CIDA
CONFEDERAZIONE ITALIANA DIRIGENTI E ALTE PROFESSIONALITÀ
LAZIO

POLO TECNICO PROFESSIONALE GALILEO
Informatica e Meccanica

Roma, 9 maggio 2018

I.T.I.S. Galileo Galilei
Il nuovo Regolamento sulla privacy e la scuola
Responsabilità e messa in conformità dell'Istituto Scolastico

Regolamento europeo e la scuola: cosa fare, quando e chi lo deve fare

Relatore: Giuseppe GALGANO

privacy in chiaro

Il problema non è fare la cosa giusta …

… ma sapere quale sia la cosa giusta.

Lyndon B. Johnson

Di cosa parleremo

- Introduzione alla protezione dei dati
- Il Regolamento UE 679/2016 (GDPR)
- Le principali azioni da compiere
- Implicazioni operative
- Punti di attenzione degli istituti scolastici
- Domande

Giuseppe GALGANO

Esperienze in ambito Data Protection

- Consulenza alle organizzazioni in ambito del Trattamento dei Dati Personali.
- Formatore sulla tematica Data Protection, relatore presso convegni e commissario in sessioni di esame per certificazione DPO.
- Coordinatore del Gruppo DPO-Data Protection di Federmanager Roma.
- Autore di articoli di divulgazione sull'argomento e coautore del testo "La certificazione della Data Protection" - Freni Angelo Editore.

Certificazioni/Qualificazioni

- Data Protection Officer
- Data Protection Auditor/Lead Auditor
- AXELOS M_o_R® (2010) Foundation
- Privacy Implementer PECB-CLPI ISO29100™
- Privacy Consultant

Introduzione alla protezione dei dati

Introduzione alla protezione dei dati

Esistono persone che NON posseggono
Dati Personali?

Esistono organizzazioni che NON utilizzano
Dati Personali?

L'argomento ci coinvolge tutti!

Introduzione alla protezione dei dati

Le istituzioni europee sono state sempre sensibili al tema della «riservatezza» sin dalla loro costituzione.

- Nel 1950, il diritto al **rispetto della vita privata** fu consacrato dall'art. 8 della Convenzione Europea.

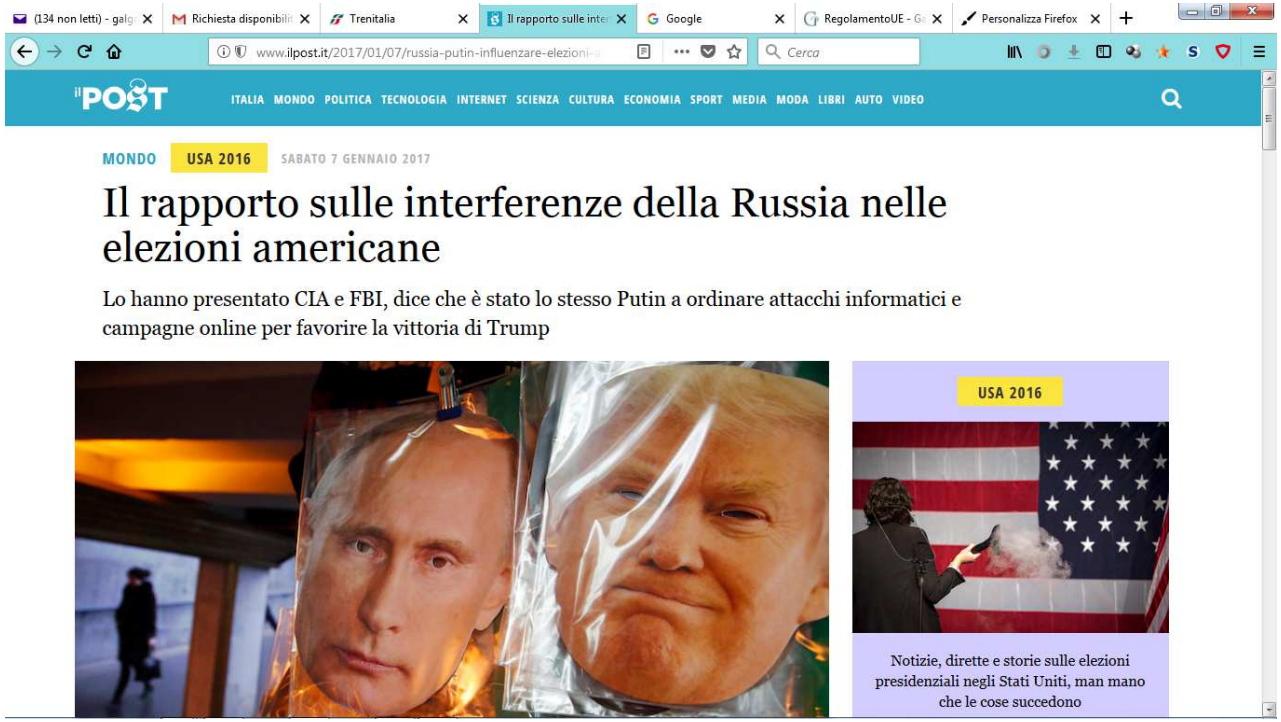
- Nel 2000 la Protezione dei dati di carattere personale è sancito come **diritto fondamentale** dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea

Introduzione alla protezione dei dati
Dalla parte dei cittadini

Perché tutta questa attenzione?
Perché è importante proteggere i Dati Personali?

- Pubblicità non gradite
- Concorrenza sleale
- Discriminazioni
- Manipolazioni
- … …

Introduzione alla protezione dei dati
Dalla parte dei cittadini



Utilizzando in modo *raffinato* i Dati Personali si possono manipolare le persone o le masse

Introduzione alla protezione dei dati
Dalla parte delle organizzazioni

Perché tutta questa attenzione?
Perché è importante proteggere i Dati Personali?

- Evitare costi per la non conformità

- Mantenimento della reputazione
  Tutte le organizzazioni, pubbliche e private, possono subire importanti conseguenze sulla loro reputazione in caso di violazioni alla norma o in caso di violazioni di dati personali.
  Conseguenze possibili sono perdita di credibilità e riduzione di finanziamenti o di giro d'affari.

Introduzione alla protezione dei dati
Dalla parte delle organizzazioni

Money transfer: Garante privacy, 11 mln di multa a cinque società per uso illecito di dati

Sanzioni per oltre 11 milioni di euro sono state comminate dal Garante privacy a cinque società che operano nel settore del money transfer per aver usato in modo illecito i dati personali di più di mille persone inconsapevoli

(estratto da: www.garanteprivacy.it)

Introduzione alla protezione dei dati

Cittadini e organizzazioni come possono cautelarsi?

Acquisendo maggiore consapevolezza

Introduzione alla protezione dei dati
Siamo consapevoli? Gli utenti

Ingenuità della gente riguardo i propri dati personali

Introduzione alla protezione dei dati
Siamo consapevoli? Le organizzazioni

Gran Bretagna: attacco hacker a gestore telefonico TalkTalk. A rischio i dati di 4 milioni di utenti

Alcuni utenti hanno già denunciato che sono state sottratte centinaia di sterline dai loro conti dopo che i pirati informatici hanno colpito. A TalkTalk inoltre è arrivata un'insolita "richiesta di riscatto", tramite un'email, di cui non è stata rivelata l'entità. E' probabile che il riscatto riguardi proprio i dati che sono stati sottratti nel corso dell'attacco

23 ottobre 2015

Fonte: http://www.rainews.it/

Introduzione alla protezione dei dati
Siamo consapevoli? Le organizzazioni

FINECO
BANK

Introduzione alla protezione dei dati

Cittadini e organizzazioni come possono cautelarsi?

Acquisendo maggiore consapevolezza

Conoscendo e applicando le regole

Il Regolamento UE 679/2016 (GDPR)

Il Regolamento UE 679/2016

Fonti di diritto derivato: due strumenti della UE

Le **DIRETTIVE**
Sono indirizzate solo agli Stati membri e non sono obbligatorie in tutti i loro elementi, in quanto vincolano i destinatari solo riguardo al risultato da raggiungere, lasciando alla loro discrezione la scelta dei mezzi e della forma

I **REGOLAMENTI**
Hanno una portata generale, sono obbligatori in tutti i loro elementi e direttamente applicabili

Il Regolamento UE 679/2016

La prima norma organica dell'Unione europea è stata la **Direttiva 95/46 (Tutela e libera circolazione dei dati personali)**.

A questa sono poi seguite

- Direttiva 2002/58 CE (Telecomunicazioni)
- Direttiva 2006/24 CE (Conservazione di dati)
- Decisione quadro 977/2008 (dati scambiati dalle autorità di polizia)
- Direttiva 2009/136 CE (E-Privacy)
- …

I testi dei documenti sono disponibili nel sito http://eur-lex.europa.eu

Il Regolamento UE 679/2016

In Italia la direttiva 95/46 CE è stata recepita tramite il
D.Lgs. 196 del 30 giugno 2003
Codice in materia di protezione dei dati personali
(Codice delle Privacy)

Il Codice della Privacy ha, tra le altre, disciplinato
l'Autorità Garante per la protezione dei dati personali
(G.P.D.P.)
autorità amministrativa indipendente che si occupa di tutti gli ambiti, pubblici e privati, nei quali occorre assicurare il corretto trattamento dei dati e il rispetto dei diritti delle persone connessi all'utilizzo delle informazioni personali.

