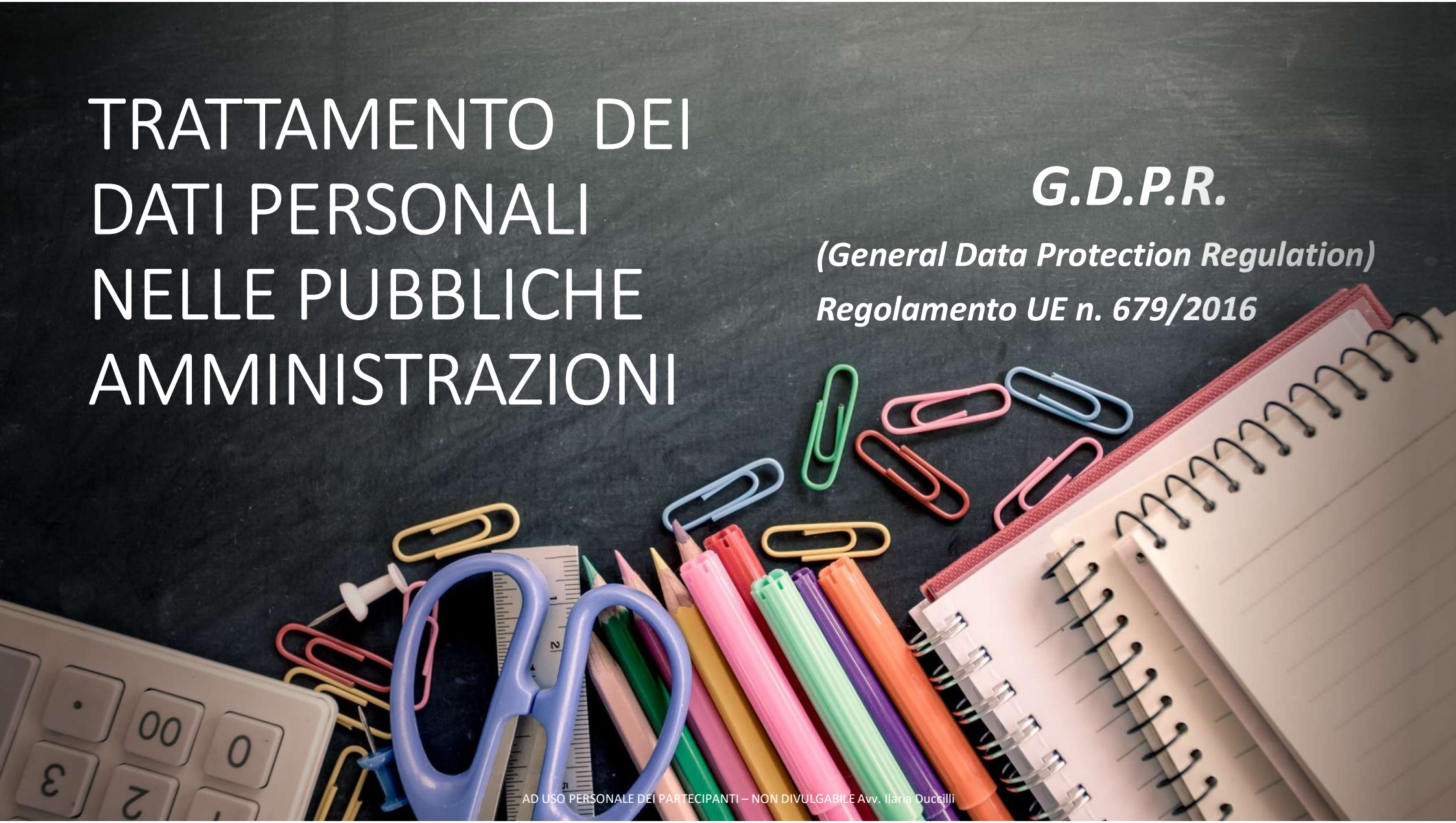
TRATTAMENTO DEI DATI PERSONALI NELLE PUBBLICHE AMMINISTRAZIONI

G.D.P.R.

(General Data Protection Regulation)

Regolamento UE n. 679/2016



LE PRINCIPALI FONTI

- REGOLAMENTO UE N. 679 /2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

- DECRETO LEGISLATIVO 101/2018 (in vigore dal 19.09.2018) di adeguamento al G.D.P.R. della normativa nazionale (Codice Privacy D.Lgs. 196/2003)

ENTRATA IN VIGORE ED APPLICAZIONE (art. 99 G.D.P.R.)

- Il Reg. UE 679/16 (approvato il 14 aprile 2016 dal Parlamento) è stato pubblicato nella Gazzetta Ufficiale dell'Unione Europea n. 119/2016: 4 Maggio 2016
- è entrato in vigore: 24 Maggio 2016
- Si applica in tutti i Paesi della UE dal 25 Maggio 2018. I Paesi della UE hanno avuto due anni di tempo per adeguare alle nuove norme le politiche del trattamento dei dati.
- Dal 25 maggio 2018 **il Regolamento è immediatamente applicabile senza necessità di recepimento**
- La direttiva 95/46 CE è stata abrogata a decorre dal 25 maggio 2018

COSA E' ACCADUTO ALLA NORMATIVA ITALIANA?

Il D.LGS. 101/2018 (entrato in vigore il 19.09.2018) di adeguamento della normativa nazionale al G.D.P.R. ha:

- ABROGATO le disposizioni del Codice privacy (D.lgs. N. 196/2003) incompatibili con il G.D.P.R.;
- MODIFICATO il Codice Privacy, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento (UE) 2016/679;
- COORDINATO le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate dal G.D.P.R.
- ha reinserito le sanzioni penali non previste dal G.D.P.R.

A CHI SI APPLICA IL G.D.P.R.? (art. 2 G.D.P.R.)

