Nuovo Regolamento Privacy (UE) 679/2016

Strategia pragmatica di adeguamento per le scuole

dott. Vicenti Francesco

IT Administrator & Linux Specialist

Specializzato in reti e sicurezza

E: francesco@vicenti.it

© 2018 Restart Informatica
Tutti i diritti riservati

Una nuova fonte normativa per la privacy

- Il Regolamento UE 2016/679 del 27 aprile 2016 concerne la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati; è stato pubblicato nella GUCE il 4 Maggio 2016, è entrato in vigore il 24 maggio 2016 ed è diventato direttamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018.

- In quanto Regolamento UE (diverso da direttiva) non richiede una legge nazionale di recepimento.

© 2018 Restart Informatica
Tutti i diritti riservati

Quale la filosofia?

- **Il Regolamento promuove la responsabilizzazione (*accountability)*** dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

- **Il principio chiave è "privacy by design"**, cioè garantire la protezione dei dati sin dalla fase di ideazione e progettazione di un trattamento o di un sistema e adottare comportamenti che consentano di prevenire rischi per la protezione dei dati.

© 2018 Restart Informatica
Tutti i diritti riservati

Cosa cambia ???

Codice della Privacy 196/03	Regolamento UE 2016/679
Normative frammentate, non uniformi fra i vari paesi membri dell'Unione Europea.	Regole comuni per tutti i paesi così da eliminare disparità di trattamento per i soggetti interessati del trattamento.
Per definire la legge applicabile si considerava la sede del Titolare del trattamento.	La legge è applicata nella sede in cui avviene il trattamento. I Titolari (tra i quali anche social network, piattaforme web e motori di ricerca) saranno quindi soggetti alla normativa europea anche se aventi sede al di fuori dell'UE.
Non vi erano particolari requisiti per l'informativa, che pertanto era spesso lunga, incomprensibile e con richiami normativi complessi.	L'informativa deve essere accessibile, concisa e scritta con linguaggio chiaro e semplice con un numero limitato di riferimenti normativi. Deve essere fornita per iscritto.

© 2018 Restart Informatica
Tutti i diritti riservati

Cosa cambia ???...

Codice della Privacy	Regolamento UE 2016/679
Non vi erano particolari obblighi di tenuta della documentazione comprovante il regolare espletamento dei trattamenti dati.	Introdotto il principio di "*Accountability*", ovvero della responsabilità "*verificabile*". **E' obbligatorio documentare tutti i trattamenti effettuati**
La privacy era intesa come elemento finale delle attività di trattamento, in quanto gli eventuali vizi nella raccolta dei dati potevano essere "sanati" anche dopo che i trattamenti erano già stati effettuati.	Introdotti i principi di "Privacy by Design" e "Privacy by Default", i quali implicano che i trattamenti debbano essere concepiti sin dal momento della loro ideazione nel rispetto delle regole fissate dal legislatore.

© 2018 Restart Informatica
Tutti i diritti riservati

Cosa cambia ???...

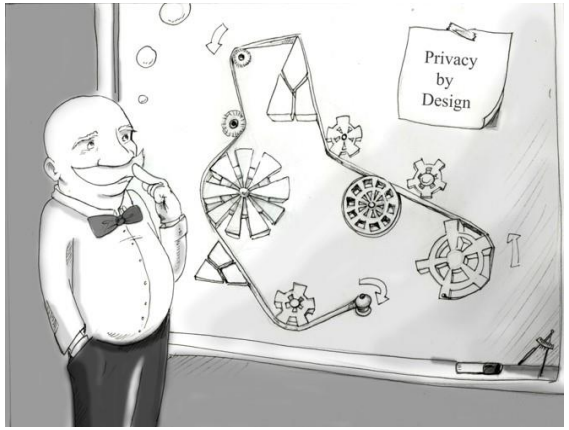
Codice della Privacy	Regolamento UE 2016/679
Non era stabilito alcun obbligo di notifica delle eventuali violazioni dei dati personali	E' stato sancito l'obbligo, per il Titolare, di comunicare le violazioni (*data breach*) all'Autorità Garante, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, nonché al soggetto interessato, qualora la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà.
Non era prevista alcuna figura di raccordo tra i soggetti del trattamento e l'Autorità Garante.	Introduzione della figura del Data Protection Officer (DPO/RPD), figura professionale obbligatoria per alcune categorie di soggetti Titolari del trattamento, che dovrà fungere da referente con il Garante e dovrà avere requisiti e competenze elevate. Il DPO potrà essere sia un dipendente che un collaboratore con regolare contratto.

