ISTITUTO DI ISTRUZIONE SECONDARIA SUPERIORE
"Cataldo Agostinelli"
Comprensivo di: Liceo Classico/Scientifico – I.T.E.S. – I.P.S.S.S. – I.P.S.I.A – I.P.S.E.O.A
Via Ovidio – 72013 Ceglie Messapica (BR)
C.F. 90015850747
Email: bris006001@istruzione.it – bris006001@istruzione.it
www.istitutoagostinelli.edu.it
☎ 0831377890 - 🖷 0831379023

Circolare n. 231

Ai Docenti
Al Personale ATA
Ai Genitori
A tutti gli Stakeholders

"DATA BREACH"

PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI

AI SENSI DEL REGOLAMENTO EUROPEO 679/2016

Sommario

PREMESSA

L'art. 33 del Regolamento generale sulla protezione dei dati 679/2016 G.D.P.R. ha introdotto l'obbligo in capo al Titolare del trattamento di notifica all'Autorità di controllo – Autorità Garante per la protezione dei dati personali (d'ora in poi per brevità Autorità Garante) - delle violazioni dei dati personali (c.d. data breach).

Una violazione dei dati personali (c.d. data breach) se non affrontata in modo adeguato e tempestivo può provocare danni fisici, materiali o immateriali alle persone fisiche: quali la perdita del controllo dei dati personali che li riguardano o la limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

Per prevenire o mitigare tali pregiudizi, il Titolare del trattamento deve notificare la violazione, senza ingiustificato ritardo e, ove possibile entro 72 ore da quando ne è venuto a conoscenza all' Autorità Garante.

L'obbligo di comunicazione viene meno solo qualora il Titolare ritenga che la violazione dei dati personali presenti un rischio improbabile in termini di pregiudizio per i diritti e le libertà delle persone fisiche.

Nel caso di rischio elevato, oltre alla notifica all'Autorità Garante, il Titolare è tenuto a dare comunicazione della violazione anche all'interessato ai sensi dell'art. 34 del G.D.P.R.

Qualora la notifica non sia effettuata entro 72 ore, essa dovrà essere corredata dei motivi del ritardo.

A fronte del mancato rispetto dell'obbligo di notifica l'Autorità Garante può:

- applicare misure correttive previste dall'art. 58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati);
- oppure in aggiunta o in luogo delle misure correttive di cui all'art. 58 GDPR irrogare sanzioni amministrative pecuniarie ai sensi dell'art. 83 GDPR (fino a 10.000,000 Euro e per le imprese fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore).

SCOPO DELLA PROCEDURA

L'Istituto comprensivo n.13 di Bologna, nella sua qualità Titolare del trattamento dei dati personali, ha predisposto la presente procedura interna per una corretta e rapida gestione delle violazioni dei dati personali al fine di:

- assicurare il rispetto delle prescrizioni del G.D.P.R.;
- garantire la migliore tutela dei diritti e libertà degli interessati (alunni, docenti, collaboratori, assistenti amministrativi, famiglie);
- salvaguardare il proprio patrimonio informativo istituzionale.

Di seguito sono individuate le modalità operative di gestione delle violazioni dei dati personali (individuazione della violazione, ruoli e compiti all'interno dell'Istituto nella gestione del data breach, accertamenti da effettuare, modalità di notifica etc.).

NORMATIVA E DOCUMENTI DI RIFERIMENTO

La presente procedura è stata redatta sulla base della seguente normativa e documentazione:

- *Regolamento UE 679/2016, considerando n. 85, 86, 87, 88 artt. 33, 34;*
- *Decreto legislativo 196/2003, modificato dal decreto legislativo del 10 agosto 2018, n. 101*
- *Linee Guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento UE 2016/679 elaborate dal Gruppo di lavoro articolo 29 per la protezione dei dati personali, adottate il 3 ottobre 2017- versione emendata e adottata in data 6 febbraio 2018.*

In particolare si riportano integralmente gli artt. 33 e 34 del G.D.P.R.

Art. 33 del GDPR: *"Notifica di una violazione dei dati personali all'autorità di controllo"*

1. In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, 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.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
   a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
   b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
   c) descrivere le probabili conseguenze della violazione dei dati personali;
   d) descrivere le 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;
   e) qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo;

f) il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34 del GDPR: "*Comunicazione di una violazione dei dati personali all'interessato*"

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 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 di cui al paragrafo 1;
   c) detta 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.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

DEFINIZIONI GENERALI

- «*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 (art. 4, punto 1 GDPR);
- "*categorie particolari di dati personali*": dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 G.D.P.R.);

- "Dati relativi a condanne penali e reati": dati personali relativi a condanne penali e a reati o connessi a misure di sicurezza (art. 10 G.D.P.R.);
- *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 (art. 4, punto 2 GDPR);
- *«titolare del trattamento»*: 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, punto 7 GDPR)
- *«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 (art. 4, punto 8 GDPR);
- "*autorizzato al trattamento*": persona fisica, espressamente designata che opera sotto l'autorità del Titolare del trattamento (art. 29 GDPR e art. 2- quaterdecies D.lgs. n. 196/2003, modificato dal D.Lgs. 10 agosto 2018, n. 101,
- «*violazione dei dati personali*»: 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 (art. 4, punto 12 GDPR);
- «*autorità di controllo»:* l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 (art. 4, punto 21 GDPR- art. 2 bis D.lgs. n. 196/2003, modificato dal D.Lgs. 10 agosto 2018, n. 101);

Strumenti informatici:

- "*Dispositivi Fissi*": si intendono gli strumenti informatici non facilmente removibili dal perimetro aziendale quali personal computer, server locali, stampanti affidati alle persone autorizzate per uso professionale;
- "*Dispositivi Mobili*": in generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili, quali chiavette USB, SD cards, hard disk esterni, tablet e smartphone

AMBITO DI APPLICAZIONE DELLA PROCEDURA

La presente procedura è rivolta:

- a dirigente scolastico e suoi collaboratori, docenti, personale ATA (dsga, assistenti amministrativi e collaboratori scolastici), alunni, che durante lo svolgimento delle attività scolastiche possono venire a conoscenza di una violazione dei dati personali, nonché a l le famiglie, qualora anch'esse vengano a conoscenza di una violazione dei dati personali.

