



MEDING CONSULTING
CONSULENZA E FORMAZIONE AZIENDALE

La Scuola e la protezione dei dati



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Fondamenti normativi

Il diritto alla protezione del dato nell'ordinamento italiano:

Art. 3 Costituzione (pari dignità sociale dell'uomo)

Art. 13 Costituzione (inviolabilità della libertà della persona)

La riservatezza è dunque quell'interesse che in base ad una certa valutazione legislativa e sociale risulta fondamentale per l'individuo al quale si riconosce un certo ambito privato dal quale poter escludere l'altrui ingerenza e l'indiscriminata pubblicizzazione di ciò che lo riguarda nell'intimo. Il rifiuto di tale riconoscimento finirebbe col menomare gravemente la persona pregiudicando la sua dignità.

Definendo la riservatezza un valore essenziale della persona , il diritto alla privacy diventa **diritto inviolabile tutelato dall'Art. 2 della Costituzione**

30 Giugno 2003

viene approvato il decreto legislativo n. 196, recante il Codice in materia di protezione dei dati personali

25 Maggio 2018

sono state abrogate le disposizioni contenute nel DLGS 196 del 2003 relative alla privacy andate in conflitto con il nuovo regolamento GDPR.

e' entrato in vigore il regolamento generale sulla protezione dei dati (***General Data Protection Regulation***), ufficialmente **regolamento (UE) n. 2016/679** e meglio noto con la sigla **GDPR** immediatamente applicabile e direttamente vincolante.

4 Settembre 2018

Con la pubblicazione in Gazzetta Ufficiale n°205 del 4 settembre 2018 il Decreto legislativo n. 101 del 10 agosto 2018, contenente le disposizioni per l'adeguamento della normativa nazionale sulla privacy alle disposizioni del regolamento (UE) 2016/679.

Viene allineata la normativa italiana alle disposizioni Europee contenute nel GDPR (General Data Protection Regulation)

Principio di “Accountability”/Responsabilizzazione

Il Titolare del trattamento è competente per il rispetto di tutti i principi applicabili al trattamento di dati personali ed è in grado di provarlo («responsabilizzazione»).

Conservazione dei dati

1. I dati possono essere conservati per un arco di tempo non superiore al conseguimento delle finalità.
2. E' possibile la conservazione anche per periodi più lunghi quando i dati sono trattati esclusivamente a fini di archiviazione nel pubblico interesse, ricerca scientifica, storica o a fini statistici (principio di limitazione della conservazione).

Conservazione dei dati nella scuola

ILLIMITATA

Verbali Consiglio di classe/ Collegio docenti

Determinazioni dirigenziali

Inchieste/ indagini ambientali

ELIMINABILI

Richieste per trasporto alunni

Documentazione utenze

Modelli 770 (50 anni)



GDPR - Regolamento generale sulla protezione dei dati (UE/2016/679)

Articolo 6 - Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
 - a) l'interessato **ha espresso il consenso al trattamento dei propri dati** personali per una o più specifiche finalità;
 - b) il trattamento è **necessario all'esecuzione di un contratto** di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
 - c) il trattamento è **necessario per adempiere un obbligo legale** al quale è soggetto il titolare del trattamento;
 - d) il trattamento è **necessario per la salvaguardia degli interessi vitali dell'interessato** o di un'altra persona fisica;
 - e) il trattamento è **necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento**;
 - f) il trattamento è **necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi**, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.
2. **La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.**



Il **consenso dei minori** è valido a **partire dai 14 anni** (il limite di età può essere abbassato fino a 13 anni dalla normativa nazionale); prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

DEVE essere, in tutti i casi, libero, specifico, informato e inequivocabile e NON è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo).

Cos'è il Trattamento dei dati

Art. 4. Definizioni

Ai fini del precedente codice si intende per:

- a) **“Trattamento”**, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.



Dati personali

Sono dati personali le **informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica** e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..