Il testo del Codice Privacy è disponibile nel sito http://www.garanteprivacy.it

Il Regolamento UE 679/2016

Rispetto alla normativa di base adottata oltre 20 anni fa sono intervenuti:

1. Cambiamenti nel contesto

- Fenomeno della globalizzazione
- Nuove tecnologie
- Nuovi servizi collegati alle nuove tecnologie

2. Frammentazione e disomogeneità del quadro normativo

- Tempi e modi diversi, da parte dei 28 paesi membri, di recepire la direttiva 95/46 CE e le successive norme
- Provvedimenti in materia Privacy adottati dai singoli stati

Per dare una risposta ai due punti nasce la nuova normativa europea

Il Regolamento UE 679/2016

Il 24 maggio 2016, dopo l'approvazione e la pubblicazione in Gazzetta ufficiale dell'Unione europea, è entrato in vigore il **GDPR** o, in modo completo,

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

Il GDPR diverrà totalmente operativo a partire dal **25 maggio 2018**

.. e il Codice della Privacy che fine fa?

Il Regolamento UE 679/2016

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Gdpr, Garante privacy: nessuna pronuncia su differimento applicazione sanzioni

Con riferimento a notizie circolanti in Internet è necessario precisare che non è vero che il Garante per la protezione dei dati si sia pronunciato sul differimento dello svolgimento delle funzioni ispettive e sanzionatorie né il provvedimento richiamato nei siti attiene a tale materia.

Nessun provvedimento del Garante, peraltro, potrebbe incidere sulla data di entrata in vigore del Regolamento europeo fissata al 25 maggio 2018.

Roma, 19 aprile 2018

Il Regolamento UE 679/2016

Il Regolamento

- definisce i principi
- governa i rapporti tra i vari attori coinvolti

al fine di tutelare i dati personali delle persone fisiche

… ancora sul Regolamento UE

Alcune definizioni

Dato personale

qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

… ancora sul Regolamento UE

Alcune definizioni

Trattamento

qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

… ancora sul Regolamento UE

Le figure: ruoli e responsabilità

Interessato

è il proprietario del dato personale (nelle scuole: studenti e dipendenti).

L'interessato affida i propri dati alle organizzazioni per specifiche e identificate finalità sulla base di un rapporto fiduciario disciplinato dal Regolamento

… ancora sul Regolamento UE

Le figure: ruoli e responsabilità

Titolare
persona fisica o giuridica (entità nel suo complesso) cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo di sicurezza.

È il "garante supremo" della fiducia dell'interessato.

Risponde all'interessato e all'Autorità Garante del trattamento dei Dati Personali.

Può avvalersi di figure di supporto.

… ancora sul Regolamento UE

Le figure: ruoli e responsabilità

Responsabile
persona fisica o giuridica (entità nel suo complesso) preposto dal titolare al trattamento di dati personali.

È una figura facoltativa ma, se il titolare affida all'esterno della propria organizzazione dei trattamenti, deve essere sempre individuato e formalmente nominato.

Esempi di affidamenti esterni

- Gestore mensa
- Strutture per progetti alternanza scuola lavoro
- RSPP
- Servizi di assistenza informatica
- Servizi di cloud
- Dismissione PC
- …

… ancora sul Regolamento UE

Le figure: ruoli e responsabilità

Responsabile
È individuato dal titolare tra coloro che, per esperienza, capacità e affidabilità, fornisce idonea garanzia circa il rispetto delle disposizioni vigenti in materia dei Dati Personali.

Nel Sistema Protezione Dati Personali la risorsa, l'organizzazione o il professionista nominati responsabile del trattamento devono avere competenze elevate.

Può rispondere di eventuali danni cagionati all'interessato.

… ancora sul Regolamento UE

Le figure: ruoli e responsabilità

Spetta al Titolare e al Responsabile:

- la definizione dei compiti, dei ruoli e delle responsabilità per la gestione di tutte le fasi del trattamento dei dati personali, con particolare riferimento alla necessità di garantire la loro sicurezza;
- l'adozione di specifiche procedure atte a completare e rafforzare le contromisure tecnologiche presenti.

… ancora sul Regolamento UE

Le figure: ruoli e responsabilità

Persone autorizzate al trattamento
Sono così identificate tutte le persone fisiche che operano su dati personali per conto del titolare o del responsabile.