- Solo al **trattamento dei dati personali di persone fisiche**;
- Riguarda trattamenti **interamente o parzialmente automatizzati e i trattamenti non automatizzati se i dati personali sono contenuti in un archivio o sono destinati a confluirvi.**
- Non si applica al trattamento dei dati personali di persone decedute, ma gli Stati membri possono prevedere delle norme, come ha fatto l'Italia.
- **Non si applica al trattamento di dati di persone giuridiche.**

<u>Il Regolamento non si applica ai trattamenti di dati personali effettuati:</u>

- da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico (considerando 18);
- per attività che non rientrano nell'ambito di applicazione del diritto dell'UE (sicurezza nazionale);
- dagli Stati membri nell'esercizio delle attività che riguardano la politica estera e di sicurezza comune dell'UE;
- da autorità di pubblica sicurezza

AMBITO DI APPLICAZIONE TERRITORIALE (art. 3 GDPR)

Il Regolamento si applica al trattamento:

- dei dati personali effettuato da un Titolare o Responsabile stabilito nella UE, indipendentemente dal fatto che il trattamento sia effettuato o meno nella UE;
- di dati personali, effettuato da Titolari o Responsabili non stabiliti nell'UE, quando ha ad oggetto dati personali di interessati che si trovano nella UE e riguarda l'offerta di beni o servizi (anche non a pagamento) ai suddetti interessati oppure il monitoraggio del loro comportamento nel territorio della UE;
- effettuato da un Titolare che non stabilito nell'UE, ma in un luogo soggetto al diritto di uno Stato UE in virtù del diritto internazionale pubblico (esempio rappresentanza diplomatica o consolare di uno Stato membro)

Cosa sono i DATI PERSONALI?

Per «DATI PERSONALI», ai sensi **dell'art. 4 del Regolamento UE**, si intendono le informazioni riguardanti 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.

Esempi di dati personali:

- Identificativi: nome e cognome; numero della carta d'identità;
- di contatto: indirizzo di casa; indirizzo e-mail, come nome.cognome@minerbio.it
- dati sulla posizione (ad es. la funzione di posizionamento su un telefono cellulare)*;
- Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro...)
- dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, etc)
- un indirizzo IP (Internet Protocol);
- un ID cookie* per la navigazione su siti

*In alcuni casi è prevista una normativa settoriale specifica che regola, ad esempio, l'uso dei dati relativi alla posizione o all'uso dei cookie: la direttiva e-privacy (direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 (GU L 201 del 31.7.2002, pag. 37) e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio del 27 ottobre 2004 (GU L 364 del 9.12.2004, pag. 1).

(Fonte tratta da: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_i)

Esempi di dati NON personali:

- Codice Fiscale dell'IC Minerbio;
- Indirizzo pec, come: boic82700p@pec.istruzione.it
- dati resi anonimi (affinché i dati siano considerati veramente anonimi, l'anonimizzazione deve essere irreversibile).

<u>Per approfondimenti:</u>

- Articolo 2, articolo 4, punti 1 e 5; considerando 14, 15, 26, 27, 29 e 30 del regolamento
- WP 01248/07/IT, WP 136 - Parere 4/2007 sul concetto di dati personali
- Gruppo di lavoro ex articolo 29 - Parere 05/2014 sulle tecniche di anonimizzazione

DATI SENSIBILI E GIUDIZIARI?

NEL G.D.P.R. NON SI USA PIU' QUESTA TERMINOLOGIA

SI PARLA DI CATEGORIE PARTICOLARI DI DATI (ART. 9)

E

DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (ART. 10)

CATEGORIE PARTICOLARI DI DATI PERSONALI (art. 9 G.D.P.R.) «ex dati sensibili»

Dati che:

- **rivelino l'origine razziale o etnica**:
- **le opinioni politiche**:
- **le convinzioni religiose**
- **dati relativi alla salute:**
- l'appartenenza sindacale,
- dati genetici,
- dati biometrici intesi a identificare in modo univoco una persona fisica,
- dati relativi alla vita sessuale o all'orientamento sessuale della persona

Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

CATEGORIE PARTICOLARI DI DATI PERSONALI (art. 9 G.D.P.R.) «ex dati sensibili» Quali dati «sensibili» tratta la Scuola?

- **Dati idonei a rivelare l'origine razziale o etnica:** possono essere trattati dalla scuola per favorire l'integrazione degli alunni stranieri
- **le convinzioni religiose:** trattati per la fruizione insegnamento religione cattolica o delle attività alternative a tale insegnamento.
- **dati relativi alla salute:** l'assegnazione del sostegno agli alunni disabili; per la composizione delle classi; per la gestione delle assenze per malattia; per l'insegnamento domiciliare e ospedaliero nei confronti degli alunni affetti da gravi patologie; per la partecipazione alle attività sportive, alle visite guidate e ai viaggi di istruzione.
- **le opinioni politiche**: per garantire la costituzione e il funzionamento degli organismi di rappresentanza: ad esempio, le consulte e le associazioni degli studenti e dei genitori.

DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (art. 10)

Sono dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati.

QUANDO LA SCUOLA PUÒ TRATTARE DATI GIUDIZIARI?

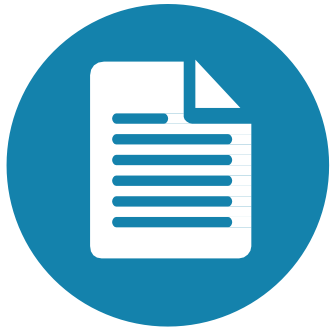
Ad esempio: - per assicurare il diritto allo studio a soggetti sottoposti a regime di detenzione o di protezione.