© 2018 Restart Informatica
Tutti i diritti riservati

I passi fondamentali

1) Privacy by design (*il processo alle intenzioni*)

In particolare, con l'espressione **"privacy by design"**, il Regolamento Europeo richiamare l'attenzione dei titolari sull'esigenza che la protezione dei dati personali venga garantita **"fin dalla progettazione".**



A questo proposito, l'art. 25, paragrafo 1 del Regolamento stabilisce che **il titolare del trattamento dei dati personali** deve **adottare delle misure tecniche e organizzative idonee** a dare concreta attuazione a quelle che sono le disposizioni e i principi in materia di protezione dei dati e garantire in questo modo i diritti degli interessati.

© 2018 Restart Informatica
Tutti i diritti riservati

I passi fondamentali…

2) Privacy by default

Il secondo concetto introdotto dal GDPR, sempre all'art. 25, è invece quello di **"privacy by default".** Con questa espressione il legislatore europeo ha affermato la necessità che la protezione dei dati personali sia garantita **"per impostazione predefinita".**

Le soluzioni a cui il titolare del trattamento potrà affidarsi potranno consistere, ad esempio, nella riduzione al minimo del trattamento dei dati personali, nella pseudonimizzazione dei dati personali, nella massima trasparenza sulle finalità e sulle modalità del trattamento di dati personali, nel consentire all'interessato di controllarne il trattamento rendendo facilmente ed effettivamente esercitabili i diritti previsti dal Regolamento.

Inoltre, il titolare dovrà attenersi a questi criteri in tutte le fasi di trattamento: nella fase dello sviluppo, della progettazione, della raccolta, della selezione e dell'utilizzo di dati personali e sempre alla luce di un'attenta analisi del contesto specifico di riferimento.

.

© 2018 Restart Informatica
Tutti i diritti riservati

I passi fondamentali

3) Trattamento lecito, equo e trasparente

Alle aziende che trattano dati personali viene richiesto di trattare i dati personali in modo lecito, equo e trasparente. Cosa significa? Cerchiamo di capirlo:

Lecito significa che tutti i trattamenti devono essere basati su uno scopo legittimo.

Equo indica che le aziende si assumono la responsabilità e non trattano i dati per scopi diversi da quelli legittimi.

Trasparente significa che le società devono informare gli interessati delle attività di trattamento dei loro dati personali.

© 2018 Restart Informatica
Tutti i diritti riservati

I passi fondamentali

4) I Diritti degli interessati/di accesso

Agli interessati è stato dato il **diritto di chiedere all'azienda quali informazioni questa abbia su di loro e cosa faccia con queste informazioni**. Inoltre, l'interessato ha il diritto di chiederne la rettifica, opporsi al trattamento, presentare un reclamo o anche chiedere la cancellazione o il trasferimento dei propri dati personali (da esercitare entro 30 / 90 giorni)

5) Il Consenso

Se e quando la società intende trattare i dati personali oltre allo scopo legittimo per cui sono stati raccolti tali dati, è necessario che sia richiesto un consenso chiaro ed esplicito all'interessato. Una volta raccolto, questo consenso deve essere documentato e l'interessato è autorizzato a ritirare il proprio consenso in qualsiasi momento.
Inoltre, per il trattamento dei dati dei minori, il GDPR richiede il consenso esplicito dei genitori (o tutori) se l'età del minore è inferiore ai 16 anni.