Dati che permettono l'**identificazione diretta** - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i

Dati che permettono l'**identificazione indiretta**, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa);

Dati rientranti in particolari categorie: si tratta dei **dati** c.d. "**sensibili**", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute, alla vita o all'orientamento sessuale. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici e i dati biometrici;

Dati relativi a condanne penali e reati: si tratta dei dati c.d. "giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.



Origini razziali ed etniche I dati sulle origini razziali ed etniche possono essere trattati dalla scuola per favorire l'integrazione degli alunni stranieri.

Convinzioni religiose Gli istituti scolastici possono utilizzare i dati sulle convinzioni religiose al fine di garantire la libertà di culto e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento.

Stato di salute I dati idonei a rivelare lo stato di salute possono essere trattati per l'adozione di specifiche misure di sostegno per gli alunni disabili o con disturbi di apprendimento; per la gestione delle assenze per malattia; per l'insegnamento domiciliare e ospedaliero a favore degli alunni affetti da gravi patologie; per la partecipazione alle attività sportive, alle visite guidate e ai viaggi di istruzione.

Convinzioni politiche Le opinioni politiche possono essere trattate dalla scuola esclusivamente per garantire la costituzione e il funzionamento degli organismi di rappresentanza: ad esempio, le consulte e le associazioni degli studenti e dei genitori.

Dati di carattere giudiziario I dati di carattere giudiziario possono essere trattati per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione o di protezione, come i testimoni di giustizia. Eventuali contenziosi Il trattamento di dati sensibili e giudiziari è previsto anche per tutte le attività connesse ai contenziosi con gli alunni e con le famiglie (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce all'autorità giudiziaria, etc.), e per tutte le attività relative alla difesa in giudizio delle istituzioni scolastiche.



GDPR e PRINCIPALI ADEMPIMENTI PER LA P.A.

- Nomina DPO o RPD responsabile protezione dati
- Registro trattamenti
- DPIA "valutazione d'impatto sulla protezione dei dati" o "Data protection impact assesment"
- Rivalutazione liceità dei trattamenti
- Individuazione e definizione dei ruoli
- Misure di sicurezza



Compiti più importanti DPO

Attività di informazione e consulenza al titolare o al responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento, sugli obblighi derivanti dal regolamento e da altre disposizioni dell'Unione o degli Stati membri in materia di protezione dei dati;

Sorveglianza sull'osservanza, da parte del titolare o del responsabile del trattamento, **del regolamento** e delle altre disposizioni dell'Unione o degli Stati membri in materia di protezione dei dati, compresa l'attribuzione delle responsabilità, sensibilizzazione e formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

Fornire, se richiesto, un **parere sulla “valutazione d'impatto”** della protezione dei dati e sorvegliarne l'adempimento ai sensi dell'art. 35;

Cooperare con l'autorità di controllo, e **fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento**, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.



INDIVIDUAZIONE E DEFINIZIONE DEI RUOLI

1 CONTITOLARI

2 RESPONSABILI (esterni) DEL TRATTAMENTO

3 AUTORIZZATI

4 RESPONSABILE PROTEZIONE DATI DPO

NB: dal principio di “Privacy by design” di cui all’art. 25 deriva che gli autorizzati (ossia quelli che per il Codice privacy erano/sono gli “incaricati”) debbono essere nominati prima dell’avvio del trattamento.

TITOLARE DEL TRATTAMENTO

TITOLARE DEL TRATTAMENTO La persona fisica, l'impresa, la pubblica amministrazione, l'associazione, etc. cui fa capo effettivamente il trattamento di dati personali e alla quale spetta assumere le decisioni fondamentali sugli scopi e sulle modalità del trattamento medesimo (comprese le misure di sicurezza). In ambito scolastico, il titolare del trattamento in genere è il Ministero dell'Istruzione, dell'Università e della Ricerca, o **l'istituto scolastico** di riferimento.