- Per finalità di difesa in giudizio (contenziosi con gli alunni e con le famiglie: reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce all'autorità giudiziaria, etc.) e in generale in caso di contezioso

LE NOVITA'

LE FIGURE PRIVACY

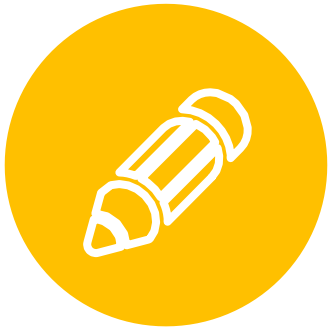
IL CONSENSO



L'INFORMATIVA

NUOVI DIRITTI

DATA BREACH



PRIVACY BY DESIGN

ACCOUNTABILITY

Chi sono i Protagonisti

PERSONA FISICA
Soggetto interessato dal trattamento dei dati personali

DPO
Data Protection Officer

RESPONSABILE
della Protezione dei DATI

CONTITOLARE

TITOLARE
del Trattamento

RESPONSABILE
del Trattamento

Soggetto autorizzato al trattamento

SOGGETTI INTERESSATI IN AMBITO SCOLASTICO

Il soggetto interessato è la persona fisica alla quale si riferiscono i dati

<u>In ambito scolastico sono soggetti interessati:</u>

- gli studenti
- Le famiglie
- I docenti
- DS, DSGA, assistenti amministrativi, collaboratori scolastici
- consulenti
- fornitori

TITOLARE DEL TRATTAMENTO

Chi è il Titolare del trattamento?

È la persona fisica o giuridica, **l'autorità pubblica**, il servizio o altro organismo che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento di dati personali**

(Parere Autorità Garante 9 dicembre 1997 sull'individuazione del Titolare del Trattamento)

Cosa deve fare?

- Deve mettere in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è conforme al GDPR (principio di ACCOUNTABILITY)
- Dette misure devono essere riesaminate e aggiornate

Parere Autorità Garante 9 dicembre 1997 sull'individuazione del Titolare del Trattamento

«qualora il trattamento sia effettuato nell'ambito di una persona giuridica, di una pubblica amministrazione o di un altro organismo, **il «titolare» è l'entità nel suo complesso** (ad esempio, la società, il ministero, l'**ente pubblico,** l'associazione, ecc.) **anziché taluna delle persone fisiche che operano nella relativa struttura e che concorrono, in concreto, ad esprimerne la volontà o che sono legittimati a manifestarla all'esterno** (ad esempio, l'amministratore delegato, il ministro, il direttore generale, il presidente, il legale rappresentante, ecc.).

Nel caso dell'Istituzione scolastica il Titolare è il Liceo, rappresentata dal DS pro tempore

CONTITOLARI DEL TRATTAMENTO (art. 26)

La contitolarità ricorre allorquando due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento.

Sono i soggetti ai quali competono le decisioni in ordine alle finalità, alle

modalità del trattamento di dati personali e agli strumenti utilizzati.

Esempio: MIUR e Istituto Scolastico

RESPONSABILE DEL TRATTAMENTO (art. 28 G.D.P.R.)

Chi è il Responsabile del Trattamento?

- La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- Deve presentare garanzie sufficienti, ovvero deve essere in grado di garantire misure tecniche e organizzative adeguate,
- Il responsabile del trattamento non può ricorrere ad un altro responsabile senza previa autorizzazione del titolare
- Esempi di Responsabili del trattamento: fornitori registri elettronici, fornitori posta elettronica, fornitori piattaforme DAD e DDI

Come viene nominato?

Con un contratto o altro atto giuridico che indichi:

- la durata del trattamento
- la natura e la finalità del trattamento
- il tipo di dati personali e le categorie di interessati
- gli obblighi e i diritti del titolare del trattamento.

SUB RESPONSABILE ART. 28, IV COMMA G.D.P.R.

- Nel caso in cui il fornitore dei servizi si avvalga di altro fornitore per il trattamento dei dati, dovrà essere esplicitamente autorizzato per iscritto dall'istituzione scolastica a designarlo sub-responsabile, in maniera specifica o generale, rendendo disponibile al titolare del trattamento l'elenco di tali soggetti (art. 28, par. 2 del Regolamento).
- Il sub-responsabile dovrà attenersi agli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra l'istituzione scolastica e il primo responsabile.
- Il fornitore che si avvalga di sub-responsabili risponde direttamente nei confronti dell'istituzione scolastica in relazione ad eventuali inadempimenti o violazioni della propria catena di subfornitura.

I CONTRATTI CON I FORNITORI PER L'ATTIVAZIONE DELLA DAD E DID

- Didattica a distanza: prime indicazioni del Garante privacy - Provvedimento 26 marzo 2020

- Linee Guida sulla DDI adottate con D.M. n. 89 del 7 agosto 2020

Didattica digitale integrata e tutela della privacy: indicazioni generali: documento 3.09.2020 predisposto dal Gruppo di lavoro congiunto MIUR e Ufficio del Garante per la protezione dei dati personali

Chi sceglie gli strumenti da utilizzare?

Spetta alle Scuole - quali titolari del trattamento - la scelta e la regolamentazione, anche sulle base delle indicazioni fornite dalle autorità competenti, degli strumenti più utili per la realizzazione della didattica a distanza

Le scelte dovranno conformarsi **ai principi di privacy by design e by default**

Quali piattaforme prediligere?

Piattaforme o servizi che forniscono esclusivamente **attività di didattica a distanza** e **che offrano garanzie adeguate in materia di protezione dei dati personali**

Laddove si ritenga di ricorrere a piattaforme più complesse e "generaliste", che non eroghino servizi rivolti esclusivamente alla didattica, si dovranno **attivare, di default, i soli servizi strettamente necessari alla formazione, configurandoli in modo da MINIMIZZARE i dati personali da trattare, sia in fase di attivazione dei servizi, sia durante l'utilizzo degli stessi da parte di docenti e studenti.** **ATTENZIONE**: si dovrà evitare il ricorso a dati sulla geolocalizzazione, ovvero a sistemi di social login che, coinvolgendo soggetti terzi, comportano maggiori rischi e responsabilità

Cosa occorre fare quando si sceglie una piattaforma?

Qualora la piattaforma prescelta comporti il trattamento di dati personali di studenti, alunni o dei rispettivi genitori per conto della scuola, il rapporto con il fornitore dovrà essere regolato **con contratto** o altro atto giuridico (art. 28 del Regolamento). E' il caso, ad esempio, del registro elettronico, il cui fornitore tratta i dati per conto della scuola e, pertanto, assume il ruolo di responsabile del trattamento.