GESTIONE DATA BREACH

FASE: SEGNALAZIONE

Ciascun soggetto suindicato che venga a conoscenza di una violazione dei dati personali è tenuto:

ad avvisare immediatamente il Dirigente Scolastico, anche per le vie brevi telefonicamente o recandosi presso il Suo Ufficio;

- successivamente a compilare, entro e non oltre 2 ora dalla conoscenza della violazione, il modello 1 messo a diposizione dal Titolare, consegnandolo al Dirigente Scolastico di persona oppure inviandolo tramite e.mail all'indirizzo:

boic85700e@istruzione.it

FASE: GESTIONE DA PARTE DEL DIRIGENTE SCOLASTICO E DEI SUOI COLLABORATORI CON L'AUSILIO DEL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

Il Dirigente Scolastico, venuto a conoscenza della violazione:

- convoca immediatamente i Suoi collaboratori ed informa il Responsabile delle Protezione dei dati personali;
- indi avvia gli accertamenti necessari per comprendere il contesto del trattamento, la natura dei dati personali coinvolti e qualunque informazione utile per una completa valutazione dell'episodio;
- in base al tipo di violazione (ad. esempio su supporto analogico o su supporti informatici), si avvale di professionisti esterni: quali consulenti informatici e società specializzate al fine di mitigare e attenuare i rischi derivanti dalla possibile violazione;
- informa il Responsabile del trattamento dei dati allorquando la violazione coinvolga dati trattati da un Responsabile del trattamento, ciò al fine di far avviare tutte le verifiche necessarie;
- documenta l'esito preliminare dell'indagine utilizzando il modello 2

II FASE: VALUTAZIONI DEL TITOLARE E ATTIVITA' CONSEGUENTI

Il Titolare, valutati gli elementi a disposizione, insieme con il DPO che fornisce un suo parere:

- chiude l'accertamento senza annotazione nel registro delle notificazioni qualora sia palese che la violazione non riguarda dati personali;
- in caso di accertata violazione dei dati personali, potrà:

a) annoterà la violazione nel Registro senza effettuare alcuna notificazione qualora sia improbabile che essa presenti un rischio per i diritti e le libertà degli interessati;

b) in caso di rischio ai diritti e alle libertà degli interessati, annoterà la violazione nel Registro ed effettuerà la notificazione all'Autorità Garante utilizzando il modello 3. Qualora il rischio

ai diritti e alle libertà degli interessati sia elevato oltre all'annotazione nel Registro, effettuerà anche la comunicazione agli interessati sussistendo i presupposti di cui dall'art. 34 del GDPR.

VIOLAZIONE DEI DATI PERSONALI

Affinché tutti i soggetti coinvolti nella procedura di data breach possano svolgere i compiti di rispettiva competenza è necessario chiarire che cosa si intende per violazione dei dati personali.

Ai sensi dell'art. 4, punto 12 del GDPR per violazione dei dati personali si intende: 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.

La violazione di dati personali è quindi un particolare tipo di incidente di sicurezza.

È importante chiarire che non tutti gli incidenti di sicurezza sono necessariamente violazioni di dati personali.

Le violazioni di dati personali si distinguono in:

1. "*violazione di riservatezza*", in caso di divulgazione dei dati personali o acceso agli stessi non autorizzati o accidentali;
2. "*violazione di integrità*", in caso di modifica non autorizzata o occidentaledei dati personali;
3. "*violazione di disponibilità*", in caso di perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Una violazione potrebbe comprendere una o più tipologie.

Di seguito si riporta una tabella in cui sono indicate in via meramente esemplificativa possibili violazioni di dati personali:

TIPO DI VIOLAZIONE DATA BREACH	DEFINIZIONE	ESEMPI
1. VIOLAZIONE DELLA RISERVATEZZA	In caso di divulgazione o accesso non autorizzato o accidentale di dati personali	• perdita di una chiave USB con dati personali non crittografati di cui terzi potrebbero essere venuti in possesso • segnalazione, anche da parte di un terzo, di un episodio nel quale un soggetto non autorizzato accidentalmente ha ricevuto dati personali

2. VIOLAZIONE DELL'INTEGRITÀ	• in caso di modifica non autorizzata o occidentale dei dati personali;	• il Titolare rileva che c'è stata una possibile intrusione nella sua rete che potrebbe aver compromesso l'integrità dei dati • modifica di dati personali o categoria di dati personali contenuti in documenti.
a) Perdita di disponibilità dei dati	in caso di perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.	- furto o smarrimento di un dispositivo (Hard Disk) contenente dati personali. - furto computer dall'ufficio - copia unica di dati personali crittografata da ransomware, o comunque crittografata utilizzando una chiave di cifratura non più disponibile - cancellazione volontaria o accidentale di dati di cui se ne deve assicurare la conservazione - impossibilità di ripristinare l'accesso ai dati, ad esempio da un backup. - interruzione significativa del normale servizio anche in caso di interruzione di corrente o attacco da blocco di servizio "denial of service", tale da rendere i dati personali non disponibili. - annullamento di attività che presuppongono un trattamento di dati personali a causa di un disservizio tecnico

		- perdita, anche solo temporanea, di disponibilità (ad esempio nel caso in cui i dati possono essere successivamente ripristinati dal backup) causata da un'infezione dei sistemi informatici, ransomware. - pirata informatico contatta la scuola dopo aver hackerato il sistema informatico per chiedere un riscatto. - distruzione o perdita di una copia o un backup di dati personali detenuti dai soggetti autorizzati a trattarli, ma i dati sono ancora detenuti dalla scuola - perdita di documenti contenenti categorie particolari di dati personali

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

Una volta che il Titolare ha appurato che è avvenuta una violazione dei dati personali sarà necessario capire se da essa possono derivare rischi ai diritti e alle libertà delle persone onde verificare l'obbligatorietà della notifica al Garante ed eventualmente ai soggetti interessati.