AUTORIZZATI (incaricati)

INCARICATO DEL TRATTAMENTO Il dipendente (un professore, un componente della segreteria, DSGA etc.) o il collaboratore che per conto del titolare del trattamento dei dati (ad esempio il Ministero dell'Istruzione, dell'Università e della Ricerca) elabora o utilizza materialmente i dati personali sulla base delle istruzioni ricevute dal titolare medesimo (e/o dal responsabile, se designato).

INTERESSATO

**La persona cui si riferiscono i dati personali
(ad esempio lo studente o il professore).**



DIRITTO DI ACCESSO AI DATI PERSONALI

Anche in ambito scolastico, ogni persona ha diritto di conoscere se sono conservate informazioni che la riguardano, di apprenderne il contenuto, di farle rettificare se erronee, incomplete o non aggiornate. Per esercitare questi diritti è possibile rivolgersi direttamente al **“titolare del trattamento”** (in genere l’istituto scolastico di riferimento) anche tramite suoi incaricati o responsabili del trattamento dei dati. Se non si ottiene risposta, o se il riscontro non risulta adeguato, è possibile rivolgersi al Garante o alla magistratura ordinaria. Diverso è il caso dell’accesso agli atti amministrativi che, infatti, non è regolato dal Codice della privacy, né vigilato dal Garante per la protezione dei dati personali. Come indicato nella legge n. 241 del 1990 (e successive modifiche), spetta alla singola amministrazione (ad esempio alla scuola) valutare se esistono i presupposti normativi che permettono di prendere visione e di estrarre copia di documenti amministrativi ai soggetti con un “interesse diretto, concreto e attuale” alla conoscibilità degli atti. Inoltre il diritto di accesso ai dati e ai documenti detenuti dalla pubblica amministrazione (cosiddetto accesso civico), è consentito nelle forme e nei limiti di cui al d.lgs. n.33 del 2013, come modificato dal d.lgs. n.97 del 2016.



Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibili fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche **concisa, trasparente e facilmente accessibile**, oltre a utilizzare un **linguaggio semplice e chiaro**.

Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. **L'esercizio dei diritti è, in linea di principio, gratuito** per l'interessato, ma possono esservi eccezioni



VIOLAZIONE DELLA PRIVACY

In caso di violazione della privacy - come ad esempio la diffusione sul sito internet della scuola dei dati personali in assenza di una idonea base normativa, oppure il trattamento dei dati senza aver ricevuto una adeguata informativa o senza aver espresso uno specifico e libero consenso, qualora previsto - la persona interessata (studente, professore, etc.) può presentare al Garante un'apposita "segnalazione" gratuita o un "reclamo" (più circostanziato rispetto alla semplice segnalazione e con pagamento di diritti di segreteria).

Il "ricorso", invece, è riservato al caso in cui il titolare del trattamento non abbia dato adeguato riscontro alla richiesta dell'interessato di esercitare i propri diritti (accesso ai dati personali, aggiornamento, rettifica, opposizione,) assicurati dal Codice della privacy. In alternativa al ricorso presentato al Garante, la persona interessata può rivolgersi all'autorità giudiziaria ordinaria

Diritto di cancellazione (diritto all'oblio) (art.17)

Il diritto cosiddetto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata.

Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: 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" (*art. 17, paragrafo 2*).

Verbali consiglio di classe prima dei 10 anni, foto pubblicate ecc....

Ha **un campo di applicazione più esteso** di quello di cui all'art. 7, comma 3, lettera b), del Codice, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (*si veda art. 17, paragrafo 1*).

Privacy e vita dello studente

TEMI IN CLASSE Non lede la privacy l'insegnante che assegna ai propri alunni lo svolgimento di temi in classe riguardanti il loro mondo personale o familiare. Nel momento in cui gli elaborati vengono letti in classe - specialmente se riguardano argomenti delicati - è affidata alla sensibilità di ciascun insegnante la capacità di trovare il giusto equilibrio tra le esigenze didattiche e la tutela dei dati personali. Restano comunque validi gli obblighi di riservatezza già previsti per il corpo docente riguardo al segreto d'ufficio e professionale, nonché quelli relativi alla conservazione dei dati personali eventualmente contenuti nei temi degli alunni.