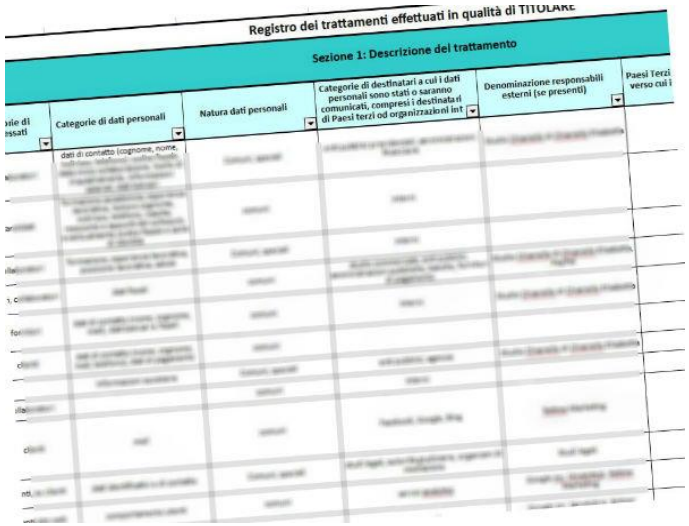
© 2018 Restart Informatica
Tutti i diritti riservati

I passi fondamentali…

6) Registro dei trattamenti (ex DPS)

Tutti i titolari e i responsabili di trattamento, devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30.

Si tratta di uno strumento fondamentale allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico –indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.



© 2018 Restart Informatica
Tutti i diritti riservati

I passi fondamentali…

7) Diritto di cancellazione – diritto all'oblio

è il diritto di cancellazione dei propri dati personali in forma rafforzata. I titolari hanno l'obbligo, se hanno reso pubblici tali dati, ad esempio pubblicandoli su un sito web, di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione". Rispetto al D. Lgs. n. 196/2003 l'interessato ha il diritto di chiedere la cancellazione dei propri dati **anche dopo la revoca del consenso al trattamento.**

