Privacycert®

sistema integrato gestione privacy

Privacycert è una società specializzata nell'analisi di conformità del trattamento e della gestione dei Dati Personali, nel rispetto di tutti i requisiti e delle misure previste dalla vigente normativa.

Il "*Sistema Integrato Gestione Privacy*" consente il raggiungimento ed il mantenimento degli standard previsti dal legislatore in ambito privacy.

Privacy & PA
Regolamento UE n. 679/2016

Avv. Manlio Filippo Zampetti

Studio Legale Avv. Manlio Filippo Zampetti

Presidente C.d.A. Privacycert Lombardia S.r.l.
avvocatozampetti@gmail.com – lombardia@privacycert.it

L'applicazione della normativa PRIVACY negli Istituti Scolastici

All'interno dell'ambito scolastico è importante che ci sia una **sensibilizzazione** sulle norme per la Protezione dei Dati Personali per:

- **riaffermare** quotidianamente quei principi di **civiltà**, come la **riservatezza** e la **dignità** della persona, che devono sempre essere al centro della formazione di ogni cittadino.

ESEMPIO:
Il documento pubblicato sul sito internet di una scuola che **riporta i dati sulla salute** di uno studente:

➡ **non è semplicemente una svista in tema di protezione dati**, ma una violazione della normativa e un grave potenziale danno causato allo sviluppo di un giovane.

1. DEFINIZIONI:

- DATO PERSONALE
- DATO SENSIBILE
- TRATTAMENTO
- INTERESSATO
- TITOLARE DEL TRATTAMENTO
- RESPONSABILE DEL TRATTAMENTO
- INCARICATO DEL TRATTAMENTO
- INFORMATIVA
- MISURE DI SICUREZZA
- DIFFUSIONE
- COMUNICAZIONE
- RECLAMO
- RICORSO
- SEGNALAZIONE

2. NORMATIVA PRIVACY: REGOLE GENERALI

2.1 DIRITTO DI ACCESSO AI DATI PERSONALI

Ogni individuo ha il diritto, anche in ambito scolastico, per tutto ciò che concerne i **dati personali**, di:

- **conoscere** se sono conservate informazioni che lo riguardano;
- **apprendere** il contenuto dei dati;
- **rettificare** i dati se erronei, incompleti o non aggiornati.

Per esercitare questi diritti è possibile rivolgersi **al titolare, al responsabile o all'incaricato** del trattamento.

Ogni responsabile del Trattamento, incaricato del trattamento ed eventuale rappresentante del responsabile del trattamento **conserva** la documentazione di tutti i trattamenti effettuati **sotto la propria responsabilità**.

(Artt. 22 e 28 Reg. EU)

2.2 DATI SENSIBILI E GIUDIZIARI

I Dati sensibili sono i dati personali dai quali è possibile rilevare la razza, l'origine etnica, la religione o le convinzioni personali, le opinioni politiche, l'appartenenza sindacale, i dati genetici o relativi alla salute ed alla sfera sessuale, i dati inerenti condanne penali o misure di sicurezza.

Il trattamento di tali informazioni diventa lecito se «*riguarda dati resi manifestamente pubblici dall'interessato*».

In sintesi riassumendo i dati sensibili riguardano:

- ORIGINI RAZZIALI ED ETNICHE
- CONVINZIONI RELIGIOSE
- STATO DI SALUTE
- OPINIONI POLITICHE
- DATI DI CARATTERE GIUDIZIARIO

2.3 VIOLAZIONE DELLA PRIVACY

In caso di **violazione** della Privacy l'interessato può rivolgersi al **Garante**:

- Tramite un reclamo/segnalazione gratuita;
- Tramite ricorso, qualora il titolare si rifiutasse di conferire un adeguato riscontro alla sua richiesta.

In alternativa è possibile rivolgersi **all'autorità giudiziaria** ordinaria.