Per evitare di dover designare ulteriori responsabili del trattamento si potranno utilizzare servizi on line accessibili al pubblico e forniti direttamente agli utenti, con funzionalità di videoconferenza ad accesso riservato. Alcuni di questi servizi sono, peraltro, facilmente utilizzabili anche senza la necessaria creazione di un account da parte degli utenti.

In questi casi non occorrerà nominare alcun Responsabile del trattamento

Cose devono verificare le Istituzioni Scolastiche nella scelta del fornitore?

Le istituzioni scolastiche dovranno assicurarsi (anche in base a specifiche previsioni del contratto stipulato con il fornitore dei servizi designato responsabile del trattamento), che i **dati trattati per loro conto siano utilizzati solo per la didattica a distanza**. Saranno, in tal senso, utili specifiche istruzioni, tra l'altro, **sulla conservazione dei dati, sulla cancellazione** - al temine del progetto didattico - **di quelli non più necessari,** nonché **sulle procedure di gestione di eventuali violazioni di dati personali.**

Bisogna verificare che i dati non siano utilizzati per fini di marketing o di profilazione.

Cose devono verificare le istituzioni Scolastiche nella scelta del fornitore?

I trattamenti dei dati degli studenti svolti dalle piattaforme quali responsabili del trattamento deve limitarsi a quanto strettamente necessario per la fornitura dei servizi richiesti ai fini della didattica on line

Non devono essere effettuate operazioni ulteriori, preordinate al perseguimento di finalità proprie del fornitore.

E’ inammissibile il condizionamento, da parte dei gestori delle piattaforme, della fruizione dei servizi di didattica a distanza alla sottoscrizione di un contratto o alla prestazione– da parte dello studente o dei genitori – del consenso al trattamento dei dati connesso alla fornitura di ulteriori servizi on line, non necessari all’attività didattica.

SOGGETTI AUTORIZZATI AL TRATTAMENTO

Art. 29 G.D.P.R.: sono coloro che trattano i dati sulla base delle istruzioni ricevute dal Titolare del trattamento e che hanno accesso ai dati (es. collaboratori scolastici, ufficio personale, ufficio alunni, protocollo, docenti, etc.)

Art. 2-quaterdecies del Codice Privacy (Attribuzione di funzioni e compiti a soggetti designati) «Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità»

LA FORMAZIONE (art. 29 e 32 GDPR)

Art. 29 «*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali non può trattare tali dati se non è istruito in tal senso dal titolare*”.

Il principio è ribadito dall’art. 32, paragrafo 4, che prevede: “il *titolare del trattamento ed il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell’Unione o degli Stati membri*”.

LE ISTRUZIONI

I SOGGETTI AUTORIZZATI DOVRANNO ATTENERSI SCRUPOLOSAMENTE ALLE ISTRUZIONI RICEVUTE CHE SARANNO DIVERSE A SECONDA DELLE MANSIONI SVOLTE ALL'INTERNO DELL'ISTITUTO

RESPONSABILE DELLA PROTEZIONE DEI DATI «DPO»

REQUISITI

- Può essere una persona fisica o giuridica;
- Può operare alle dipendenze del titolare o del responsabile del trattamento oppure sulla base di un contratto di servizi (Dpo esterno) ;
- Adempie alle sue funzioni in piena autonomia e indipendenza;
- Possiede un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali
- **Per le Pubbliche Amministrazione la nomina è obbligatoria (art. 37 G.D.P.R.)**

RESPONSABILE DELLA PROTEZIONE DEI DATI «DPO»

COMPITI

- Sorvegliare l'osservanza del regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione, del contesto e delle finalità;
- Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e ne sorveglia lo svolgimento ai sensi dell'articolo 35;
- Informa e sensibilizza il titolare o il responsabile del trattamento, nonché i dipendenti, riguardo agli obblighi derivanti dal regolamento o da altre disposizioni in materia di protezione di dati;
- Cooperare con Il Garante e funge da punto di contatto su ogni questione connessa al trattamento;
- Supporta il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un registro delle attività di trattamento.

CHE COSA SI INTENDE PER TRATTAMENTO DEI DATI PERSONALI?

Il trattamento consiste in: 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

I PRINCIPI DEL TRATTAMENTO come devono essere trattati i dati personali? *ART. 6 G.D.P.R.*

- In modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime,
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
- esatti e, se necessario, aggiornati;
- conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (limitazione della conservazione);
- Il titolare deve adottare misure adeguate, tecniche e organizzative, che garantiscano l'integrità e la riservatezza del dato.

LICEITA' DEL TRATTAMENTO (INDIVIDUAZIONE BASE GIURICA) art. 6 GDPR

Il trattamento è lecito se ricorre almeno una delle seguenti condizioni:

a) consenso espresso;

b) **obbligo contrattuale**;

c) **obbligo di legge al quale è soggetto il Titolare del trattamento**;

d) interessi vitali dell'interessato o di un'altra persona fisica (esempio emergenza umanitaria, catastrofe naturale). N.B. si può invocare tale base giuridica solo se nessuna delle altre basi può trovare applicazione;

e) **interesse pubblico**;

f) legittimo interesse del titolare

art. 2 ter D.lgs. n. 196/2003 e s.m.i. (da ultimo D.L. 8.10.2021 n.139 conv con mod. in Legge 3.12.2021 n. 205)

Comma 1. La base giuridica del trattamento per le PA può essere costituita da **una norma di legge** o **di regolamento** o da **atti amministrativi generali**

Comma 1 bis Il trattamento dei dati personali da parte di un'amministrazione pubblica è anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti. **In modo da assicurare che tale esercizio non possa arrecare un pregiudizio effettivo e concreto alla tutela dei diritti e delle libertà degli interessati, le disposizioni di cui al presente comma sono esercitate nel rispetto dell' articolo 6 del Regolamento.**

Comma 2. a comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista ai sensi del comma 1 o se necessaria ai sensi del comma 1-bis.

Comma 3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1 o se necessarie ai sensi del comma 1-bis. In tale ultimo caso, ne viene data notizia al Garante almeno dieci giorni prima dell'inizio della comunicazione o diffusione.

IL CONSENSO: QUANDO NON SERVE?

Il consenso è solo una delle possibili basi giuridiche del trattamento.