© 2018 Restart Informatica
Tutti i diritti riservati

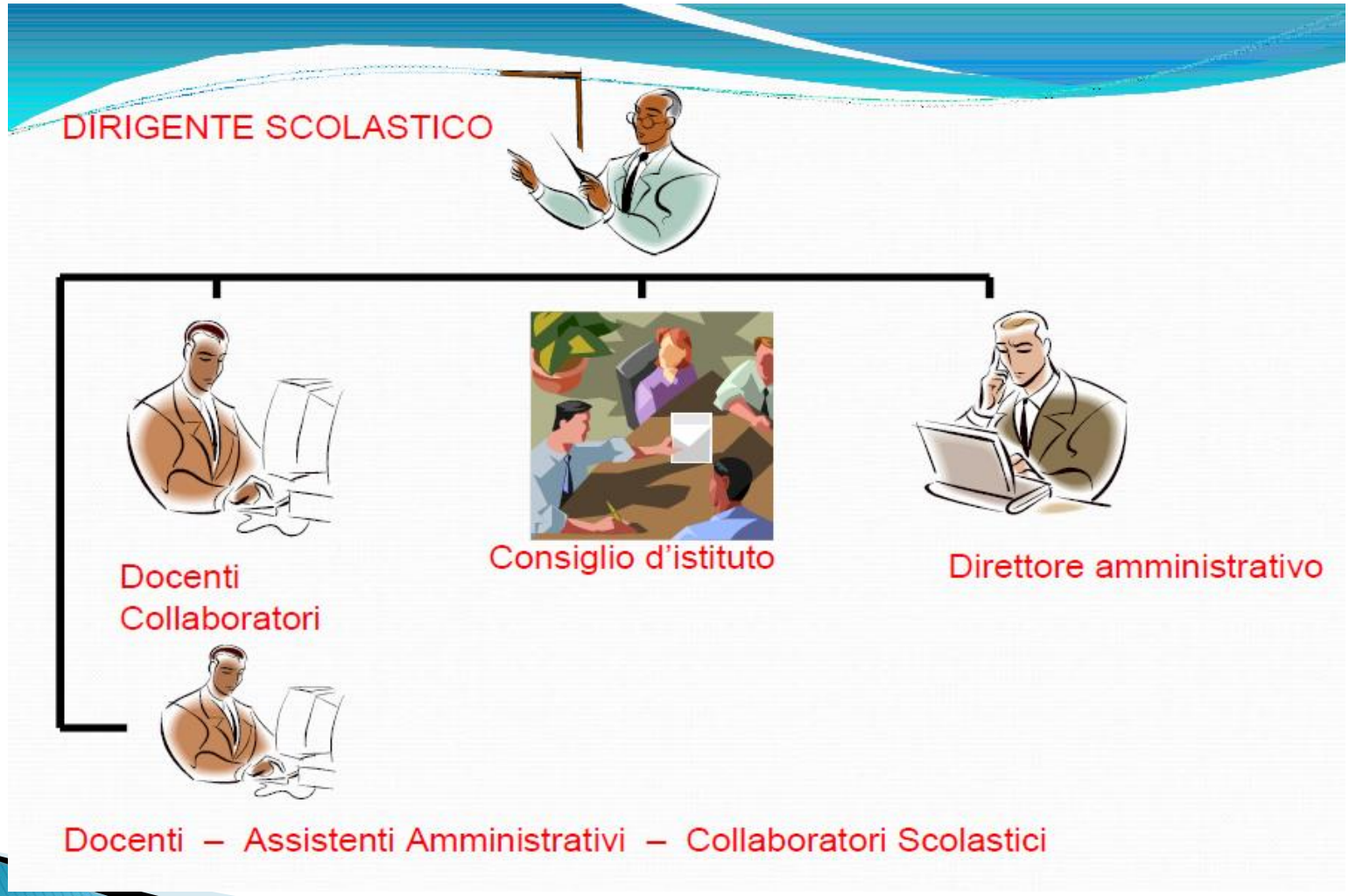
La privacy nella scuola

DATO PERSONALE Qualsiasi informazione che riguardi persone fisiche (come uno studente o un professore) che permettono l'identificazione diretta. Sono, tra gli altri, dati personali: **il nome e cognome, l'indirizzo di residenza, il codice fiscale, l'impronta digitale ecc.**

DATO SENSIBILE **Qualunque dato che può rivelare l'origine razziale ed etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'appartenenza a partiti, sindacati o ad associazioni, lo stato di salute e la vita sessuale, anche dati economici.**

© 2018 Restart Informatica
Tutti i diritti riservati

La privacy nella scuola



© 2018 Restart Informatica
Tutti i diritti riservati

La privacy nella scuola

Direttore amministrativo

- Contabilità
- Area personale
- Area didattica
- Area affari generali

- Didattica
  - Dati relativi agli alunni
- Personale
  - Gestione del personale
- Contabilità
  - Stipendi
  - Archivi relativi ai fornitori
- Affari generali
  - Protocollo
  - Archivio
  - Rapporti con enti e imprese

© 2018 Restart Informatica
Tutti i diritti riservati

La privacy nella scuola

Area didattica / Dati relativi agli alunni

Cartaceo

❑ DATI PERSONALI

- Fascicolo personale
  - ✓Curriculum studi
  - ✓Dati personali
  - ✓Dati dei genitori
  - ✓Fotografia
- Registro iscrizioni
- Registro tasse scolastiche
- Registro certificati
- Registro diplomi

© 2018 Restart Informatica
Tutti i diritti riservati

La privacy nella scuola

Area personale / Gestione del personale

Cartaceo

- ❑ COMUNICAZIONE dati personali

- ✓Elenchi del personale
- ✓Elenchi elettorali
- ✓Registro dei consigli di classe
- ✓Registro dei voti
- ✓Registro esiti esami e idoneità
- ✓Pratiche viaggi istruzione
- ✓Invio dati al CSA
- ✓INPS
- ✓INPDAP
- ✓Servizi Vari (MEF)
- ✓Ragioneria (MEF)
- ✓Altre scuole