3. LE FIGURE SCOLASTICHE INTERESSATE

Le **figure coinvolte** nel trattamento dei dati sono:

- Il **Dirigente Scolastico** in qualità di **titolare**, quale rappresentante dell'Istituzione scolastica, con il compito di indicare i responsabili e gli incaricati;
- Il **Direttore dei Servizi Generali e Amministrativi** (D.S.G.A.), in qualità di **responsabile** avente la diretta responsabilità nella gestione del personale amministrativo;
- Il **personale Docente,** in qualità di **incaricato** a trattare i dati sensibili degli alunni;
- Il **personale ATA**, in qualità di **incaricato** a trattare i dati personali limitatamente all'ambito del proprio servizio.

4. LE TIPOLOGIE DEI DATI PERSONALI

Le tipologie dei dati personali trattati in un **Istituto Scolastico**, in riferimento alle persone fisiche nel suo interno, interessano rispettivamente:

- **Alunni**, per i quali vengono trattati:
  - Dati comuni
  - Dati sensibili
- **Personale scolastico**, per il quale vengono trattati:
  - Dati comuni
  - Dati sensibili
  - Dati giudiziari
- **Familiari** degli alunni, per i quali vengono trattati:
  - Dati comuni
- **Fornitori**, per i quali vengono trattati:
  - Dati comuni

5. Introduzione al Reg. Europeo n. 679/2016

Il Parlamento Europeo, in data 14 Aprile u.s., ha **APPROVATO** definitivamente il c.d. "**pacchetto protezione dati**", che si compone di due diversi strumenti:

- un nuovo **Regolamento** concernente la "*tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati*";
- una nuova **Direttiva** indirizzata alla "*regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all'esecuzione delle sanzioni penali*"**.**

La pubblicazione del Nuovo Regolamento sulla Gazzetta UE è avvenuta in data **4 maggio 2016**.

A partire dal ventesimo giorno dalla pubblicazione (24 maggio p.v.), gli **Stati membri** avranno **due anni** di tempo per allineare la normativa nazionale alle nuove prescrizioni introdotte dal Nuovo Regolamento, che diventerà definitivamente applicabile in tutto il territorio UE a partire dal **25 maggio 2018**.

5.1 Principi CONFERMATI con il Nuovo Reg. UE n. 679/2016:

- **Il trattamento ESCLUSIVO** di dati personali **di persone fisiche** (non giuridiche) per scopi diversi dall'uso personale;
- **La distinzione** fra trattamento di dati personali **comuni** e trattamento di dati c.d. **sensibili;**
- **Gli obblighi** di informare l'interessato sull'uso che verrà fatto dei suoi dati personali;
- **Gli obblighi** di ottenere il consenso per i trattamenti non necessari o per i trattamenti di particolari tipi di dati.

5.2 I principali 8 impatti del Regolamento

1. **NUOVE INFORMAZIONI** da gestire;
2. **DIMOSTRAZIONE** della «*compliance*» (o in inglese, c.d. Principio dell'Accountability);
3. **VALUTAZIONE d'Impatto** della gestione dei dati personali;
4. Nomina di un **R.P.D.** (o in inglese, c.d. Data Protection Officer);
5. Segnalazione di una **VIOLAZIONE di Dati** (o in inglese c.d. Data Breach);
6. Nuovi requisiti per i **fornitori;**
7. Accresciuti obblighi **di trasparenza** ;
8. **SANZIONI** più rigide rispetto al Codice della Privacy n. 196/2003.

1.0 Nuove informazioni per gli interessati

❖ **Domanda:** Quali sono i nuovi **Obblighi** e i nuovi **Diritti** per l'Interessato?

Obbligo di informare gli interessati anche in merito a:

- Tempi di conservazione dei dati
- Origine dei dati
- Diritto alla portabilità dei dati e restrizioni
- Diritto ad adire l'Autorità di controllo competente.

Nuovi diritti:

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

2.0 La responsabilizzazione del Titolare del Trattamento ex Art. 24 (Reg. UE n. 679/2016)

Tenuto conto della natura, dell'ambito di applicazione, del contesto e della finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, **il titolare del trattamento deve** attuare:

- **misure minime ed adeguate** per garantire che il trattamento dei dati sia effettuato conformemente al Regolamento;
- **politiche adeguate** in materia di protezione dei dati personali.