Esso non serve, ad esempio nei casi di:

- Esecuzione di un contratto;
- Adempimento di un obbligo legale;
- Salvaguardia degli interessi vitali dell'interessato o altra persona fisica;
- Esecuzione compito interesse pubblico;
- perseguimento legittimo interesse.

Occorre il consenso per la didattica a distanza o ddi?

NO, **non occorre richiedere il consenso** per il trattamento dei dati personali di docenti, alunni, studenti, genitori, funzionali allo svolgimento dell'attività didattica a distanza.

La base giuridica del trattamento è individuata per l'attività didattica a distanza nell'art. 3 del d.l. 23 febbraio 2020, n. 6 e art. 2, lett. m) e n), del d.P.C.M. dell'8 marzo 2020

PERCHE' NON OCCORRE IL CONSENSO PER LA DAD O DDI?

Il consenso dei genitori, **che non costituisce una base giuridica idonea per il trattamento dei dati in ambito pubblico e nel contesto del rapporto di lavoro**, non è richiesto perché l'attività svolta, sia pure in ambiente virtuale, rientra tra le attività istituzionalmente assegnate all'istituzione scolastica, ovvero di didattica nell'ambito degli ordinamenti scolastici vigenti. Pertanto, le istituzioni scolastiche sono legittimate a trattare tutti i dati personali necessari al perseguimento delle finalità collegate allo svolgimento della DDI nel rispetto dei principi previsti dalla normativa di settore

PARTICOLARI CATEGORIE DI DATI: BASI GIURIDICHE (ART. 9 G.D.P.R)

ANCHE PER IL TRATTAMENTO DELLE CATEGORIE PARTICOLARI DI DATI PERSONALI E' NECESSARIO INDIVIDUARE LE BASI GIURIDICHE:

a) consenso esplicito;

b) obblighi del Titolare in materia di diritto del lavoro e della sicurezza sociale e protezione sociale (obblighi previsti dalla normativa italiana, dell'UE o dal contratto collettivo) e/o per consentire l'esercizio dei diritti dell'interessato;

……g) trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri;

Art. 2-sexies D.lgs. n. 196/2003 (Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante)

1. I trattamenti delle categorie particolari di dati personali necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

2. Fermo quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie:

..... bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario;

INFORMATIVE

- Le informative devono avere una forma concisa, trasparente, intellegibile e facilmente accessibile.

- Sono fornite per iscritto o con altri mezzi, ad esempio elettronici.

- Se richiesto dall'interessato, possono essere fornite anche oralmente purché in questo caso sia comprovata con altri mezzi l'identità dell'interessato.
- Potranno essere fornite in combinazione con icone standardizzate che dovranno essere definite dalla Commissione europea.

Liceità, correttezza e trasparenza del trattamento

Le istituzioni scolastiche devono assicurare la trasparenza del trattamento **informando gli interessati (alunni, studenti, genitori e docenti), con un linguaggio comprensibile anche ai minori**, in ordine, in particolare, alle caratteristiche essenziali del trattamento che deve limitarsi all'esecuzione dell'attività didattica a distanza

TEMPI DELL'INFORMATIVA: QUANDO DEVE ESSERE FORNITA?

- Se i dati sono raccolti presso l'interessato, nel momento in cui sono ottenuti;

- Se non sono raccolti direttamente presso l´interessato, entro un termine ragionevole che non può superare un mese dalla raccolta, oppure dalla comunicazione dei dati a terzi o all'interessato.

CONTENUTI DELL'INFORMATIVA (art. 13) – DATI RACCOLTI PRESSO L'INTERESSATO

- l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- i dati di contatto del DPO, ove applicabile;
- le finalità del trattamento nonché la base giuridica;
- nel caso in cui la base giuridica del trattamento sia il legittimo interesse del titolare o di terzi, specificare quale è il legittimo interesse ;

  gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

CONTENUTI DELL'INFORMATIVA (art. 13) – DATI RACCOLTI PRESSO L'INTERESSATO

- In caso di trasferimento dei dati personali a un paese terzo o a un'organizzazione internazionale occorre specificarlo, indicando altresì attraverso quali modalità avviene il trasferimento (l'esistenza o l'assenza di una decisione di adeguatezza della Commissione; garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti - tra cui le norme vincolanti d´impresa - BCR, e clausole contrattuali modello-)

In aggiunta alle informazioni suindicate, nel momento in cui dati sono ottenuti, il titolare fornisce le seguenti ulteriori informazioni:

il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

CONTENUTI DELL'INFORMATIVA (art. 13) – DATI RACCOLTI PRESSO L'INTERESSATO

- l'esistenza dei diritti dell'interessato (accesso, rettifica, cancellazione, limitazione del trattamento, opposizione al trattamento, diritto alla portabilità dei dati;
- qualora il trattamento sia basato sul consenso, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo all'Autorità Garante;

CONTENUTI DELL'INFORMATIVA (art. 13) – DATI RACCOLTI PRESSO L'INTERESSATO

- se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

- l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

NUOVA INFORMATIVA IN CASO DI TRATTAMENTO PER FINALITA' DIVERSA

Ricordarsi sempre che nel caso in cui il titolare del trattamento intenda trattare **ulteriormente i dati personali per una finalità diversa** da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento deve fornire all'interessato informazioni in merito a tale diversa finalità.

CONTENUTI DELL'INFORMATIVA (art. 14) – DATI NON RACCOLTI PRESSO L'INTERESSATO

In aggiunta alle informazioni indicate nell'art. 13 occorre specificare:

- le categorie dei dati trattati;
- la fonte da cui hanno origine i dati personali trattati e se provengono da fonti accessibili al pubblico.

Tempi dell'informativa:

Entro un termine ragionevole che non può superare un mese dalla raccolta, oppure dalla comunicazione dei dati a terzi o all'interessato.