© 2018 Restart Informatica
Tutti i diritti riservati

La privacy nella scuola

STUDENTI E FAMIGLIE INFORMATE

Tutte le scuole – sia quelle pubbliche, sia quelle private – **hanno l'obbligo di far conoscere agli "interessati" (studenti, famiglie, professori, etc.) come vengono trattati i loro dati personali**. Devono cioè rendere noto, attraverso un'adeguata informativa, quali dati raccolgono, come li utilizzano e a quale fine.

TRATTAMENTO DEI DATI NELLE ISTITUZIONI SCOLASTICHE PUBBLICHE

Le istituzioni scolastiche pubbliche possono trattare **solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali** oppure quelli espressamente previsti dalla normativa di settore.

Non è tuttavia necessario ottenere il consenso per trattare i dati richiesti ai fini dell'iscrizione o di altre attività scolastiche.

© 2018 Restart Informatica
Tutti i diritti riservati

La privacy nella scuola

ISCRIZIONI

Tutti gli istituti di ogni ordine e grado – sia quelli che aderiscono al sistema di iscrizioni on line predisposto dal Ministero sia quelli che utilizzano moduli cartacei – ma anche gli enti locali eventualmente competenti devono prestare particolare attenzione alle informazioni che richiedono per consentire l'iscrizione scolastica. I moduli base, ad esempio, possono essere adattati per fornire agli alunni ulteriori servizi secondo il proprio piano dell'offerta formativa (POF), ma **non possono includere la richiesta di informazioni personali eccedenti e non rilevanti (ad esempio lo stato di salute dei nonni o la professione dei genitori) per il perseguimento di tale finalità.** Particolare attenzione deve essere prestata inoltre all'eventuale raccolta di dati sensibili. Il trattamento di questi dati, oltre a dover essere espressamente previsto dalla normativa, richiede infatti speciali cautele e può essere effettuato solo se i dati sensibili sono indispensabili per l'attività istituzionale svolta

© 2018 Restart Informatica
Tutti i diritti riservati

La privacy nella scuola

VOTI ED ESAMI

Gli esiti degli scrutini o degli esami di Stato sono pubblici. Le informazioni sul rendimento scolastico sono soggette ad un regime di conoscibilità stabilito dal Ministero dell'Istruzione dell'Università e della Ricerca. È necessario però che, **nel pubblicare i voti degli scrutini** e degli esami nei tabelloni, l'istituto scolastico **eviti di fornire**, anche indirettamente, informazioni sulle condizioni di salute degli studenti, o **altri dati personali non pertinenti**. **Il riferimento alle "prove differenziate" sostenute dagli studenti portatori di handicap o con disturbi specifici i apprendimento (DSA), ad esempio, non va inserito nei tabelloni, ma deve essere indicato solamente nell'attestazione da rilasciare allo studente.**

© 2018 Restart Informatica
Tutti i diritti riservati

La privacy nella scuola

DALLA SCUOLA AL LAVORO

Su esplicita richiesta degli studenti interessati, e/o di altre istituzioni scolastiche 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.

© 2018 Restart Informatica
Tutti i diritti riservati

La privacy nella scuola

SMARTPHONE E TABLET

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**.

Si deve quindi prestare particolare attenzione prima di caricare immagini e video su blog o social network, oppure di diffonderle attraverso mms o sistemi di messaggistica istantanea.

© 2018 Restart Informatica
Tutti i diritti riservati

La privacy nella scuola

FOTO E VIDEO

Il Garante della privacy, ha chiarito che la scuola non deve chiedere il consenso per la pubblicazione SUL SITO INTERNET DELL'ISTITUTO (NO SOCIAL/WHATSAPP) di foto, proprio perché si suppone che si tratti di foto istituzionali.

