagliata l'idea di valutare il graduale abbandono di sistemi americani passando quindi a omologhi europei. In tal senso, per la ricerca di sistemi alternativi, è possibile affidarsi ad una ricerca in internet oppure al sito "*european alternatives*" [European Alternatives] in cui sono raggruppati un cospicuo numero di sistemi alternativi a quelli americani, tutti prodotti in UE. A tal riguardo, si ricorda che prima di adottare una nuova piattaforma sarà comunque necessario verificare la sua certificazione sul marketplace AGID (ora marketplace dell'Agenzia per la Cybersicurezza Nazionale).

OPZIONE 1

VANTAGGI: Questa scelta permetterà alla scuola di essere immune da critiche in merito all'invio di dati personali in USA.

SVANTAGGI: Si tratta di un percorso lungo e, in alcuni casi, non privo di costi, anche solo in termini di tempo necessario per adeguarsi ai nuovi e meno noti sistemi.

OPZIONE 2 - MANTENERE I SISTEMI AMERICANI SENZA ALCUN ACCORGIMENTO

Questa opzione è indubbiamente la più semplice ma, come immaginerete, è anche la meno *compliant* a quelli che sono i dettami del Regolamento Europeo. Certo, potrete sempre dire che il Ministero ha suggerito di usare Google, potrete dire che "così fan tutti", ma la verità è che il mantenimento di tali sistemi, ad oggi, per tutte le ragioni di cui sopra, è da ritenersi illegittimo salvo l'utilizzo di misure idonee a ridurre il rischio (come vedremo dopo).

OPZIONE 2

VANTAGGI: È gratis ed è quello che stanno facendo in molti; se tra qualche mese, poi, venisse approvato il Privacy Shield 2, non avreste più alcun problema.

SVANTAGGI: Sarete sempre in balia di altri: oggi di associazioni come MonitoraPA, domani dell'eventuale annullamento del prossimo Privacy Shield. In ogni caso, le criticità evidenziate dalla decisione Schrems II continueranno ad esistere, anche dopo l'adozione di un nuovo accordo transatlantico, mettendo a serio rischio i diritti dei vostri studenti, anche in presenza di un nuovo Privacy Shield. Il nuovo accordo, infatti, renderebbe giustificato ma non per questo completamente immune da rischi, l'invio di dati in USA.

OPZIONE 3 - MANTENERE I SISTEMI USA, RIDUCENDO IL RISCHIO

Il principio di *accountability*, pilastro del GDPR, responsabilizza il Titolare del trattamento (il Dirigente Scolastico) concedendo a quest'ultimo la possibilità di fare delle valutazioni sul livello di rischio dei trattamenti che desidera intraprendere. In sostanza, salvo rari casi, non esistono divieti assoluti nella normativa GDPR, ma solo avvisi di rischio elevato. In linea con questo principio, nemmeno la sentenza Schrems II o le successive linee guida di EDPB si sono mai spinti sino a ritenere sempre e comunque vietato del tutto l'invio di dati in USA.

Ripetiamo: l'invio di dati in USA può essere proseguito anche dopo Schrems II ma, per farlo, occorre adottare precauzioni spesso oggettivamente troppo difficili e dispendiose per una scuola.

Per capirci, queste sono alcune delle indicazioni di MonitoraPA per poter proseguire con l'utilizzo dei sistemi Google:

- acquistare per ciascuno studente un laptop da utilizzare esclusivamente per la connessione scolastica ai servizi di Google;
- tutti i laptop devono essere privi di circuiteria GSM/4G/5G, possibilmente privi di telecamera e microfono (da disabilitare successivamente se presenti), dello stesso identico modello, con la stessa identica configurazione e versione del sistema operativo, perché minime variazioni potrebbero essere utilizzate per identificare gli utenti;
- acquistare per ciascun docente un laptop da utilizzare esclusivamente per la connessione scolastica ai servizi di Google;
- tutti i laptop di studenti e insegnanti andranno configurati per accedere ad internet esclusivamente tramite VPN;
- ogni 3 mesi, ogni studente e ogni insegnante dovrà riconsegnare il proprio laptop ai sistemisti.