N.B.: L'adesione ai codici di condotta o ad un meccanismo di certificazione può essere utilizzata come elemento per **DIMOSTRARE** il rispetto degli obblighi da parte del titolare del trattamento.

3.0 La Valutazione d'Impatto sulla protezione dei dati (Art. 35 Reg .UE)

Qualora un tipo di trattamento presenti un «**rischio** elevato» per i diritti e le libertà delle persone fisiche, il **titolare** deve effettuare:

- una **Valutazione dell'Impatto del Trattamento** (*o analisi del rischio*) sulla protezione dei dati personali.

La **Valutazione d'Impatto** sulla protezione dei dati **è richiesta** specialmente nei seguenti casi:

- **Trattamento automatizzato**, su cui si basano decisioni che hanno **effetti giuridici** o che incidono in modo analogo su persone fisiche;
- **Trattamenti**, su larga scala, di **categorie particolari** di dati personali;
- **Sorveglianza** sistematica, su larga scala, di una **zona accessibile al pubblico**.

3.1 Cosa deve contenere la Valutazione d'Impatto ai sensi dell'Art. 35 del Regolamento Europeo?

La **VALUTAZIONE D'IMPATTO** deve almeno contenere:

- **Descrizione** e **finalità** dei trattamenti previsti;
- Valutazione di **necessità** e **proporzionalità** dei trattamenti;
- Valutazione dei **rischi** per i diritti e le libertà degli interessati;
- Le **misure** previste per affrontare eventuali rischi.

3.2 Cosa deve contenere la Valutazione d'Impatto ai sensi dell'Art. 35 del Regolamento Europeo?

- **Domanda:** Chi deve compilare la Valutazione D'Impatto?

Il titolare o il responsabile del Trattamento dovrebbero consultarsi con il **DPO (Data Protection Officer)** sulle seguenti tematiche:

- La conduzione di una Valutazione d'Impatto;
- quale metodologia da adottare nel condurre un DPIA;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, **per attenuare i rischi** per i diritti e gli interessi delle persone interessate;
- se il «DPIA» sia stato condotto correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi ai requisiti in materia di protezione dei dati.

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

4.1 Nomina ex artt. 37 – 39 Reg. UE

✓ Obbligatorietà

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

✓ Requisiti

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

✓ Indipendenza

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

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

Compiti Generali ai sensi dell'Art. 39 del Regolamento Europeo:

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

4.3 Compiti Specifici ai sensi del Reg. UE n. 679/2016:

1. **Aiutare** a condurre la **Valutazione d'Impatto** (c.d. in inglese, *Data Protection Impact Assessment, DPIA*)
2. **Registro delle attività dei trattamenti**: In merito al registro delle attività dei trattamenti, la sua tenuta è un obbligo che ricade sul titolare e sul responsabile, e non sul **DPO**. La sua obbligatorietà viene scaturita dalla presenza di un numero di 250 dipendenti o maggiore, e alla presenza di un «*rischio elevato*» di Tutela di dati personali.
3. **Data breach**: In merito al «*data breach*», il **DPO** svolge un ruolo chiave nella notifica e comunicazione delle **violazioni di dati personali**.

Niente vieta al titolare o al responsabile del trattamento di affidare al DPO ***il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile stesso.***

Inoltre*, si osservi che l'art. 33, par. 3, lettera b)* ***GDPR****, ove sono indicate le informazioni da fornire all'autorità di controllo, prevede che* ***tali informazioni comprendano anche il nominativo*** *(e non solo le informazioni di contatto)* ***del DPO****.*

4.4 Dubbi organizzativi

- **Domanda:** Quali sono le risorse/supporti che il Titolare deve mettere a disposizione del DPO?

- supporto attivo della funzione di DPO da parte del senior management;
- tempo sufficiente per l'espletamento dei compiti affidati;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;
- comunicazione ufficiale della designazione del DPO a tutto il personale;
- accesso garantito ad altri servizi all'interno della struttura del titolare/del responsabile in modo da ricevere tutto il supporto, le informazioni o gli input necessari;
- formazione permanente.