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

1. discriminazioni
2. furto o usurpazione d'identità
3. perdite finanziarie
4. pregiudizio alla reputazione
5. perdita di riservatezza dei dati personali protetti da segreto professionale
6. decifratura non autorizzata della pseudonimizzazione
7. danno economico o sociale significativo
8. privazione o limitazione di diritti o libertà
9. impedito controllo sui dati personali all'interessato 10.danni fisici, materiali o immateriali alle persone fisiche.

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. 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 (ad. esempio dati vaccinali, relativi alla salute degli alunni);
  - 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. alunni minorenni: ad. esempio in caso di dati personali relativi all'indirizzo di residenza).

NOTIFICA AL GARANTE: TEMPI, CONTENUTO

Il Titolare, in caso di violazione dei dati personali provvede senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza (cioè quando abbia un ragionevole grado di certezza del verificarsi della violazione) a notificare la violazione all'Autorità Garante.

Se la comunicazione è effettuata successivamente al termine delle 72 ore, questa deve essere corredata delle ragioni del ritardo.

È comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione, anche a seguito di ulteriori indagini e attività di follow-up (c.d. notificazione in fasi).

La notifica va trasmessa al Garante per la protezione dei dati personali, inviandola all'indirizzo: protocollo@pec.gpdp.it e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.

L'oggetto del messaggio deve contenere obbligatoriamente la dicitura "notifica violazione dati personali" e opzionalmente la denominazione del Titolare del trattamento.

La notifica dovrà contenere i seguenti elementi:

a) descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) nome e i dati di contatto del Titolare o di altra persona presso cui ottenere più informazioni;
c) descrizione delle probabili conseguenze della violazione dei dati personali;
d) 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

Il Dirigente Scolastico coadiuvato dal DPO e dalla società informatica e/o consulente informatico eventualmente incaricato curerà la compilazione della comunicazione utilizzando il modello 3.

COMUNICAZIONE AGLI INTERESSATI

Nel caso in cui dal data breach possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste devono essere informate senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

Il Dirigente Scolastico coadiuvato dal DPO predispone una comunicazione con un linguaggio semplice e chiaro da inviare all'interessato/agli interessati e da lui sottoscritta.

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.

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.

COMPITI DEI RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART. 28 GDPR

Ogni Responsabile del trattamento, qualora venga a conoscenza di un potenziale data breach che riguardi dati personali che tratta per conto del Titolare, informa il Titolare tempestivamente di essere venuto a conoscenza di una violazione, nei termini e con le modalità convenute nei contratti di nomina come Responsabile del trattamento ex art. 28 G.D.P.R.

Il Responsabile dovrà indicare:

- una descrizione della natura della violazione della sicurezza, comprendente il volume e la tipologia di dati personali, le categorie e il numero approssimativo di persone interessate;
- le conseguenze probabili della violazione della sicurezza;
- una descrizione delle misure adottate o proposte per far fronte alla violazione della sicurezza, ivi comprese, se del caso, le misure atte a mitigarne i possibili effetti negativi.

Il Responsabile del trattamento:

- fornisce assistenza al Titolare per far fronte alla violazione e alle sue conseguenze soprattutto in capo agli interessati coinvolti;
- intraprende tutte le azioni correttive necessarie e appropriate, a spese proprie, per prevenire il ripetersi di tale violazione della sicurezza dei dati personali.

Il Titolare del trattamento, ricevuta la comunicazione della violazione di sicurezza da parte del Responsabile del trattamento, effettua gli accertamenti ritenuti necessari al fine di valutare la sussistenza degli obblighi di cui agli artt. 33 e 34 del
G.D.P.R. secondo quanto indicato nei precedenti paragrafi.

REGISTRO DELLE VIOLAZIONI DEI DATI PERSONALI

Al fine di documentare le violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio, il Liceo in qualità di Titolare del trattamento ha predisposto il registro delle violazioni dei dati personali ai sensi dell'art. 33, comma 5, del GDPR.

Il Dirigente Scolastico o il soggetto da lui delegato ne curerà la compilazione in caso di eventuali data breach, inserendo tutte le informazioni utili e necessarie per la gestione della violazione dei dati personali.

CASISTICA LINEE GUIDA

Di seguito si riporta una tabella, tratta dalle *Linee Guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento UE 2016/679, elaborate dal Gruppo di lavoro articolo 29 per la protezione dei dati, adottate il 3 ottobre 2017, versione emendata e adottata in data 6 febbraio 2018,* contenente alcuni esempi di

possibili violazioni di dati personali e di comportamenti da assumere. L'elencazione è meramente esemplificativa:

ESEMPIO	NOTIFICA ALL'AUTORITA' GARANTE?	COMUNICAZIONE ALL'INTERESSATO?	NOTE/ RACCOMANDAZIONI
Un titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante un'effrazione.	No	No	Fintantoché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica.
Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare del trattamento impedisce ai clienti di chiamare il titolare del trattamento e accedere alle proprie registrazioni.	no	no	Questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5. Il titolare del trattamento deve conservare adeguate registrazioni in merito.
Un titolare del trattamento subisce un	Sì, effettuare la segnalazione all'autorità di controllo,se vi sono probabili conseguenze per le persone fisiche in quanto	Sì, effettuare la segnalazione alle persone fisiche, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di	Se fosse stato disponibile un backup e i dati avessero potuto essere ripristinati in tempo utile, non sarebbe stato necessario segnalare

attacco tramite *ransomware* che provoca la cifratura di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, diventa evidente che l'unica funzionalità dal *ransomware* era la cifratura dei dati e che non vi erano altri *malware* presenti nel sistema.	si tratta di una perdita di disponibilità	disponibilità dei dati, nonché di altre possibili conseguenze.	La violazione all'autorità di controllo o alle persone fisiche, in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o di riservatezza. Tuttavia, qualora l'autorità di controllo fosse venuta a conoscenza dell'incidente conaltri mezzi, avrebbe potuto prendere in considerazione lo svolgimento di un'indagine al fine di valutare il rispetto dei requisiti di sicurezza più ampi di cui all'articolo 32.
Una e-mail viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari.	Sì, la notifica all'autorità di controllo può essere obbligatoria se è interessato un numero elevato di persone, se vengono rivelati dati sensibili ose altri fattori presentano rischi elevati (ad esempio il messaggio di posta elettronica contiene le password iniziali).	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato soltanto un numero limitato di indirizzi di posta elettronica.