Già ad un primo sguardo è evidente che difficilmente una scuola pubblica potrebbe permettersi i costi monetari e di tempo necessari per adempiere a tale procedura. Sul punto, peraltro, è da evidenziare come l'art. 32 GDPR, espressione diretta del principio di *accountability* preveda che: *tenendo conto dello* ***stato dell'arte*** *e dei* ***costi di attuazione****, nonché della natura, dell'****oggetto****, del* ***contesto*** *e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.*

È quindi proprio il GDPR a dirci che la norma non può essere letta in modo cieco ma deve essere oggetto di valutazioni soggettive che tengano conto di una serie di variabili quali i costi, il contesto e lo stato dell'arte. In tal senso, se si volesse scegliere questa opzione, sarebbe necessario adottare una serie di accorgimenti, così come indicati più avanti, alla luce dei quali abbiamo già provveduto a redigere una valutazione di impatto che invieremo in versione aggiornata già nelle prossime settimane.

OPZIONE 3

VANTAGGI: La scuola, nel rispetto del principio di *accountability* e nel rispetto dei criteri di cui all'art. 32 GDPR potrebbe dire di aver fatto il possibile per ridurre il rischio.

SVANTAGGI: Queste misure costituiscono un tentativo di riduzione del rischio, ma è chiaro che non tutelano al 100% dai rischi evidenziati nella decisione Schrems II in caso di eventuali istruttorie da parte dell'Autorità Garante.

Integrazione – maggio 2023

Ciò premesso, qualora la scuola fosse intenzionata a continuare ad utilizzare i sistemi USA adottando soluzioni di riduzione del rischio, potremmo consigliare di procedere nel seguente modo:

- La scuola potrebbe utilizzare in via preferenziale il registro elettronico per tutte le comunicazioni scuola/famiglia e scuola/alunni contenenti dati personali.
- La scuola dovrebbe chiudere tutti gli account di posta generati in nome e per conto degli studenti utilizzando i servizi americani.
- La scuola potrebbe usare l'archiviazione su cloud (es: G Drive) solo per condividere documenti e informazioni del tutto privi di dati personali. La condivisione con gli alunni di tali documenti (privi di dati) potrà avvenire usando un link accessibile senza obbligo di log-in, in modo da rendere possibile agli studenti l'accesso senza obbligarli alla creazione di account alcuno.
- Qualora, in via eccezionale, fosse assolutamente imprescindibile condividere, con studenti e famiglie, dati personali, utilizzando i sistemi di archiviazione su cloud, si consiglia di sostituire all'interno di tali documenti il nome degli alunni ad un codice alfanumerico che individui univocamente l'alunno, magari anche per tutto l'anno scolastico (pseudonimizzazione).

In ogni caso si renderà necessario redigere una DPIA/data protection impact assessment (meglio, una TIA/transfert impact assessment) che, in accordo con il principio di accountability, consenta di valutare l'effettivo rischio di tale trattamento. A tal fine, si allega il modello di DPIA/TIA da noi predisposto con riferimento all'invio di dati in USA.

ULTERIORI CONSIGLI PER RIDURRE IL RISCHIO

ATTIVITÀ	RISCHIO
Invio e-mail prive di dati personali nel corpo messaggio.	Se il documento non contiene dati personali, l'unico rischio è quello relativo all'utilizzo di indirizzi e-mail dai quali si evincano nome e cognome del mittente o del destinatario.
	SOLUZIONE PROPOSTA
	Utilizzare indirizzi e-mail diversi da nome.cognome@scuola.it. Ad esempio, l'indirizzo potrebbe essere n.c.@scuola.it (ancora meglio se del tipo "docenti.classe2A@scuola.it). In ogni caso il suggerimento è quello di usare indirizzi mail ospitati su server della scuola o su server UE di fornitori affidabili.

ATTIVITÀ	RISCHIO
Invio mail contenenti dati personali nel corpo messaggio.	Se il documento contiene dati personali (oltre all'indirizzo e-mail), qualora si utilizzino servizi e-mail statunitensi, gli stessi potrebbero non essere adeguati alla normativa UE, mettendo quindi in pericolo la riservatezza dei dati di studenti e docenti.
	SOLUZIONE PROPOSTA
	Utilizzare servizi e-mail con server in Unione Europea (o in stati ritenuti adeguati dalla UE) evitando quindi i servizi statunitensi tipo Gmail e simili. Nella maggior parte dei casi il sito della scuola è ospitato su server UE, per questo motivo potrebbe essere consigliabile utilizzare e-mail ospitate sul dominio di tale sito scolastico. Se, nonostante tutto, si preferisce continuare ad utilizzare servizi americani, è necessario che nel corpo messaggio non si faccia in alcun modo riferimento a persone identificate o identificabili anonimizzando i dati personali contenuti nel messaggio.