Non potrebbe risultare troppo arbitrario il concetto di foto istituzionale?

Quello che regola la pubblicazione delle foto da parte della scuola nella sua qualità di Pubblica Amministrazione e per i soli fini istituzionali è senza dubbio il **principio di "non eccedenza"** ed il buonsenso. Per spiegarci meglio, il processo educativo spesso non può dirsi concluso senza la diffusione degli aspetti salienti dello stesso verso l'utenza territoriale e gli stakeholder. Basti pensare, ad esempio, alla partecipazione delle squadre scolastiche ai Debate Game, attività certamente istituzionale, che per loro natura assumono valenza educativa quando svolte in pubblico e diffuse come buona pratica anche in streaming. In questo caso la pubblicazione è lecita e senza dubbio necessaria per le finalità didattiche perseguite. Al contrario, invece, la pubblicazione delle fotografie della festa di carnevale sembra, a chi scrive, meno giustificabile per fini istituzionali e, pertanto, evitabile.

© 2018 Restart Informatica
Tutti i diritti riservati

La privacy nella scuola

FOTO E VIDEO

Il Garante, a scanso di equivoci, per attribuire il carattere istituzionale alla pubblicazione delle fotografie nel sito web della scuola, propone di usare il PTOF della scuola. In che senso? Il PTOF è il documento che esprime l'offerta formativa della scuola o, in altre parole, come la scuola intende implementare le finalità istituzionali per le quali opera. Se la scuola argomenta nel PTOF le motivazioni e i contesti per i quali la pubblicazione delle fotografie sono parte dell'offerta formativa ecco che, concordemente al parare del garante, la pubblicazione delle fotografie assume valenza istituzionale e come tale è possibile senza la richiesta del consenso.

"Commette reato la maestra che scatta in classe una foto a un bambino in presenza degli altri alunni e le invia in tempo reale tramite WhatsApp alla madre per dimostrare che il bambino non vuole stare seduto ed è sdraiato sul pavimento?"

Senza voler entrare nel merito della pratica educativa di comunicare in tempo reale con i genitori il comportamento dei figli, non pare legittima la condotta della maestra non essendo lecita la comunicazione a terzi di dati personali (in questo caso le fotografie) di studenti.

© 2018 Restart Informatica
Tutti i diritti riservati

La privacy nella scuola

IMMAGINI DI RECITE E GITE SCOLASTICHE

Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione. Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su Internet, e sui social network in particolare. **In caso di comunicazione sistematica o diffusione diventa infatti necessario, di regola, ottenere il consenso informato delle persone presenti nelle fotografie e nei video.**

© 2018 Restart Informatica
Tutti i diritti riservati

Quali misure di sicurezza adottare?

La struttura informatica dovrà essere organizzata secondo procedure che siano conformi al GDPR, in grado di assicurare "riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento" (art. 32 Regolamento UE 2016/679).

Tra le possibili misure informatiche:

1) SISTEMI DI TRACCIABILITÀ E CONTROLLO DEGLI ACCESSI AI DATI

Sistemi per tracciare tutti gli accessi alla base dati, volti a rilevare eventuali violazioni e intrusioni.

2) SISTEMI FIREWALL E ANTIVIRUS

Strumenti in grado di prevenire il rischio di intrusioni o accessi abusivi al sistema informativo.

© 2018 Restart Informatica
Tutti i diritti riservati

Quali misure di sicurezza adottare?

3) SOLUZIONI DI BACKUP E DISASTER RECOVERY

Soluzioni di backup e salvataggio dei dati e misure idonee a garantirne il ripristino. Quindi procedure in grado di "ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico" (art. 32 Regolamento UE 2016/679).

4) CRITTOGRAFIA DEI DATI

Utilizzo di sistemi di cifratura in grado di rendere i dati personali incomprensibili agli utenti non autorizzati.