Ceglie Messapica, 02/02/2023

Il titolare del Trattamento dei dati personali

IL DIRIGENTE SCOLASTICO

(Dott.ssa Angela ALBANESE)

ISTITUTO DI ISTRUZIONE SECONDARIA SUPERIORE
"Cataldo Agostinelli"
Comprensivo di: Liceo Classico/Scientifico – I.T.E.S. – I.P.S.S.S. – I.P.S.I.A – I.P.S.E.O.A
Via Ovidio – 72013 Ceglie Messapica (BR)
Email: bris006001@istruzione.it – bris006001@istruzione.it
☎ 0831377890 - 🖷 0831379023

	Violazioni dati personali (Data Breach)		
DATA EVENTO	**TIPO DI EVENTO**	**DATI INTERESSATI**	**GESTIONE ***

*: Inserire i termini della gestione e le modalità con il riferimento all'eventuale comunicazione all'Autorità di controllo competente (Garante Privacy)

ISTITUTO DI ISTRUZIONE SECONDARIA SUPERIORE
"Cataldo Agostinelli"
Comprensivo di: Liceo Classico/Scientifico – I.T.E.S. – I.P.S.S.S. – I.P.S.I.A – I.P.S.E.O.A
Via Ovidio – 72013 Ceglie Messapica (BR)
Email: bris006001@istruzione.it – bris006001@istruzione.it
☎ 0831377890 - 🖷 0831379023

MODULO PER LA RACCOLTA DELLE INFORMAZIONI SUL DATA BREACH

Data della segnalazione	
Nome e Cognome o Denominazione del soggetto che effettua la segnalazione	
in qualità di	☐ Responsabile del trattamento ☐ Soggetto autorizzato al trattamento

Descrizione sommaria dell'evento

_____

_____

_____

_____

_____

_____

Quando si è verificato il Data Breach?

☐ In data
_____

☐ Tra il _____ e il _____

☐ In un periodo di tempo non ancora determinato _____

☐ E' ancora in corso_____

In caso di smarrimento di dispositivi, supporti portatili, faldoni, fascicoli o documenti, dove si è verificato il Data Breach?

Indicare il tipo di violazione

- ☐ Sola lettura (i dati sono stati letti, ma non copiati)
- ☐ Copia (i dati sono stati copiati)
- ☐ Alterazione (i dati presenti nei sistemi o negli archivi fisici sono stati alterati o modificati)
- ☐ Cancellazione (i dati sono stati cancellati dai sistemi e non sono più nella disponibilità del Titolare del Trattamento)
- ☐ Furto (i dati non sono più presenti sui sistemi del titolare o nei suoi archivi e sono in possesso dell'autore del Data Breach
- ☐ Crittografia (i dati sono ancora presenti sui sistemi del titolare, ma sono crittografati dall'autore del Data Breach)
- ☐ Altro (specificare)

Dispositivo o assett oggetto della violazione

- ☐ Computer fisso
- ☐ Computer portatile aziendale
- ☐ Computer portatile personale
- ☐ Dispositivo mobile aziendale
- ☐ Dispositivo mobile personale
- ☐ Documento cartaceo
- ☐ File o parte di esso
- ☐ Unità di backup
- ☐ Asset di rete
- ☐ Altro (specificare)

Descrizione sintetica degli asset coinvolti, della loro ubicazione, indicazione del nominativo del loro responsabile

_____

_____

_____

Quanti interessati sono stati coinvolti dal Data Breach?

- ☐ N.° _____ di interessati
- ☐ Circa _____ di interessati
- ☐ Un numero imprecisato di interessati

Quali sono le categorie di dati coinvolte dal Data Breach?

- ☐ Dati anagrafici
- ☐ Dati di pagamento
- ☐ Dati di contatto
- ☐ Dati di identificazione e di accesso
- ☐ Dati sanitari
- ☐ Dati relativi alla confessione religiosa
- ☐ Dati relativi all'orientamento filosofico
- ☐ Dati relativi all'appartenenza sindacale
- ☐ Dati relativi all'appartenenza politica
- ☐ Dati sull'orientamento o sulla vita sessuale
- ☐ Dati sull'origine razziale o etnica
- ☐ Dati genetici
- ☐ Dati biometrici
- ☐ Dati giudiziari

Qual è il livello di gravità del Data Breach?

- ☐ Basso
- ☐ Medio
- ☐ Alto

Misure tecniche e organizzative già in essere per la mitigazione o il contrasto del rischio verificatosi

_____

_____

_____

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Ransomware

Attenzione al ransomware. Il programma che prende "in ostaggio" il tuo dispositivo

L'emergenza sanitaria da Covid2019 - che porta molte più persone e per molto più tempo ad essere connesse online e ad utilizzare dispositivi digitali - sembra essere affiancata da un pericoloso "contagio digitale", alimentato da malintenzionati che diffondono software "malevoli" per varie finalità illecite. Una delle attività più diffuse e dannose è attualmente il cosiddetto ransomware.

1. Cos'e' il ransomware?

Il ransomware è un programma informatico dannoso ("malevolo") che può "infettare" un dispositivo digitale (PC, tablet, smartphone, smart TV), bloccando l'accesso a tutti o ad alcuni dei suoi contenuti (foto, video, file, ecc.) per poi chiedere un **riscatto** (in inglese, "ransom") da pagare per "liberarli".

La richiesta di pagamento, con le relative istruzioni, compare di solito in una finestra che si apre automaticamente sullo schermo del dispositivo infettato. All'utente viene minacciosamente comunicato che ha poche ore o pochi giorni per effettuare il versamento del riscatto, altrimenti il blocco dei contenuti diventerà definitivo.