ATTIVITÀ	RISCHIO
Invio mail contenenti dati personali negli allegati.	Se la mail con dominio Gmail e simili viene utilizzata per l'invio di allegati/documenti contenenti informazioni sullo studente o su altri docenti, questo potrebbe provocare grossi problemi per la riservatezza dei dati di studenti e colleghi.
	SOLUZIONE PROPOSTA
	Utilizzare servizi e-mail con server in Unione Europea (o in stati ritenuti adeguati dalla UE) evitando quindi i servizi statunitensi oppure utilizzare un server a scuola con diverse cartelle accessibili ai docenti/ATA in base alla classe. Se si vuole continuare ad utilizzare servizi americani, allora è necessario che i documenti siano epurati da ogni riferimento a persone identificate o identificabili.

ATTIVITÀ	RISCHIO
Deposito documenti contenenti dati personali di studenti e docenti su cloud.	Se il cloud ha sede in paesi diversi dalla UE (o da quelli considerati adeguati) è possibile che tale condotta comporti un grosso pericolo per la riservatezza dei dati di studenti e docenti.
	SOLUZIONE PROPOSTA

	Utilizzare cloud con sede in Unione Europea oppure utilizzare un server a scuola con diverse cartelle accessibili ai docenti/ATA delle diverse classi. Il collegamento al server della scuola dovrebbe avvenire preferibilmente con VPN. Il cloud americano potrà invece essere utilizzato solo per depositare documenti privi di riferimenti a persone identificate o identificabili. Infine, in via residuale, è concesso l'utilizzo di servizi americani per depositare documenti non anonimi, ma solo previa adozione da parte della scuola di procedure di pseudonimizzazione e cifratura con chiave segreta o, comunque, non comunicata tramite servizi americani.

ATTIVITÀ	RISCHIO
Riunioni da remoto in videoconferenza.	Secondo le linee guida dell'Autorità Tedesca, anche l'utilizzo di sistemi di video conferenza con server in USA può arrecare pericolo ai dati.
	SOLUZIONE PROPOSTA
	L'unica soluzione capace di azzerare il rischio è quella di utilizzare sistemi con server in UE. Differentemente, al solo scopo di ridurre il rischio, il suggerimento è quello di usare sistemi che garantiscano cifratura end to end. Nel caso di utilizzo di sistemi americani, sarà poi opportuno evitare di utilizzare il proprio nome per identificarsi durante la call, preferendo invece degli pseudonimi se non addirittura dei codici. Infine, quanto alle immagini, sarebbe preferibile spegnere il video o, comunque accenderlo per brevi momenti.

ATTIVITÀ	RISCHIO
Utilizzo di sistemi di messaggistica.	**In generale è sconsigliato l'utilizzo di sistemi di messaggistica.** Qualora ciò fosse concesso dal Dirigente, se nei messaggi tra colleghi dovessero essere contenuti dati personali è possibile che da ciò derivi un rischio per la riservatezza delle informazioni di studenti e colleghi.
	SOLUZIONE PROPOSTA
	La soluzione migliore è quella di evitare sistemi di messaggistica. Qualora ciò non fosse possibile, il consiglio è quello di omettere l'indicazione di dati personali di studenti o di docenti, i quali potranno essere identificati in un secondo momento oppure mediante uno pseudonimo o un codice.

RAPPORTI SCUOLA/ALUNNI

ATTIVITÀ	RISCHIO
Invio tracce per i compiti.	Le tracce non contengono riferimenti diretti a studenti. Il rischio è quindi praticamente nullo.
	SOLUZIONE PROPOSTA
	Evitare di inserire nelle tracce riferimenti o comunque dati capaci di identificare o rendere identificabile uno studente.