Diritti degli Interessati (artt. 15 -22)

Diritto di accesso (art. 15)
Diritto di rettifica (art.16)
Diritto di cancellazione «c.d. diritto all'oblio» (art. 17)
Diritto di limitazione di trattamento (art. 18)
Diritto alla portabilità dei dati (art. 20). Non si applica al trattamento 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 (art. 20, comma 3 GDPR)
Diritto di opposizione (art. 21)
Revoca del consenso (solo se il trattamento dei sati basava sul consenso)

Processo decisionale automatizzato, compresa la profilazione (art.22)

RECLAMO

Art 77 del Regolamento UE 679/1996 e artt. da 140-bis a 143 del Codice privacy.

- La presentazione del reclamo è gratuita
- Sul sito del Garante è rinvenibile un modello di reclamo

(https://www.garanteprivacy.it/home/modulistica-e-servizi-online/reclamo)

IL NUOVO APPROCCIO ALLA TUTELA DEI DATI PERSONALI

ANALISI DEI RISCHI

ART. 32 REG.UE 2016/679

PRIVACY BY DESIGN

ART, 25 REG.UE 2016/679

PRIVACY BY DEFAULT

ART, 25 REG.UE 2016/679

SICUREZZA DEL TRATTAMENTO (art. 32)

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono **in atto misure tecniche e organizzative** adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

PRIVACY BY DESIGN – PRIVACY BY DEFAULT (art. 25)

Il titolare del trattamento, sia la momento di determinare i mezzi del trattamento, sia all'atto del trattamento stesso deve mettere in atto misure tecniche ed organizzative adeguate (quali la pseudonimizzazione, la minimizzazione dei dati).

Ciò implica una progettazione sin dall'inizio della propria policy privacy e quindi del trattamento dei dati.

MISURE DI SICUREZZA

- Procedure di identificazione e autenticazione informatica degli utenti;
- Assegnazione agli utenti di credenziali o dispositivi di autenticazione;
- Definizione di differenti profili di autorizzazione per i soggetti autorizzati (accesso selettivo ai dati)
- Definizione di password policy adeguate (regole di composizione, scadenza periodica, ecc.)
- cifratura dei dati (es. sito web e allegati Mail contenenti dati particolari)
- Utilizzo firewall
- Utilizzo sistemi anti malware e antivirus costantemente aggiornati
- Aggiornamento periodico software di base;
- Backup e disaster recovery per garantire la disponibilità dei dati
- vulnerability assessment penetration test/monitoraggio delle attività di rete
- pseudonimizzazione anonimizzazione dei dati (es. Password)
- intrusion detection (per verificare accessi non autorizzati)
- conservazione digitale,
- Protezione documentazione cartacea (riporre i documenti in appositi fascicoli e sistemarli in armadi chiusi a chiave)

RANSOMWARE: CHE COS'E'?

Ransomware: è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un RISCATTO (ransomin inglese) da pagare per rimuovere la limitazione.

- Ci sono due tipi principali di ransomware:
- **i cryptor** (che criptano i file contenuti nel dispositivo rendendoli inaccessibili);
- **i blocker** (che bloccano l'accesso al dispositivo infettato)

I PUNTI DEBOLI SFRUTTATI DAL RANSOMWARE

- **Vulnerabilità dei software dei sistemi:** si verifica quando le misure di sicurezza non sono adeguate o sono compromesse e di conseguenza più facilmente attaccabili.
- **Formazione del personale:** scarsa formazione degli utenti in relazione all'uso degli strumenti tecnologici.
- **Comportamenti non appropriati degli utenti**: ad esempio apertura di allegati sospetti per disattenzione e/o curiosità (errore umano)

COME SI DIFFONDE?

In particolare attraverso **comunicazioni ricevute via e-mail che:**

• sembrano apparentemente provenire da soggetti conosciuti e affidabili (ad esempio pubbliche amministrazioni, corrieri espressi, operatori telefonici, ecc.);

• contengono allegati da aprire (spesso "con urgenza"), oppure link da cliccare e banner (per verificare informazioni o ricevere importanti avvisi), collegati a software malevoli.

Fonte
https://www.garanteprivacy.it/temi/cybersecurity/ransomware

COME DIFENDERSI?

LA PRIMA REGOLA E' LA PRUDENZA

- Leggere sempre con attenzione i messaggi visualizzati nel PC e in particolare durante la navigazione, prima di cliccare su SI.
- Diffidare delle email di cui non si conosce l'indirizzo del mittente; in questo caso non aprire mai gli allegati o i programmi ivi contenuti, né selezionare i link indicati;
- Aprire unicamente i file o i programmi provenienti da fonti affidabili e solo previa verifica con un programma antivirus aggiornato;
- non aprire mai allegati con estensioni "strane" (ad esempio, allegati con estensione ".exe" sono a rischio, perché potrebbero installare applicazioni di qualche tipo nel dispositivo);

COME DIFENDERSI?

- **Controllare l'indirizzo del mittente**: si può passare la freccia del mouse su eventuali link o banner pubblicitari ricevuti via e-mail o presenti su siti web senza aprirli (così, in basso nella finestra del browser, si può vedere l'anteprima del link da aprire e verificare se corrisponde al link che si vede scritto nel messaggio: in caso non corrispondano, c'è ovviamente un rischio).
- **Diffidare di email** apparentemente provenienti da Pubbliche Amministrazioni: le PA non utilizzano la posta elettronica per certi tipi di comunicazioni; ad esempio, è improbabile che una PA vi contatti via email per chiedere soldi o informazioni riservate.
- **Verificare la validità di un indirizzo o di un link ricevuto via e mail:** a volte gli indirizzi cambiano di poco (anche per una sola vocale o consonante diversa)
- **Non rispondere alle spam,**
- **Prestare attenzione alla grammatica e all'ortografia**

QUALI SONO LE MISURE DI SICUREZZA DA ATTUARE PER RIDURRE IL RISCHIO?