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).

2. Come si diffonde?

Anche se in alcuni casi (non molto frequenti) il ransomware può essere installato sul dispositivo tramite sofisticate forme di attacco informatico (es: controllo da remoto), questo tipo di software malevoli si diffonde soprattutto attraverso comunicazioni ricevute via e-mail, sms o sistemi di messaggistica che:

• sembrano apparentemente provenire da **soggetti conosciuti e affidabili** (ad esempio, corrieri espressi, gestori di servizi, operatori telefonici, pubbliche amministrazioni, ecc.), oppure da **persone fidate** (colleghi di lavoro, conoscenti);

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

In altri casi, il ransomware può essere scaricato sul dispositivo quando l'utente:

• clicca **link o banner pubblicitari su siti web** (un canale molto usato è rappresentato dai siti per adulti) o social network;

• naviga su **siti web creati ad hoc o "compromessi"** da hacker per diventare veicolo del contagio ransomware.

Il ransomware può essere diffuso da malintenzionati anche attraverso **software e app** (giochi, utilità per il PC, persino falsi anti-virus), offerti gratuitamente per invogliare gli utenti al download e infettare così i loro dispositivi.

E' bene ricordare che **ogni dispositivo "infettato" ne può "contagiare" altri**. Il ransomware può diffondersi sfruttando, ad esempio, le sincronizzazioni tra dispositivi, i sistemi di condivisione in cloud, oppure può impossessarsi della rubrica dei contatti e utilizzarla per spedire automaticamente ad altre persone messaggi contenenti link e allegati che diventano veicolo del ransomware.

3. Come difendersi?

La prima e più importante forma di difesa è la prudenza. Occorre evitare di aprire messaggi provenienti da soggetti sconosciuti o con i quali non si hanno rapporti (ad es. un operatore telefonico di cui non si è cliente, un corriere espresso da cui non si aspettano consegne, ecc.) e, in ogni caso, se si hanno dubbi, non si deve cliccare su link o banner sospetti e non si devono aprire allegati di cui si ognora il contenuto.

Anche se i messaggi provengono da soggetti a noi noti, è comunque bene adottare alcune piccole accortezze. Ad esempio:

- 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);

- non scaricare **software da siti sospetti** (ad esempio, quelli che offrono gratuitamente prodotti che invece di solito sono a pagamento);

- **scaricare preferibilmente app e programmi da market ufficiali**, i cui gestori effettuano controlli sui prodotti e dove è eventualmente possibile leggere i commenti di altri utenti che contengono avvisi sui potenziali rischi;

- se si usa un pc, 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).

E' inoltre utile:

• installare su tutti i dispositivi un **antivirus con estensioni anti-malware**;

• **mantenere costantemente aggiornati** il sistema operativo oltre che i software e le app che vengono utilizzati più spesso;

• utilizzare dei sistemi di **backup** che salvino (anche in maniera automatica) una copia dei dati (sono disponibili soluzioni anche libere e gratuite per tutti i sistemi operativi). Con un corretto backup, in caso di necessità, si potranno così ripristinare i dati contenuti nel dispositivo, quantomeno fino all'ultimo salvataggio.

4. Come liberarsi dal ransomware?

Pagare il riscatto è solo apparentemente la soluzione più facile. Oltre al danno economico, si corre infatti il rischio di non ricevere i codici di sblocco, o addirittura di finire in "liste di pagatori" potenzialmente soggetti a periodici attacchi ransomware.

La soluzione consigliata è quella di rivolgersi a **tecnici specializzati** capaci di sbloccare il dispositivo.

Un'alternativa efficace è quella di **formattare il dispositivo**: ma in questo caso, oltre ad eliminare il malware, si perdono tutti i dati in esso contenuti. Per questo è fondamentale (come suggerito) effettuare backup periodici dei contenuti (che è sempre una buona prassi) in modo da non perderli in caso di incidenti (es: danneggiamento del dispositivo, ecc.) o attacchi informatici che necessitano di interventi di ripristino.

E' sempre consigliabile segnalare o denunciare l'attacco ransomware alla **Polizia postale** (**https://www.commissariatodips.it**), anche per aiutare a prevenire ulteriori illeciti.

È possibile, inoltre, rivolgersi al **Garante** nel caso si voglia segnalare una eventuale violazione in materia di dati personali (furto di identità, sottrazione di dati personali, furto di contenuti, ecc.), seguendo le indicazioni della pagina **https://www.garanteprivacy.it/home/diritti/come-agire-per-tutelare-i-tuoi-dati-personali**.

ISTITUTO DI ISTRUZIONE SECONDARIA SUPERIORE
"Cataldo Agostinelli"
Comprensivo di: Liceo Classico/Scientifico – I.T.E.S. – I.P.S.S.S. – I.P.S.I.A – I.P.S.E.O.A
Via Ovidio – 72013 Ceglie Messapica (BR)
Email: bris006001@istruzione.it – bris006001@istruzione.it
☎ 0831377890 - 🖷 0831379023

ESERCIZIO DI DIRITTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(artt. 15-22 del Regolamento (UE) 2016/679)

Il/La sottoscritto/a.....
nato/a a.....il....., esercita con la presente richiesta i seguenti diritti di cui agli artt. 15-22 del Regolamento (UE) 2016/679:

1. Accesso ai dati personali

(art. 15 del Regolamento (UE) 2016/679)

Il sottoscritto *(barrare solo le caselle che interessano)*:
chiede conferma che sia o meno in corso un trattamento di dati personali che lo riguardano;
in caso di conferma, chiede di ottenere l'accesso a tali dati, una copia degli stessi, e tutte le informazioni, previste alle lettere da a) a h) dell' art. 15, paragrafo 1, del Regolamento (UE) 2016/679, e in particolare;

- le finalità del trattamento;
- le categorie di dati personali trattate;
- i destinatari o le categorie di destinatari, a cui i dati personali sono stati o saranno comunicati, in particolare, se destinatari di paesi terzi o organizzazioni internazionali;
- il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati, per determinare tale periodo;
- l' origine dei dati (ovvero il soggetto o la specifica fonte dalla quale essi sono stati acquisiti);
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste da tale trattamento per l'interessato.