ATTIVITÀ	RISCHIO
Ricezione compiti/e-mail dagli studenti.	La ricezione di e-mail da parte degli studenti ha due criticità: 1-nell'indirizzo mail potrebbero esserci nome e cognome degli studenti; 2- nel corpo e negli allegati potrebbero esserci dati personali degli studenti.
	SOLUZIONE PROPOSTA
	La scuola dovrebbe utilizzare sistemi mail o cloud con server in UE (vedere pagine precedenti) oppure un server a scuola con diverse cartelle accessibili agli studenti delle diverse classi. Il collegamento ai server della scuola dovrebbe avvenire preferibilmente con VPN. Se ciò non è possibile allora è necessario che gli studenti utilizzino mail prive di riferimento a nome e cognome. Inoltre, è necessario che i compiti non contengano dati personali, i quali potrebbero, ad esempio, essere sostituiti da codici.

ATTIVITÀ	RISCHIO
Deposito documenti su cloud e piattaforme edu.	L'utilizzo di sistemi cloud e piattaforme edu presenta due criticità: 1. Per accedere è necessario creare un account (solitamente usando indirizzo mail); 2. I documenti depositati potrebbero contenere dati personali.
	SOLUZIONE PROPOSTA
	La scuola dovrebbe utilizzare sistemi cloud con server in UE (vedere pagine precedenti) oppure un server a scuola con diverse cartelle accessibili agli studenti delle diverse classi. Il collegamento dovrebbe avvenire preferibilmente con VPN. Se ciò non è possibile allora è necessario che gli studenti utilizzino per iscriversi mail prive di riferimento a nome e cognome. Inoltre, è necessario che i documenti condivisi non contengano dati personali, i quali potrebbero, ad esempio, essere sostituiti da codici.

ATTIVITÀ	RISCHIO
Utilizzo sistemi per messaggi scuola/famiglia.	In generale è sconsigliato l'utilizzo di sistemi di messaggistica per le comunicazioni scuola/famiglia. Qualora ciò fosse concesso dal dirigente, se nei messaggi dovessero essere presenti dati personali è possibile che da ciò derivi un rischio per la riservatezza delle informazioni di studenti e colleghi.
	SOLUZIONE PROPOSTA
	La soluzione migliore è quella di evitare sistemi di messaggistica. Qualora ciò non fosse possibile, il consiglio è quello di omettere l'indicazione di dati personali di studenti, i quali potranno essere identificati in un secondo momento oppure mediante uno pseudonimo o un codice.

ATTIVITÀ	RISCHIO
App complementari al sistema di conference call.	Solitamente le app complementari richiedono la creazione di account tramite l'indirizzo mail degli studenti. In alcuni casi le app trattano anche altri dati personali.
	SOLUZIONE PROPOSTA
	Se la app ha server in UE non ci sono problemi. Se, invece, la app ha server fuori dalla UE allora si procede come segue: se la app richiede l'indirizzo e-mail degli studenti, è opportuno che ogni studente si doti di un indirizzo e-mail privo di riferimenti al nome e cognome. In ogni caso è necessario che lo studente non invii dato alcuno alla app.

CONCLUSIONE

Alla luce di quanto sopra è evidente che il tema dell'invio dei dati negli Stati Uniti d'America non è risolvibile rincorrendo oggi una segnalazione e domani l'altra; occorre infatti un approccio complessivo. La nostra intenzione, invero, sin dall'invio della prima versione di questo protocollo datata ottobre 2020, è sempre stata quella di aiutare le scuole a prendere coscienza del tema affinché, una volta scelta una delle strade proposte, siano consapevoli che, anche in presenza di segnalazioni o minacce di attivisti e associazioni varie, non occorre variare l'approccio adottato. Del resto, a prescindere dall'opinione che si possa avere sull'operato di Monitora PA, ciò che deve essere chiaro è che le scelte non vanno operate *ex post* per paura che un terzo segnali la scuola, ma vanno operate *ex ante*, alla luce di valutazioni di tutti i fattori in gioco.

In conclusione, il ruolo del Titolare del trattamento, ricoperto dai Dirigenti Scolastici, rappresenta una grande responsabilità, ma anche una grande opportunità per dimostrare il proprio impegno a favore della protezione dei dati personali. Per questo è importante valutare le opzioni per prendere la scelta migliore. Scegliere di essere un Titolare del trattamento diligente e attento alle normative non solo contribuisce a costruire la fiducia degli interessati (in particolare delle famiglie), ma rappresenta anche un valore aggiunto per l'immagine e la reputazione della scuola intesa nel suo complesso, e ciò a prescindere dalle sollecitazioni, giuste o sbagliate che siano, che ormai periodicamente arrivano dall'esterno.