- È fondamentale ai fini della sicurezza scaricare gli aggiornamenti del software (software update, chiamate anche “patch”), perché consentono di colmare le falle di sicurezza che vengono scoperte quasi quotidianamente, le cosiddette vulnerabilità del Sistema;
- È consigliabile programmare gli aggiornamenti in automatico.
- utilizzare dei sistemi di BACKUP che salvino (anche in maniera automatica) una copia dei dati.
- Con un corretto backup, in caso di necessità, si potranno ripristinare i dati contenuti nel dispositivo, quantomeno fino all'ultimo salvataggio

COSA NON FARE IN GENERALE

- NON aprire chiavette USB sulla propria postazione di lavoro
- NON scaricare programmi da internet se non con l'assistenza di una persona esperta e solo dopo aver verificato l'attivazione dell'antivirus e il suo aggiornamento; accertarsi di essere sul sito del produttore del software.
- NON scaricare programmi sconosciuti
- NON scaricare musica, film, file con estensioni: zip, exe, bat o non conosciute.
- NON navigare sui social e/o su siti non conosciuti

COSE DA NON FARE

Credenziali di accesso

- scrivere le password sui post-it;
- salvare le password nel browser
- inviare le password per e.mail;

Sistemi operativi

- usare sistemi operativi obsoleti (es. Winsows XP)

Consigli del Garante

Consigli flash

X TUTELARE la tua privacy con buone password

1 COME E' FATTA UNA BUONA PASSWORD

Una **buona password**

- deve essere abbastanza **lunga** (almeno 8 caratteri);
- deve contenere **caratteri di almeno 3 diverse tipologie**, da scegliere tra le 4 seguenti: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (punti, trattino, *underscore*, ecc.);
- **non** dovrebbe **contenere riferimenti** personali facili da indovinare (nome, cognome, data di nascita, ecc.);
- **andrebbe periodicamente cambiata**, almeno per i profili più importanti o quelli che usi più spesso (e-mail, *e-banking*, *social network,* ecc.).

2 UTILIZZA PASSWORD DIVERSE PER ACCOUNT DIVERSI (e-mail, *social network*, ecc.)

In caso di «furto» di una password eviterai così il rischio che anche gli altri profili che ti appartengono possano essere violati.

3 CONSERVA CON CURA LE PASSWORD

- **Non conservare mai** le password su biglietti che poi tieni nel portafoglio o indosso, oppure in *file* non protetti su pc, *smartphone* o *tablet.*
- **Evita di condividere** le password via e-mail, sms, *social network*, *instant messaging*, ecc.. Anche se le comunichi a persone conosciute, le credenziali potrebbero essere diffuse involontariamente a terzi o «rubate» da pirati informatici.
- Se usi pc, *smartphone* e altri *device* che non ti appartengono, **evita** che possano **conservare in memoria le password da te utilizzate.**

MISURE ORGANIZZATIVE

- Nomina per iscritto dei soggetti autorizzati al trattamento dei dati (nomina del personale);
- istruzioni/regolamento sul trattamento dei dati personali a tutto il personale
- nomina per iscritto dei responsabili esterni
- accesso controllato ai dati mediante assegnazione di credenziali;
- procedura modifica credenziali
- armadi chiusi
- documentazione/Policy aggiornate
- formazione di tutto il personale
- gestione delle postazioni da lavoro
- Adozione registro delle attività di trattamento

COSA E' IL REGISTRO DEI TRATTAMENTI (art. 30 G.D.P.R.)

E' un documento contenente le principali informazioni relative alle operazioni di trattamento svolte dal titolare e, se nominato, dal responsabile del trattamento

Costituisce uno dei **principali elementi di accountability** del titolare, in quanto strumento **idoneo a fornire un quadro aggiornato dei trattamenti** in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività.

Il registro deve avere **forma scritta, anche elettronica**, e deve essere esibito su richiesta al Garante.

QUALI SONO LE MODALITÀ DI CONSERVAZIONE E DI AGGIORNAMENTO DEL REGISTRO?

Comunicato stampa dell'8 ottobre 2018 del Garante della privacy

- deve essere mantenuto costantemente aggiornato poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere.
- Qualsiasi cambiamento, in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.
- Il Registro può essere compilato sia in formato cartaceo che elettronico ma deve in ogni caso recare, in maniera verificabile, la data della sua prima istituzione (o la data della prima creazione di ogni singola scheda per tipologia di trattamento) unitamente a quella dell'ultimo aggiornamento. In quest'ultimo caso il Registro dovrà recare una annotazione del tipo:

"- scheda creata in data XY"

"- ultimo aggiornamento avvenuto in data XY"

QUAL E' IL CONTENUTO DEL REGISTRO DEI TRATTAMENTI? (art. 30 GDPR)

Il registro contiene le seguenti informazioni:

a) nome e i dati di contatto del titolare del trattamento. Ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e dpo;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

QUAL E' IL CONTENUTO DEL REGISTRO DEI TRATTAMENTI? (art. 30 GDPR)

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

QUAL E' IL CONTENUTO DEL REGISTRO DEI TRATTAMENTI? (art. 30 GDPR)

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

VIOLAZIONI DEI DATI PERSONALI "DATA BREACH"

L'art. 4, punto 12 del GDPR definisce **la violazione dei dati personali** come:

«*la violazione* ***di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati»***

In cosa consiste una violazione dei dati personali?

Violazione della riservatezza: in caso di divulgazione dei dati personali o acceso agli stessi non autorizzati o accidentali

esempio : invio email a destinatario errato –furto documenti –furtosmartphone; invio una mail inserendo i destinatari nella casella «A:» anziché in CCN se gli indirizzi dei destinatari non dovevano essere conosciuti dagli altri

Violazione dell'integrità: modifica non autorizzata dei dati

Violazione della disponibilità: in caso di perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Esempio: attacco ransonware | cancellazione accidentale contratto

COSA FARE IN CASO DI "DATA BREACH"? (art. 33 GDPR)

Segnalare immediatamente al Dirigente la violazione descrivendo cosa è accaduto.

Il titolare del trattamento dovrà notificare:

- la **violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è venuto a conoscenza della violazione**, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo;

- Senza ingiustificato ritardo **agli interessati, quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.**

VALUTAZIONE RISCHIO

In caso di:

- Rischio assente: la notifica al Garante non è obbligatoria. Tale ipotesi si verifica ad esempio quando i dati personali, oggetto della violazione, sono dati pubblici.