2. Richiesta di intervento sui dati

(artt. 16-18 del Regolamento (UE) 2016/679)

Il sottoscritto chiede di effettuare le seguenti operazioni *(barrare solo le caselle che interessano)*:

rettificazione e/o aggiornamento dei dati (art. 16 del Regolamento (UE) 2016/679);

cancellazione dei dati (art. 17, paragrafo 1, del Regolamento (UE) 2016/679), per i seguenti motivi *(specificare quali)*:

a)...;

b)....;

c)...;

nei casi previsti all' art. 17, paragrafo 2, del Regolamento (UE) 2016/679, l' attestazione che il titolare ha informato altri titolari di trattamento della richiesta dell' interessato di cancellare link, copie o riproduzioni dei suoi dati personali;

limitazione del trattamento (art. 18) per i seguenti motivi *(barrare le caselle che interessano)*:

- contesta l' esattezza dei dati personali;
- il trattamento dei dati è illecito;
- i dati sono necessari all' interessato per l' accertamento, l' esercizio o la difesa di un diritto in sede giudiziaria;
- l' interessato si è opposto al trattamento dei dati ai sensi dell' art. 21, paragrafo 1, del Regolamento (UE) 2016/679.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

3.Portabilità dei dati[1]

(art. 20 del Regolamento (UE) 2016/679)

Con riferimento a tutti i dati personali forniti al titolare, il sottoscritto chiede di *(barrare solo le caselle che interessano)*:

ricevere tali dati in un formato strutturato, di uso comune e leggibile da dispositivo automatico;

trasmettere direttamente al seguente diverso titolare del trattamento *(specificare i riferimenti identificativi e di contatto del titolare: .....)*:

tutti i dati personali forniti al titolare;

un sottoinsieme di tali dati.

La presente richiesta riguarda (indicare i dati personali, le categorie di dati o il trattamento cui si fa riferimento):

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

4. Opposizione al trattamento

(art. 21, paragrafo 1 del Regolamento (UE) 2016/679)

Il sottoscritto si oppone al trattamento dei suoi dati personali ai sensi dell' art. 6, paragrafo 1, lettera e) o lettera f), per i seguenti motivi legati alla sua situazione particolare (specificare):

_____

_____

_____

_____

_____

1

5. Opposizione al trattamento per fini di marketing diretto

(art. 21, paragrafo 2 del Regolamento (UE) 2016/679)

Il sottoscritto si oppone al trattamento dei dati effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Il sottoscritto:

Chiede di essere informato, ai sensi dell' art. 12, paragrafo 4 del Regolamento (UE) 2016/679, al più tardi entro un mese dal ricevimento della presente richiesta, degli eventuali motivi, che impediscono al titolare di fornire le informazioni o svolgere le operazioni richieste.

Chiede, in particolare, di essere informato della sussistenza di eventuali condizioni che impediscono al titolare di identificarlo come interessato, ai sensi dell' art. 11, paragrafo 2, del Regolamento (UE) 2016/679.

Recapito per la risposta[2]**:**

Via/Piazza

Comune Provincia Codice postale

oppure

e-mail/PEC:

Eventuali precisazioni

Il sottoscritto precisa (fornire eventuali spiegazioni utili o indicare eventuali documenti allegati):

(Luogo e data) **(Firma)**

2 Allegare copia di un documento di riconoscimento

ISTITUTO DI ISTRUZIONE SECONDARIA SUPERIORE
"Cataldo Agostinelli"
Comprensivo di: Liceo Classico/Scientifico – I.T.E.S. – I.P.S.S.S. – I.P.S.I.A – I.P.S.E.O.A
Via Ovidio – 72013 Ceglie Messapica (BR)
Email: bris006001@istruzione.it – bris006001@istruzione.it
☎ 0831377890 - 🖷 0831379023

INFORMATIVA AI SENSI DEGLI ART. 13-14-15 DEL GDPR (GENERAL DATA PROTECTION REGULATION) 2016/679

SCAMBIO DATI RELATIVI ALLA SITUAZIONE VACCINALE

Prima che Lei ci fornisca i dati personali che La riguardano, in applicazione del Regolamento Europeo sulla protezione dei dati personali, è opportuno che prenda visione si una serie di informazioni che La possono aiutare a comprendere le motivazioni per le quali i Suoi dati verranno trattati e quali sono i diritti che potrà esercitare rispetto a questo trattamento.

Introduzione e definizioni generali	Come è noto il "Decreto Vaccini" (D.L. 73/2017 convertito con Legge 119/2017) prevede che il sistema scolastico, statale e paritario, i servizi educativi per l'infanzia nonché i centri di formazione professionale regionali, attivino un canale di comunicazione con le Aziende Sanitarie Locali competenti al fine di assicurare l'applicazione della normativa che prevede, tra l'altro, conseguenze per i minori di anni 16 che non risultino essere in regola con gli obblighi vaccinali introdotti dalla Legge. A tale fine il Ministero dell'Istruzione, **Università** e Ricerca, di concerto con il Ministero della Salute, hanno emesso in data 27 Febbraio 2018 un documento recante: "*Indicazioni operative per l'attuazione dell'articolo 18-ter del D.L. 148/2017 convertito con modificazioni dalla L. 172/2017, e per l'attuazione dell'articolo 3 del D.L. 73/2017 convertito con modificazioni dalla L. 119/2017, per gli anni scolastici/calendari annuali 2017/18 e 2018/19*". Di tale documento è stata data comunicazione preventiva al Garante per la Protezione dei Dati Personali, che in data 22 Febbraio 2018 ha espresso parere favorevole (Registro dei provvedimenti n.117) con particolare riferimento alle **modalità** tecniche di comunicazione indicate all'Allegato A del medesimo documento recanti: "***modalità*** *operative per lo scambio dei dati relativi alla situazione vaccinale degli iscritti tra le istituzioni scolastiche/educative e formative a l'Azienda sanitaria locale competente*".