Il Regolamento specifica che chiunque agisca sotto l'autorità del titolare o del responsabile del trattamento, che abbia accesso a dati personali, **non può trattare tali dati se non è istruito** in tal senso dal titolare del trattamento.

Le istruzioni devono essere impartite tramite:

- **formazione**
- **lettere**
- **mansionario**
- **disciplinare interno**

… ancora sul Regolamento UE

Le figure: ruoli e responsabilità

DPO o RPD

È una figura di garanzia, già contemplata da alcune legislazioni europee, introdotta in Italia dal Regolamento.

Quando è previsto

Dovranno designare obbligatoriamente un Responsabile della protezione dei dati personali:

a) **amministrazioni ed enti pubblici, fatta eccezione per le autorità giudiziarie;**

…

… ancora sul Regolamento UE

Le figure: ruoli e responsabilità

DPO o RPD

Quando è previsto

Dovranno designare obbligatoriamente un Responsabile della protezione dei dati personali:

…

b) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il controllo regolare e sistematico degli interessati su **larga scala**;

c) tutti i soggetti la cui attività principale consiste nel trattamento, su **larga scala**, di categorie particolari di dati personali (1) o di dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

(1) Dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

… ancora sul Regolamento UE

Le figure: ruoli e responsabilità

DPO o RPD

Caratteristiche

Al titolare spetta individuare e nominare il DPO che deve essere designato in funzione delle qualità professionali, in particolare della **conoscenza specialistica della normativa e delle prassi in materia di protezione dei Dati Personali e della capacità di assolvere i compiti previsti dal Regolamento**.

Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

… ancora sul Regolamento UE

Le figure: ruoli e responsabilità

DPO o RPD

I compiti

Il Regolamento specifica che il DPO deve almeno svolgere i seguenti compiti:

- **informare** e fornire consulenza al Titolare …;
- **sorvegliare** l'attuazione e l'applicazione …;
- **fornire**, se richiesto, un parere …;
- **cooperare** con l'Autorità di controllo …;
- **fungere** da punto di contatto per ….

Non è una figura operativa ma consultiva e di garanzia.
La sola presenza di un "vero" DPO aumenta la conformità aziendale alla normativa agli occhi dell'Autorità Garante, degli interessati e dell'opinione pubblica.

… ancora sul Regolamento UE

Principali novità del Regolamento

Accountability

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto **misure tecniche e organizzative adeguate** per garantire, ed **essere in grado di dimostrare**, che il trattamento è effettuato conformemente al Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

… ancora sul Regolamento UE

Principali novità del Regolamento

Sanzioni

Per trattamenti dei dati personali non conformi, le sanzioni amministrative possono arrivare fino

a **20.000.000 di euro**

o, nel caso di impresa,

al **4% del fatturato mondiale annuo dell'esercizio precedente**

(vale la maggiore tra le due).

In aggiunta, il regolamento riconosce all'interessato il diritto al risarcimento del danno da parte del titolare o del responsabile del trattamento.

A questo si possono aggiungere **ulteriori sanzioni** del legislatore nazionale e, in primo luogo, quelle di natura penale.

… ancora sul Regolamento UE

Le regole base del trattamento

I dati personali devono essere

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (**liceità, correttezza e trasparenza**)
- raccolti per finalità determinate, esplicite e legittime (**limitazione della finalità**)
- esatti e, se necessario, aggiornati; ovvero cancellati o rettificati tempestivamente rispetto alle finalità per le quali sono trattati (**esattezza**)
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (**minimizzazione dei dati**)
- conservati in modo da consentire l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (**limitazione della conservazione**)
- trattati in maniera da garantirne un'adeguata sicurezza (**integrità e riservatezza**)

Il titolare del trattamento è competente per l'osservanza di questi principi fondamentali e deve essere in grado di comprovarne il rispetto.

Le principali azioni da compiere

Le principali azioni da compiere

Passi operativi obbligatori (1/3)

- Redazione della politica per la protezione dei dati personali dell'istituto
- Individuazione dei trattamenti effettuati e delle relative basi legali
- Predisposizione informativa studenti minorenni
- Predisposizione informativa studenti maggiorenni
- Predisposizione informativa dipendenti
- Predisposizione informativa sito web scolastico
- Predisposizione lettera di nomina Ministero per trattamento dati studenti
- Predisposizione procedura gestione del consenso degli interessati (minorenni, maggiorenni, dipendenti)
- Predisposizione regolamento gestione videosorveglianza e istruzioni operative (se presente)
- Regolamento utilizzo strumenti aziendali (compreso laboratorio informatico)
- …

Le principali azioni da compiere

Passi operativi obbligatori (2/3)