© 2018 Restart Informatica
Tutti i diritti riservati

Quali misure di sicurezza adottare?

5) UTILIZZO E GESTIONE DI CREDENZIALI D'ACCESSO

La protezione delle credenziali di accesso rappresenta uno dei principi fondamentali della sicurezza delle informazioni, in particolare la creazione e la gestione delle password che costituiscono la principale contromisura agli accessi non autorizzati.

La password policy si applica a tutti i servizi informatici centrali, gestionali ed applicativi, compresi quelli web, alle postazioni di lavoro, alla rete wi – fi, al servizio di posta elettronica e a tutte le applicazioni e risorse informatiche presenti in ogni istituto. Come regola generale, la password deve essere ragionevolmente complessa e difficile da individuare e/o ricavare e deve essere cambiata periodicamente (3 o 6 mesi)

© 2018 Restart Informatica
Tutti i diritti riservati

Quali misure di sicurezza adottare?

Tra le possibili misure tecniche:

1. Gestione, custodia e aggiornamento della parola chiave (Password)
2. Corretta tenuta degli Archivi cartacei (sotto chiave)
3. Controllare la qualità delle porte e delle serrature e la protezione dei locali con allarmi, illuminazione di sicurezza ecc..;
4. Controllare l'accesso ai locali e il controllo dei visitatori;
5. Corretto smaltimento dei rifiuti cartacei o elettronici;

© 2018 Restart Informatica
Tutti i diritti riservati

Le sanzioni amministrative

Le violazioni agli obblighi in capo alle imprese (20 articoli su 49) sono punite fino a 10 milioni di euro o fino al 2% del fatturato mondiale annuo.

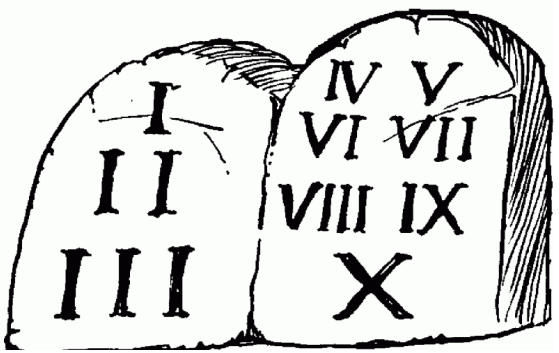
Ad esempio:

- la violazione dell'obbligo di tenuta del registro dei trattamenti;
- l'omessa consultazione preventiva dell'Autorità;
- l'omessa notifica di data breach;
- l'omessa nomina del DPO;
- l'omessa adozione di misure di sicurezza adeguate.

Gli altri 29 articoli puniscono fino a 20 milioni di euro o fino al 4 % del fatturato mondiale annuo la violazione dei principi del regolamento e dei diritti degli interessati.

© 2018 Restart Informatica
Tutti i diritti riservati

I 10 COMANDAMENTI!



1) Ognuno è RESPONSABILE PERSONALMENTE
2) Ottenere il consenso per la pubblicazione di immagini/video (Non nel PTOF)
3) Non lasciare mai documenti con dati sensibili A VISTA
4) Conservare sempre registro e altri documenti in archivi con chiave
5) Evitare la diffusione di materiale e di informazioni su Whatsapp/Social
6) Predisporre informative per ogni nuovo iscritto/docente/fornitore… (entro 30gg)
7) Garantire il diritto all'oblio e/o alla non diffusione di dati
8) Per le comunicazioni elettroniche utilizzare SEMPRE canali crittografati
9) Comunicare tempestivamente ogni violazione
10) Analizzare sempre il rischio e progettare sempre misure idonee ad evitare la diffusione non autorizzata dei dati

© 2018 Restart Informatica
Tutti i diritti riservati

Conclusioni

“Il problema non é fare la cosa giusta… ma sapere qual é la cosa giusta”

Lyndon B. Johnson

GRAZIE PER L’ATTENZIONE!

© 2018 Restart Informatica
Tutti i diritti riservati