Quali garanzie ho che i miei dati siano trattati nel rispetto dei miei diritti e delle mie libertà personali?	Lo scambio dei dati fra la scuola e l'Azienda sanitaria locale territorialmente competente avviene esclusivamente attraverso una piattaforma web di caricamento dati della Regione in formato elettronico (CSV) inserendo le credenziali fornite dall'ATS via pec. La scuola provvede alle comunicazioni oggetto della presente informativa mediante "upload" delle informazioni tramite file redatto in formato elettronico elaborabile (CSV) e "download" dell'esito della verifica tramite un file completato a cura dell'A.S.L. competente, sempre redatto in formato elettronico elaborabile (CSV). Il sistema informatico scolastico nell'ambito del quale avviene il trattamento dei dati inerenti al profilo vaccinale dell'interessato è conforme a quanto previsto dalla normativa vigente in materia di misure di sicurezza adeguate ad assicurare il livello di riservatezza richiesto dalla natura dei dati oggetto di trattamento.
Quali dati verranno trattati?	Per consentire l'identificazione certa di ogni soggetto, per ogni interessato i dati scambiati devono contenere le seguenti informazioni anagrafiche: 1. COGNOME E NOME 2. DATA DI NASCITA 3. COMUNE DI NASCITA (se straniero, il Paese di origine) 4. SESSO 5. CODICE FISCALE 6. CODICE MECCANOGRAFICO PLESSO SCOLASTICO 7. CODICE FISCALE SCUOLA 8. NOME SCUOLA 9. DESCRIZIONE SCUOLA 10. STATO VACCINALE (utilizzando esclusivamente le seguenti diciture: "non in regola con gli obblighi vaccinali", "non ricade nelle condizioni di esonero, omissione o differimento", "non ha presentato formale richiesta di vaccinazione").
Quali sono i miei diritti?	L'interessato ha diritto di chiedere al Titolare del trattamento: - L'accesso ai propri dati e la loro rettifica; L'interessato ha inoltre diritto a proporre reclamo all'Autorità di controllo dello Stato di residenza, nonché a revocare il consenso al trattamento ai sensi dell'Art. 6 del G.D.P.R. I diritti sopra esposti possono essere esercitati mediante invio di una specifica richiesta al Titolare del trattamento oppure al Responsabile della Protezione dei Dati (R.P.D./D.P.O.).
Cosa accade se non conferisco i miei dati?	Il conferimento dei dati è obbligatorio, l'eventuale rifiuto a fornire tali dati comporterà l'applicazione delle conseguenze amministrative e sanzionatorie previste dal citato "Decreto Vaccini".
Chi è il Titolare del trattamento?	L'Istituto Scolastico nella persona del Dirigente Scolastico pro tempore
Responsabile della protezione dei dati (R.P.D. / D.P.O.)	Dottor Ivano Pecis I&P Partners S.r.l. con sede in Falerna (CZ), Via Vittoria 8 - Partita I.V.A. 03735350799 Email: amministrazione@ip-privacy.it - PEC: dpo.pecis@pec.it

Nome e Cognome dell'alunno: .....

Classe: _____ Sezione: _____

FIRME PER PRESA VISIONE

Cognome e nome 1° Genitore .....

Firma ..... (*)

Cognome e nome 2° Genitore .....

Firma .....

Luogo e data .....

(*) Qualora l'informativa in oggetto venga firmata per presa visione da parte di un solo genitore, visti gli Artt. 316 comma 1 e 337 ter comma 3 del Codice Civile si presuppone la condivisione da parte di entrambi i genitori.

ISTITUTO DI ISTRUZIONE SECONDARIA SUPERIORE
"Cataldo Agostinelli"
Comprensivo di: Liceo Classico/Scientifico – I.T.E.S. – I.P.S.S.S. – I.P.S.I.A – I.P.S.E.O.A
Via Ovidio – 72013 Ceglie Messapica (BR)
Email: bris006001@istruzione.it – bris006001@istruzione.it
☎ 0831377890 - 🖷 0831379023

INFORMATIVA PRIVACY ALLE FAMIGLIE
PER I SERVIZI A SUPPORTO DELL'INCLUSIONE SCOLASTICA

Redatta ai sensi degli Artt. da 13 a 15 del Regolamento U.E. 2016/679 (G.D.P.R.)

Prima che Lei ci fornisca i dati personali che La riguardano, in applicazione del Regolamento Europeo sulla protezione dei dati personali, è opportuno che prenda visione si una serie di informazioni che La possono aiutare a comprendere le motivazioni per le quali i Suoi dati verranno trattati e quali sono i diritti che potrà esercitare rispetto a questo trattamento.