- Facsimile di Nomina a Responsabile del Trattamento per eventuali fornitori con accesso ai dati (manutentori, registro elettronico, cloud, servizi sociali, gite e visite)
- Facsimile clausole protezione dati personali per fornitori
- Processo gestione violazioni - schede sintetiche di supporto: cosa fare e come agire
- Gestione diritti degli interessati - schede sintetiche di supporto: cosa fare
- Istruzioni per gestione PC e password dipendenti con definizione di compiti e ambiti (segreteria, amministrazione, dirigente, professori, tecnici)
- Facsimile di nomina dell'Amministratore di sistema
- Guida operativa per IT - Cosa fare in caso di cloud, verifiche AGID con requisiti base
- …

Le principali azioni da compiere

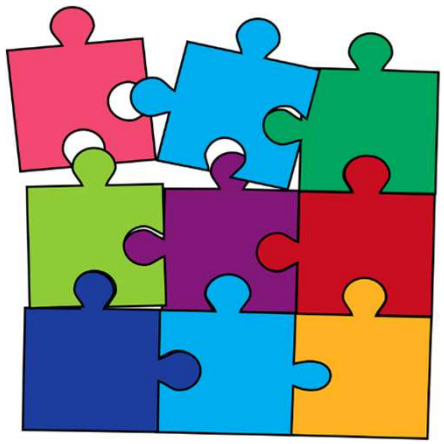
Passi operativi obbligatori (3/3)

- Gestione documenti privacy - istruzioni per la conservazione dei documenti elettronici e cartacei - eventuale smaltimento
- Linee guida valutazione fornitori
- Predisposizione corsi interni - 2 ore tutto il personale
- Predispostone corsi per personale amministrativo e di segreteria e dirigenti - ulteriori 2 ore
- Erogazione corsi
- Registro del trattamento - fac-simile con personalizzazione
- Revisione annuale privacy - aggiornamenti documentali
- Individuazione e nomina del DPO e relativa comunicazione all'Autorità Garante

Implicazioni operative

Alcune implicazioni operative

- Informativa
- Raccolta e gestione del consenso
- Gestione diritti interessati
- Gestione violazioni
- Registro del trattamento
- Gestione videosorveglianza
- Rapporti fornitori terzi
- Formazione/istruzioni addetti al trattamento
- Gestione delle evidenze
- Identificazione e nomina del DPO



Implicazioni operative

Informativa

È il documento fondamentale per instaurare il rapporto tra titolare e interessato, deve essere personalizzato rispetto alla propria organizzazione e deve essere sottoposto all'interessato ogni volta che si raccolgono, direttamente o indirettamente, dati personali. Deve indicare:

- **l'identità e i dati di contatto del titolare del trattamento e, se presente, del responsabile della protezione dei dati personali**
- **le finalità, la durata e le basi di legittimità del trattamento**
- **gli eventuali destinatari dei dati personali**
- in caso di trasferimenti verso paesi terzi o organizzazioni internazionali, dettagli in merito al luogo di trasferimento e all'esistenza di garanzie adeguate per la tutela dei loro diritti
- **le possibili conseguenze di un mancato conferimento dei dati personali**
- l'eventuale utilizzo di strumenti di profilazione o l'esistenza di decisioni automatizzate che lo riguardano
- **la possibilità di esercitare i diritti previsti e la possibilità di proporre reclami**

Implicazioni operative

Raccolta e gestione del consenso

Il consenso è lo strumento necessario per effettuare trattamenti di dati personali; esistono casi specificati nel Regolamento in cui non è obbligatorio raccoglierlo e in generale è sempre richiesto nel caso di trattamento di dati personali:

- rientranti tra le categorie particolari di dati personali (origine razziale o etnica, relativi alla salute, alla religione, all'appartenenza sindacale, ecc.)
- relativi alle condanne penali e ai reati o a connesse misure di sicurezza

Comunque, per trattare questi dati, l'autorità garante ha specificato che il consenso **non va richiesto in presenza di una idonea base normativa**. Tuttavia, oltre a dover essere espressamente previsto, sono richieste speciali cautele e il trattamento può essere effettuato **solo se i dati indicati sono indispensabili per l'attività istituzionale** svolta.

Quando previsto, il consenso va gestito per tutta la durata del trattamento.

Implicazioni operative

Gestione diritti interessati

Il Regolamento disciplina i diritti (introducendone di nuovi) che ogni interessato può esercitare nei confronti dei titolari. Quest'ultimo dovrà predisporre specifiche procedure che consentano di rispondere e adempiere alle richieste ricevute nei tempi e nei modi stabiliti.