4.5 Responsabilità del DPO

- **Domanda**: Il DPO è personalmente responsabile in caso di inosservanza degli obblighi in materia di protezione dei dati?

No, il DPO non è responsabile personalmente in caso di inosservanza degli obblighi in materia di protezione dei dati. Spetta al titolare o al responsabile del trattamento garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al regolamento. La responsabilità di garantire l'osservanza della normativa in materia di protezione dei dati ricade sul titolare / sul responsabile del trattamento.

5.0 Violazione dei dati - Data breach (artt. 33 e 34)

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

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

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

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

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

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

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

6.0 Nuovi requisiti per i fornitori

Obblighi diretti tra cui:

- **Obblighi di documentazione**: *Policy* sul trattamento dei dati, *Policy* di sicurezza, procedure atte a dimostrare la compliance con il Regolamento;
- Tenuta di un **registro delle attività di trattamento** per ciascun cliente/titolare (Art.30.2);
- **Innalzamento requisiti di sicurezza** sui dati adottando misure specifiche parametrate ai **rischi**, tra cui, pseudonimizzazione, crittografia, ecc.(Art.32);
- **Obbligo di segnalazione** al titolare dei *Data breach* (Art.33.2).

Che tipi di Responsabilità sono previsti per gli Interessati e il Titolare?

- **diretta** verso gli interessati per i danni subiti (se l'inadempimento dei propri obblighi è diretto o prevede la violazione delle istruzioni legittime del titolare);
- **solidale** con il titolare (Art.82).

6.1 Contratti con i fornitori

Clausole obbligatorie da inserire nei contratti/atti di nomina del responsabile:

- **Descrizione dettagliata** dei trattamenti: *oggetto, durata, natura e finalità dei trattamenti, tipologia di dati registrati, categorie di interessati, obblighi e diritti del titolare*.

Obbligazioni del Responsabile, tra cui:

- Elenco delle **misure tecniche e organizzative**;
- Trattamento dei dati SOLO su **istruzioni documentate** per iscritto del Titolare, **incluse eventuali previsioni sul trasferimento dei dati fuori dalla Unione Europea**;
- Obbligo nel gestire **i diritti** degli interessati: *accesso, correzione, cancellazione, limitazione, opposizione,* ***portabilità***;
- Restituzione o **cancellazione** dei dati a discrezione del Titolare alla cessazione del contratto;
- **Obblighi di cooperazione con il Titolare nel notificare i «Data Breach»** e implementare le valutazioni d'impatto.

7. Accresciuti obblighi di trasparenza (artt. 5 e 12 Reg. UE)

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

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

7.1 L'informativa

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

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

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

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

Omessa o inidonea informativa all'interessato (Artt. 161/162):

- **Da 6.000 a 36.000 euro** (rispetto alle condizioni economiche del contravventore).

7.2 Il consenso

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

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

7.3 La prova del consenso

- È innovativa la previsione introdotta dall'art. 7, par. 1:"*qualora il trattamento sia basato sul consenso,* ***il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso*** *al trattamento dei propri dati personali*";
- si pone in capo al **titolare** un vero e proprio **onere della prova** sulla raccolta del consenso;
- per converso non è necessario che il consenso sia documentato per iscritto (v. invece art. 23, co. 3 cod. privacy).

7.4 Il consenso del minore

Art. 8, comma 1:

- qualora l'interessato abbia espresso il suo consenso "*per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni*";
- "*Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale*".

❖ **Domanda:** Quali sanzioni comporta la mancata o erronea richiesta di consenso?

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

8. SANZIONI

8.1 Sanzioni amministrative D.Lgs. n. 196/03:

- Omessa o inidonea informativa all'interessato (Artt. 161/162)
  - **Da 6.000 a 36.000 euro** (rispetto alle condizioni economiche del contravventore);
- **Inosservanza** dei provvedimenti di prescrizione di **misure necessarie** o di divieto ex 154 co. I, lett c)-d) (Art. 162 ter)
  - **Da 30.000 a 180.000 euro;**
- Omessa informazione o esibizione al Garante (Art. 164)
  - **Da 10.000 a 60.000 euro.**