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 di apprendimento (DSA), ad esempio, non va inserito nei tabelloni, ma deve essere indicato solamente 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.



DISABILITÀ 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.

Recite e manifestazioni

Sul punto si è pronunciato il Garante per la protezione dei dati personali, con riferimento alle “riprese video ed alle fotografie raccolte dai genitori, durante recite e saggi scolastici”.

Il Garante ha espressamente sancito che le riprese, sebbene possano avere ad oggetto minori con disabilità fisiche, non violano la privacy, in quanto “non destinate a diffusione, ma raccolte per fini personali e destinate ad un ambito familiare o amicale”.



GESTIONE DEL SERVIZIO MENSA

Gli enti locali che offrono il servizio mensa possono trattare – secondo quanto previsto nei rispettivi regolamenti - i dati sensibili degli alunni indispensabili per la fornitura di pasti nel caso in cui debbano rispondere a particolari richieste delle famiglie legate, ad esempio, a determinati dettami religiosi o a specifiche condizioni di salute (ndr. vedi anche sezione “REGOLE GENERALI”).

Alcune particolari scelte, infatti (pasti vegetariani o rispondenti a determinati dettami religiosi) possono essere idonee a rivelare le convinzioni (religiose, filosofiche o di altra natura)



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.



CURRICULUM E IDENTITÀ DIGITALE DELLO STUDENTE

L'ultima riforma della scuola del 2015 ha istituito il cosiddetto **“Curriculum dello studente”** che, associato a un'identità digitale, raccoglie tutti i dati utili anche ai fini dell'orientamento e dell'accesso al mondo del lavoro, relativi al percorso degli studi, alle competenze acquisite, alle eventuali scelte degli insegnamenti opzionali, alle esperienze formative anche in alternanza scuola-lavoro e alle attività culturali, artistiche, musicali, sportive e di volontariato, svolte in ambito extrascolastico.

Le modalità operative per la sua realizzazione sono demandate a un apposito decreto del Ministro dell'Istruzione, dell'Università e della Ricerca, sui cui si dovrà esprimere anche il Garante per la protezione dei dati personali.



SCUOLA E NUOVE TECNOLOGIE

CYBERBULLISMO E ALTRI FENOMENI DÌ RISCHIO

Gli studenti, anche i più giovani, rappresentano spesso l'avanguardia tecnologica all'interno della scuola, grazie alla loro capacità di utilizzare le opportunità offerte da Smartphone, Tablet e altri strumenti che consentono la connessione costante in rete.

Tuttavia alla capacità tecnologica non corrisponde spesso eguale maturità nel comprendere la necessità di difendere i propri diritti e quelli di altre persone, a partire dagli stessi compagni di studio. I giovani devono essere consapevoli che le proprie azioni in rete possono produrre effetti negativi anche nella vita reale e per un tempo indefinito.

Troppi ragazzi, insultati, discriminati, vittime di Cyber bulli, soffrono, possono essere costretti a cambiare scuola o, nei casi più tragici, arrivare al suicidio.

SCUOLA E NUOVE TECNOLOGIE

CYBERBULLISMO E ALTRI FENOMENI DÌ RISCHIO

È quindi estremamente importante prestare attenzione in caso si notino comportamenti anomali e fastidiosi su un social network, su sistemi di messaggistica istantanea (come Whatsapp, Snapchat, Skype, Messenger, etc.) o su siti che garantiscono comunicazioni anonime.

Se si è vittime di commenti odiosi, di cyberbullismo, di sexting o di altre ingerenze nella propria vita privata, non bisogna aspettare che la situazione degeneri ulteriormente.

Occorre avvisare subito i compagni, i professori, le famiglie se ci si rende conto che qualcuno è insultato o messo sotto pressione da compagni o da sconosciuti.

Si può chiedere al gestore del social network di intervenire contro eventuali abusi o di cancellare testi e immagini inappropriate.