Tra i diritti esercitabili dall'interessato ricordiamo:

- diritto di accesso (da non confondere con i diritti di accesso agli atti amministrativi, regolato dalla Legge n. 241 del 1990 e s.m., e ai dati e ai documenti detenuti dalla P.A., regolato dal D.lgs. n.33 del 2013 e s.m.;
- diritto di rettifica;
- diritto alla cancellazione (diritto all'oblio);
- diritto di limitazione;
- diritto alla portabilità dei dati;
- diritto di opposizione;
- diritto di non essere sottoposto a un processo decisionale automatizzato.

Implicazioni operative

Tutti coloro che:

- trattano dati personali
- ricevono dati personali
- entrano in contatto con dati personali nell'erogazione di un contratto di servizio

devono:

- essere opportunamente istruiti
- agire, se del caso, in virtù di un contratto o di un atto giuridico vincolante che stabilisca chiaramente compiti, responsabilità e confini del trattamento
- essere selezionati in virtù di competenze e caratteristiche possedute, sulla base del principio di responsabilizzazione del titolare

Un cenno alle violazioni e alle loro cause

Le minacce diventano ogni giorno più sofisticate e sono in grado di causare danni finanziari su scala mondiale.
Anche se la quasi totalità degli attacchi ha obiettivi finanziari precisi, nel caso di enti o agenzie pubbliche il danno principale è la **reputazione**.
Gli analisti prevedono che gli attacchi continueranno a crescere.

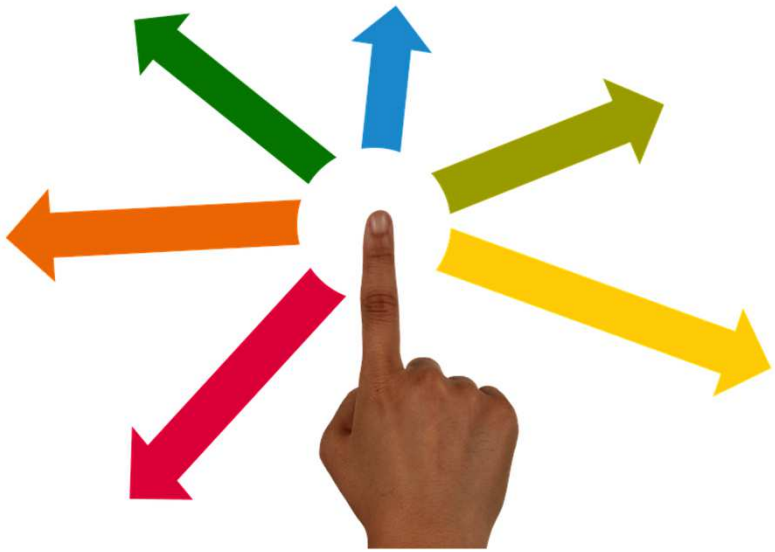
Se si escludono gli eventi legati a azioni mirate di hacker, le principali cause degli incidenti riguardano:

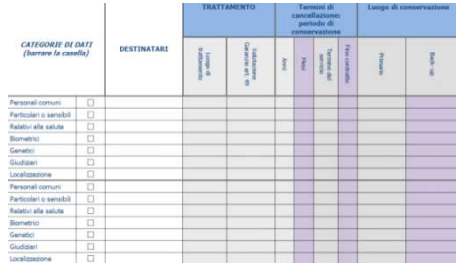
- negligenze o disattenzioni
- mancata adozione di cautele elementari o mancato rispetto dei comportamenti raccomandati
- errata valutazione delle priorità aziendali o ritardi nell'attuazione di misure elementari di protezione.

Implicazioni operative

Nomine

- Ciascun Responsabile del Trattamento (entità fisica e giuridica diversa dal Titolare del trattamento) **deve essere formalmente nominato**
- L'eventuale Responsabile della Protezione dei dati personali (RPD o DPO) – obbligatorio per tutti i soggetti pubblici e in alcuni casi particolari – **deve essere formalmente nominato**. Il suo nome deve essere comunicato all'Autorità Garante.





Implicazioni operative

Registro del trattamento

Titolare ed eventuale Responsabile, ciascuno per la propria parte, compilano obbligatoriamente il **Registro delle attività di trattamento** svolte dall'organizzazione.

Il Registro del titolare deve contenere

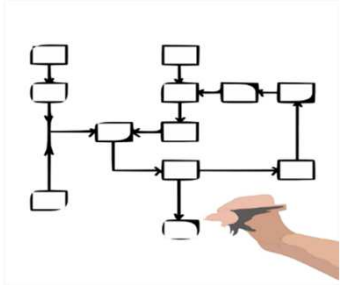
- nome e contatti del Titolare, del suo Rappresentante e, se del caso, del Responsabile della protezione dei dati;
- le finalità del trattamento, inclusi gli eventuali legittimi interessi;
- la descrizione delle categorie di interessati;
- la descrizione delle categorie di dati;
- le categorie di eventuali destinatari, inclusi quelli collocati in paesi terzi (non UE);
- la documentazione delle garanzie adeguate per tutti i trasferimenti verso i paesi terzi che avvengono nelle situazioni descritte all'articolo 49;
- i termini di cancellazione dei dati personali;
- la descrizione generale delle misure di sicurezza tecnico-organizzative.