- Rischio presente: è necessaria la notifica al Garante;

- Rischio elevato: è necessaria la notifica al Garante e la comunicazione anche agli interessati

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DELLE PERSONE FISICHE

Il rischio va riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche:

- discriminazioni
- furto o usurpazione d'identità
- perdite finanziarie
- pregiudizio alla reputazione
- perdita di riservatezza dei dati personali protetti da segreto professionale
- decifratura non autorizzata della pseudonimizzazione
- danno economico o sociale significativo
- privazione o limitazione di diritti o libertà
- impedito controllo sui dati personali all'interessato
- danni fisici, materiali o immateriali alle persone fisiche.

RISCHIO ELEVATO

I rischi per i diritti e le libertà degli interessati possono essere considerati “elevati” quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un’elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

CHE INFORMAZIONI DEVE CONTENERE LA NOTIFICA AL GARANTE?

- La notifica deve contenere almeno le informazioni sinteticamente riportate in questa pagina (art. 33, par. 3 del Regolamento (UE) 2016/679):
- una descrizione della natura della violazione dei dati personali, che comprenda, se possibile:
  - le categorie e il numero approssimativo di persone interessate;
  - le categorie e il volume approssimativo di dati personali interessati;
  - il nome e i riferimenti di contatto del responsabile della protezione dei dati (se designato dal titolare) o comunque di un referente competente a fornire informazioni;
  - una descrizione delle possibili conseguenze della violazione dei dati personali

CHE INFORMAZIONI DEVE CONTENERE LA NOTIFICA AL GARANTE?

Una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali, comprese, se del caso, le misure adottate per mitigare eventuali effetti negativi;

- **SOLO in caso di notifica effettuata oltre il termine prescritto di 72 ore**, una descrizione dei motivi del ritardo.

A partire dal 1° luglio 2021, la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/

Per semplificare gli adempimenti previsti per i titolari del trattamento, il Garante ha ideato e messo disposizione un apposito strumento di autovalutazione (self assessment) che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

Per approfondimenti

Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679 Adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017 Versione emendata e adottata il 6 febbraio 2018

https://www.garanteprivacy.it/regolamentoue/databreach

CHE INFORMAZIONI DEVE CONTENERE LA NOTIFICA AGLI INTERESSATI?

La comunicazione deve contenere:

a) nome e i dati di contatto del Titolare o di altra persona presso cui ottenere più informazioni;

b) descrizione delle probabili conseguenze della violazione dei dati personali;

c) descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi

QUANDO NON E' RICHIESTA LA NOTIFICA AGLI INTERESSATI ?

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

REGISTRO DELLE VIOLAZIONI DEI DATI PERSONALI (ART. 33, COMMA 5 GDPR)

Il Titolare deve documentare in un registro le violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio

VALUTAZIONE D'IMPATTO (DPIA) (art. 35)

Quando un tipo di trattamento prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti.

Essa è richiesta in particolare nei seguenti casi :

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

E’ necessario effettuare una valutazione di impatto ai sensi dell’art. 35 del Regolamento UE n. 2016/679 per la dad o did?

NO. La valutazione di impatto non è necessaria se il trattamento effettuato dalle istituzioni scolastiche - ancorché relativo a soggetti in condizioni peculiari quali minorenni e lavoratori - non presenta ulteriori caratteristiche suscettibili di aggravarne i rischi per i diritti e le libertà degli interessati.

Ad esempio, non è richiesta la valutazione di impatto per il trattamento effettuato da una singola scuola nell’ambito dell’utilizzo di un servizio on line di videoconferenza o di una piattaforma che non consente il monitoraggio sistematico degli utenti o comunque non ricorre a nuove soluzioni tecnologiche particolarmente invasive (quali, tra le altre, quelle che comportano nuove forme di utilizzo dei dati di geolocalizzazione o biometrici).

RESPONSABILITA' CIVILE RISARCIMENTO DANNI

L'art. 82 del G.D.P.R. sancisce che «*Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento*»

Il titolare e il responsabile del trattamento sono responsabili in solido nei confronti dell'interessato, salvo il diritto di regresso nei rapporti interni.

SANZIONI (artt. 83-84)

Il G.D.P.R. prevede sanzioni amministrative pecuniarie: effettive, proporzionate e dissuasive.

Le sanzioni amministrative pecuniarie sono inflitte in aggiunta o in luogo alle sanzioni di cui all'art. 58, par. 2, lett. da a) a h) e j) del Regolamento (avvertimenti, ammonimenti, ingiunzioni, limitazioni ai trattamenti, ordine di cancellazione, rettifica o limitazioni del trattamento, revoca della certificazione o ingiunzione all'Organismo certificatore di ritirare o non emettere la certificazione, ordine di sospensione dei flussi di dati verso un destinatario)

SANZIONI (art. 84)

fino a 10.000.000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nel caso di violazione di determinati obblighi posti dal Regolamento (ad. consenso minori ove necessario, mancata adozione di misure tecniche e organizzative; mancata designazione responsabile del trattamento, mancata tenuta registro dei trattamenti, mancata nomina DPO)

SANZIONI (art. 84)

fino a 20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nel caso di violazione degli obblighi più stringenti posti dal Regolamento (quali, ad esempio la violazione dei principi di base del trattamento, condizioni consenso, diritti degli interessati, trasferimenti dati, inottemperanza ad un ordine, ad una limitazione di trattamento o ad un ordine di sospensione di flussi di dati dell'Autorità di controllo o di un negato accesso).

OLTRE ALLE SANZIONI AMMINISTRATIVE SONO PREVISTE ANCHE ….FATTISPECIE PENALI!!

- Il decreto di adeguamento al GDPR, in vigore dal 19 settembre, ha confermato le fattispecie incriminatrici previste dal Codice della Privacy e ne ha introdotte di nuove.
  - Art. 167 Trattamento illecito di dati;
  - Art. 167-bis Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala;
  - Art. 167-ter Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala
  - Art. 168 Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante
  - Art. 170 Inosservanza di provvedimenti del Garante
  - Art. 171 Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori

Buona giornata a tutti!

Grazie per l’attenzione