8.2 Sanzioni Penali:

- Trattamento illecito di Dati (Art. 167)
  - Reclusione **da 6 a 18 mesi**
  - Reclusione **da 6 a 24 mesi**
  - Reclusione **da 1 a 3 anni;**
- Falsità nelle dichiarazioni e notificazioni al Garante (Art. 168)
  - Reclusione **da 6 mesi a 3 anni;**
- Inadeguatezza delle Misure minime di sicurezza (Art 169)
  - Reclusione **fino a 2 anni o** Ammenda **da 10.000 a 50.000 euro;**
- Inosservanza di provvedimenti del Garante (Art. 170)
  - Reclusione **da 3 mesi a 2 anni.**

8.3 Nuove **Sanzioni Reg.UE n. 679/2016**

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

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

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

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

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

Chi ne risponde?

Il titolare risponde per il **danno cagionato** dal suo trattamento che **violi** il presente Regolamento.

Il Responsabile risponde per il danno causato dal trattamento **SOLO** SE **NON** HA adempiuto agli obblighi del presente regolamento.

6. Prepararsi al Regolamento: 7 punti chiave

- **Consapevolezza del cambiamento**: analizzare e anticipare gli impatti del Regolamento (analisi dei rischi).

- **Individuazione dei trattamenti:** documentare tutti i trattamenti di dati personali effettuati dall'azienda, precisando per ciascuno di essi l'origine e la natura dei dati, le categorie di interessati, le modalità e le finalità di trattamento, i tempi di conservazione, nonché eventuali comunicazioni a soggetti terzi o diffusioni.

- **Revisione della documentazione privacy**: identificare e aggiornare le informative agli interessati, i moduli di consenso, le nomine a responsabile del trattamento e le clausole “Dati Personali” nei contratti con i fornitori o dipendenti e pianificarne l'adozione.

- **Responsabilizzazione del Titolare - Principio di Accountability**: definire un piano di compliance, che comprenda le valutazioni di impatto, la revisione dei piani di audit, delle procedure e delle policy nonché piani di formazione.

- Privacy by Design & **Data Protection Impact Assessment** (c.d. Valutazione d'Impatto): iniziare a familiarizzare con questi concetti e capire quando e come implementarli.

- Nomina di un **DPO.**

- **Data Breach**: definire le procedure per la rilevazione, segnalazione e indagine di violazioni di sicurezza (entro 72 ore dalla conoscenza dell'evento).

6.1 Linee guida del Governo per l'adeguamento al GDPR

Il 17 ottobre è stata **approvato il testo delle deleghe per l'adeguamento al GDPR**.

Nell'esercizio della **delega**, il *Governo* è tenuto a seguire, i seguenti criteri direttivi:

- **abrogare** espressamente **le disposizioni del Codice Privacy**, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679;
- **modificare il codice** di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679;
- **adeguare**, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196**, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679** con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse.

6.2 Adeguarsi al GDPR: FOCUS Istituti Scolastici

L'adeguamento al **GDPR** avviene seguendo alcuni processi:

- La nomina del **Responsabile Protezione Dati** (*c.d. D.P.O. in inglese*)
- Il piano di **Audit**, nello specifico c.d. «sopralluoghi» per definire l'organigramma, l'organizzazione e le responsabilità giornaliere in materia di Dati personali**;**
- La compilazione della «**Valutazione d'Impatto**» del Trattamento dei Dati;
- La redazione dell'**elenco degli incaricati** e del **Registro dei Trattamenti;**
- La redazione e consegna di un **Manuale di Gestione Privacy**, contenente la **documentazione obbligatoria** per la conformità normativa;
- La **Formazione** specifica del personale ai sensi dell'art. 39 GDPR;
- Le **Verifiche annuali** delle linee guida del DPO incaricato**.**

Privacycert®
sistema integrato gestione privacy

Grazie per l'attenzione!

Avv. Manlio Filippo Zampetti

Studio Legale Avv. Manlio Filippo Zampetti

Presidente C.d.A. Privacycert Lombardia S.r.l.

avvocatozampetti@gmail.com

lombardia@privacycert.it

www.privacycert.it