Implicazioni operative

Misure tecnico – organizzative adeguate al contesto
Ogni specifica situazione richiede l'implementazione di «*misure tecniche e organizzative adeguate a garantire un livello di sicurezza* ***adeguato al rischio***»

Esse possono includere
- l'adozione di strumenti tecnici
- la revisione delle procedure esistenti, delle politiche o dei processi
- la modifica di alcune delle applicazioni IT utilizzate
- l'implementazione di nuovi processi

Ogni decisione richiede una **valutazione preventiva e accurata dei rischi** connessi al trattamento di dati personali

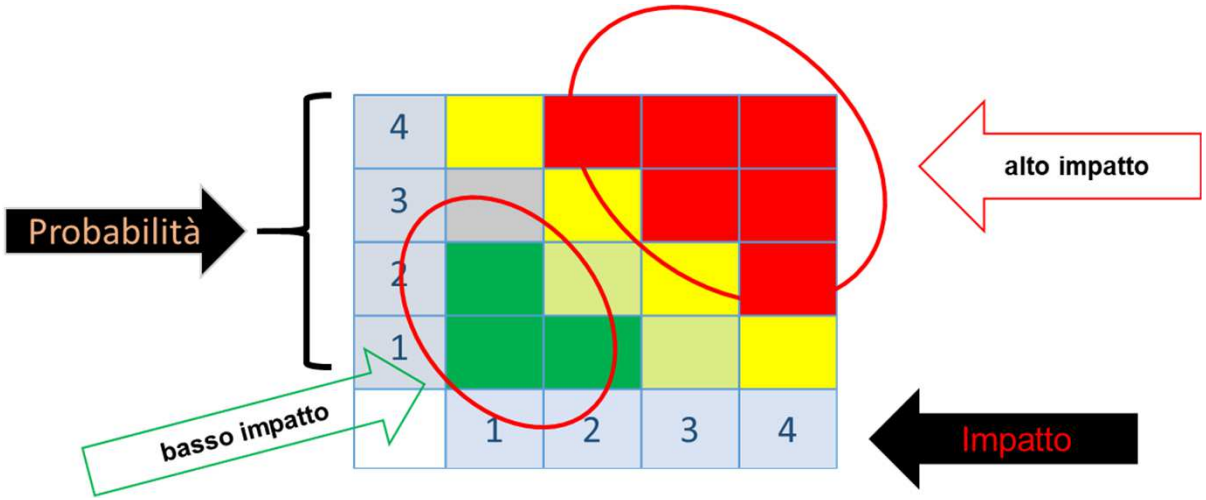


Implicazioni operative

Analisi del rischio

I rischi connessi al trattamento dei dati personali devono essere:

- identificati
- descritti
- valutati
- ridotti o mitigati con opportune azioni
- costantemente monitorati



Implicazioni operative

Ulteriori punti di attenzione

- Processi e procedure esistenti devono essere esaminati, valutati e probabilmente rivisti o, se non presenti, implementati
- Privacy by default e privacy by design
- Trasferimento di dati personali verso paesi non UE
- Risorse dedicate alla protezione dei dati (umane ed economiche)
- Opportunità di implementare e mantenere un sistema di gestione dei dati personali
- Possibilità di aderire a Codici di Condotta di settore o di sottoporsi a specifica certificazione
- Inserimento dei rischi legati al trattamento dei dati personali nella mappatura dei rischi aziendali
- Conservazione delle evidenze
- Gestione delle diverse versioni dei documenti

Punti di attenzione degli istituti scolastici

Ruolo:
- titolare del trattamento
- responsabile del trattamento incaricato dal MIUR

Interessati:
- studenti e famiglie
- personale scolastico e collaboratori

Destinatari dei dati
- MIUR
- enti locali competenti
- altre strutture pubbliche (INPS, INAIL, ASL, ecc.)
- servizi sociali
- fornitori (sevizi mensa, visite e gite, alternanza scuola lavoro, RSPP, assistenza informatica, ecc.)
- strutture/organizzazioni per finalità di orientamento, formazione e inserimento professionale