In caso di violazioni, è bene segnalare immediatamente il problema all'istituzione scolastica, al Garante della privacy e alle altre autorità competenti.

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.



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.



IMMAGINI DI RECITE E GITE SCOLASTICHE

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.

Succede spesso, tra l'altro, che una fotografia inviata a un amico o a un familiare venga poi inoltrata ad altri destinatari, generando involontariamente una comunicazione a catena dei dati personali raccolti.

Tale pratica può dar luogo a gravi violazioni del diritto alla riservatezza delle persone riprese, e fare incorrere in sanzioni disciplinari, pecuniarie e in eventuali reati.



REGISTRAZIONE DELLA LEZIONE E STRUMENTI COMPENSATIVI

È possibile registrare la lezione esclusivamente per scopi personali, ad esempio **per motivi di studio individuale**.

Per ogni altro utilizzo o eventuale diffusione, anche su Internet, è necessario prima informare adeguatamente le persone coinvolte nella registrazione (professori, studenti...) e ottenere il loro esplicito consenso.

Nell'ambito dell'autonomia scolastica, gli istituti possono decidere di regolamentare diversamente o anche di inibire l'utilizzo di apparecchi in grado di registrare.

In ogni caso deve essere sempre garantito il diritto degli studenti con diagnosi DSA (disturbi specifici dell'apprendimento) o altre specifiche patologie di utilizzare tutti gli strumenti compensativi (come il registratore) di volta in volta previsti nei piani didattici personalizzati che li riguardano.



Publicazioni on-line: pubblicità e trasparenza

Le scuole di ogni ordine e grado sono soggette a un regime di pubblicità e trasparenza. È però necessario che gli istituti scolastici prestino particolare attenzione a **non rendere accessibili informazioni che dovrebbero restare riservate o a mantenerle on-line oltre il tempo consentito**, mettendo in questo modo a rischio la privacy e la dignità delle persone a causa di un'errata interpretazione della normativa o per semplice distrazione.

In particolare, allo scopo di facilitare la corretta applicazione della normativa, il Garante ha, tra l'altro, predisposto apposite "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati".



Publicazioni on-line: pubblicità e trasparenza

La pubblicazione su Internet di informazioni personali deve essere lecita e non eccedente le finalità istituzionali perseguite.

Diversamente, tale diffusione può arrecare non solo un pregiudizio alla riservatezza individuale, ma incrementare anche il rischio che le persone interessate possano subire abusi, come il cosiddetto furto di identità.

Per i documenti non liberamente disponibili on line, restano comunque valide le regole sull'accesso previste in particolare dalla legge n.241 del 1990 e dal d.lgs. n. 33 del 2013 come modificato dal d.lgs. n.97 del 2016.



Il trattamento dei dati viene qualificato come esercizio di attività pericolosa (art. 2050 c.c.)

QUINDI

Vale il

“Principio dell’inversione dell’onere della prova”.

Attenzione:

**L’aver adottato tutte misure di sicurezza adeguate evita sanzioni amministrative o penali,
ma non esime da un eventuale risarcimento danni !!!**

Alcuni “consigli”

Massima discrezione

Pochi “scambi informativi” tra colleghi.

Nessuno “scambio informativo” con l’esterno



Reati non informatici

Il ricorso alla tecnologia informatica non è determinante per il compimento dell'atto

Alcuni esempi:

Ingiuria

Diffamazione

Minacce e molestie

Trattamento illecito dei dati personali e violazione della privacy

Violazione dei diritti d'autore



Reati informatici

Ricorso alla tecnologia informatica è determinante per il compimento dell'atto.

Alcuni esempi:

Accesso abusivo ad un sistema informatico e telematico

Diffusione di programmi diretti a danneggiare o interrompere un sistema

Danneggiamento informatico

Detenzione abusiva di codici di accesso a sistemi informatici o telematici

Frode informatica



GRAZIE PER L'ATTENZIONE



MEDING CONSULTING
CONSULENZA E FORMAZIONE AZIENDALE