Possono anche essere fonte dei dati

Punti di attenzione degli istituti scolastici

Categorie di dati trattati: studenti

- anagrafici comuni
- dati di contatto
- dati relativi alla salute dell'interessato e/o dei familiari
- informazioni giudiziarie e eventuali contenziosi
- convinzioni religiose
- origini razziali ed etniche

Categorie di dati trattati: dipendenti e collaboratori

- anagrafici comuni
- dati di contatto
- dati relativi alla salute dell'interessato e/o dei familiari
- informazioni giudiziarie
- convinzioni religiose
- appartenenza sindacale

Punti di attenzione degli istituti scolastici

Istruzioni al personale docente:

- acquisizione di consapevolezza
- gestione dei documenti cartacei (compiti in classe, comunicazioni varie, ecc.)
- utilizzo dei laboratori informatici
- gestione delle password e accesso al registro elettronico
- linee guida operative per situazioni particolari

Incontri informativi con gli studenti:

- acquisizione di consapevolezza – cittadini del domani
- pericoli connessi all'utilizzo dei social
- utilizzo dei laboratori informatici e dei dispositivi personali connessi

Punti di attenzione degli istituti scolastici

Istruzioni al personale amministrativo e di segreteria:

- acquisizione di consapevolezza
- gestione dei documenti cartacei
- la posta elettronica
- la gestione dei documenti «sensibili»
- linee guida operative per fronteggiare situazioni critiche
- assegnazione di responsabilità
- valutazione e controllo dei fornitori

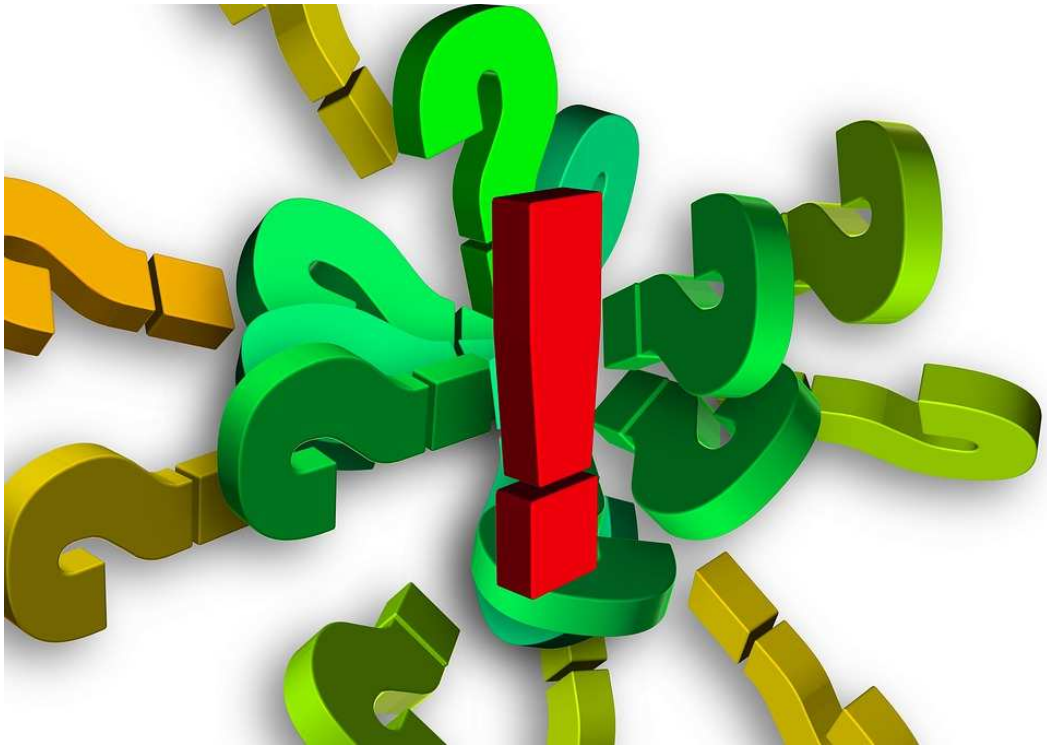
Altro

- il sito web scolastico
- i sistemi di videosorveglianza
- curriculum e identità digitale dello studente
- regolamentazione sull'utilizzo di registratori, smartphone, tablet e altri dispositivi elettronici
- pubblicità e trasparenza

Può darsi che non siate responsabili per la situazione in cui vi trovate, ma lo diventerete se non fate nulla per cambiarla.

Martin Luther King

Domande o commenti



Grazie per l'attenzione

Giuseppe Galgano
giuseppe.galgano@privacyinchiaro.it

Paola Limatola
paola.limatola@privacyinchiaro.it

Sebastiano Plutino
sebastiano.plutino@privacyinchiaro.it