Per quale finalità saranno trattati i miei dati personali?	Il trattamento dei dati personali necessari, pertinenti e non eccedenti, conseguente all'iscrizione dell'allievo all'Istituto scolastico avverrà allo scopo di ottemperare al meglio al diritto-dovere all'istruzione ed alla formazione, anche a favore di studenti diversamente abili, nell'ambito delle finalità istituzionali di questo Istituto. Il Ministero dell'Istruzione, Università e Ricerca scientifica (di seguito M.I.U.R.) ha istituito il "Sistema nazionale delle anagrafe degli studenti" che prevede che l'Istituto scrivente, ai sensi dell'Art. 13 Legge 128/2013, inserisca i dati relativi alla disabilità degli allievi (trasmettendo anche le certificazioni clinico-mediche attestanti la condizione patologica del ragazzo) sul portale informatico ministeriale dei servizi denominato "S.I.D.I." al fine di consentire il costante miglioramento dell'integrazione scolastica degli alunni disabili mediante l'assegnazione del personale docente di sostegno, ma tale accesso, in conformità con il parere espresso dall'Autorità Garante per la Protezione dei Dati Personali, avverrà separatamente tra la partizione contenente le diagnosi funzionali e gli altri dati di natura meramente anagrafica.
Quali garanzie ho che i miei dati siano trattati nel rispetto dei miei diritti e delle mie libertà personali?	Il trattamento, al fine dell'inserimento sul portale S.I.D.I., avverrà nell'ambito degli uffici di Presidenza e di segreteria da parte del Dirigente Scolastico o di suo delegato specifico in modalità sia manuale che informatica. I delegati sono: – assistenti amministrativi, per i dati trattati nell'ambito delle attività di competenza della segreteria scolastica; – tutti i docenti, per i dati di frequenza, percorso, comportamento e di profitto degli alunni; – i membri degli OO.CC., per i dati trattati nell'ambito delle sedute collegiali. A garanzia della riservatezza dei dati saranno applicate misure minime di sicurezza organizzative ed informatiche di cui viene data evidenza all'interno del "Documento delle misure a tutela dei dati delle persone" elaborato da questa Istituzione scolastica. L'Istituto ha provveduto ad impartire ai propri incaricati istruzioni precise in merito alle condotte da tenere ad alle procedure da applicare per garantire la riservatezza dei dati dei propri utenti. Non verrà eseguito su di essi alcun processo decisionale automatizzato (profilazione).
I miei dati entreranno nella disponibilità di altri soggetti?	I dati personali e particolari (sensibili inerenti allo stato di salute quali certificazioni mediche, Profilo Dinamico Funzionale, Piano Educativo Individualizzato etc.) forniti verranno comunicati al M.I.U.R. e, limitatamente ai dati anagrafici, agli Enti Locali interessati (Comune di residenza) al fine dell'erogazione dei servizi di loro competenza (fornitura di personale docente/educatore specializzato, organizzazione del servizio di trasporto, refezione etc.).** In caso di trasferimento il fascicolo personale verrà trasmesso ad altro Istituto destinatario. Gli stessi non verranno trasferiti a destinatari residenti in paesi terzi rispetto all'Unione Europea né ad organizzazioni internazionali.
Per quanto tempo terrete i miei dati?	I dati saranno conservati presso l'Istituto per tutto il tempo in cui l'iscrizione sarà attiva ed in seguito, in caso di trasferimento ad altra Istituzione o cessazione del rapporto, verranno trattenuti esclusivamente i dati minimi e per il periodo di conservazione obbligatorio previsto dalla normativa vigente.
Quali sono i miei diritti?	L'interessato ha diritto di chiedere al Titolare del trattamento: - L'accesso ai propri dati, la loro rettifica o cancellazione; - La limitazione e di opporsi al trattamento dei dati personali che lo riguardano; - La portabilità dei dati; L'interessato ha inoltre diritto a proporre reclamo all'Autorità di controllo dello Stato di residenza, nonché a revocare il consenso al trattamento ai sensi dell'Art. 6 del G.D.P.R.
Cosa accade se non conferisco i miei dati?	Il mancato, parziale o inesatto conferimento dei dati potrebbe generare quale conseguenza l'impossibilità di fornire allo studente tutti i servizi necessari per garantire il suo diritto all'istruzione ed alla formazione.

RICHIESTE DI MANIFESTAZIONE DEL CONSENSO AI SENSI DELL'ART. 7 DEL REGOLAMENTO U.E.

RICHIESTA (APPORRE UNA **X** NELLE COLONNE A DESTRA IN CORRISPONDENZA DELLA SCELTA FATTA)	ACCONSENTO	NON ACCONSENTO
Allo scopo di ottemperare al meglio al diritto-dovere all'istruzione ed alla formazione, anche a favore di studenti diversamente abili e di consentire il costante miglioramento dell'integrazione scolastica degli alunni disabili mediante l'assegnazione del personale docente di sostegno e di servizi specifici dedicati, si autorizza all'inserimento sul portale ministeriale S.I.D.I. dei dati sopra indicati.		
Qualora l'allievo dovesse cambiare Istituto di frequenza, i dati inerenti allo stato di disabilità verranno trasmessi alla nuova Istituzione Scolastica, consentendo alla stessa di accedere al fascicolo disabilità costituito presso l'Istituzione scrivente contenente il verbale di accertamento del collegio medico-legale, la diagnosi funzionale, il profilo dinamico funzionale (P.D.F.), il piano educativo individualizzato (P.E.I.) etc. (Nel caso di mancato ottenimento del consenso a tale trasmissione, il fascicolo di disabilità viene storicizzato presso l'Istituto scrivente e reso non consultabile da altra Istituzione scolastica).		
Allo scopo di favorire e attuare progetti di scambio tra istituti Scolastici, si autorizza la trasmissione dei dati relativi alla disabilità agli Istituti Scolastici di destinazione. Non saranno trasmessi documenti contenenti relazioni, diagnosi funzionali o altre informazioni mediche.		

Luogo e data .....

FIRME PER PRESA VISIONE

Cognome e nome 1° Genitore ..... Firma ..... (*)

Cognome e nome 2° Genitore .....Firma .....

(*) Qualora l'informativa in oggetto venga firmata per presa visione da parte di un solo genitore, visti gli Artt. 316 comma 1 e 337 ter comma 3 del Codice Civile si presuppone la condivisione da parte di entrambi i genitori.

(**) In caso di fini istituzionali non è richiesto alcun consenso da parte del soggetto titolare del diritto, se non in casi particolari su indicazioni del TDM di competenza.

ISTITUTO DI ISTRUZIONE SECONDARIA SUPERIORE
"Cataldo Agostinelli"
Comprensivo di: Liceo Classico/Scientifico – I.T.E.S. – I.P.S.S.S. – I.P.S.I.A – I.P.S.E.O.A
Via Ovidio – 72013 Ceglie Messapica (BR)
Email: bris006001@istruzione.it – bris006001@istruzione.it
☎ 0831377890 - 🖷 0831379023

INFORMATIVA PRIVACY AGLI UTENTI DEL SITO (newsletter)

Redatta ai sensi degli Artt. da 13 a 15 del Regolamento U.E. 2016/679 (G.D.P.R.)

La presente viene resa agli utenti che accedono al sito web dell'Istituto e che desiderano iscriversi alla newsletter informativa gratuita, presente su di esso, al fine di ricevere periodiche informazioni riguardanti la vita dell'Istituto, i commenti ai fatti, i promemoria per le scadenze ed ogni altra informazione sulle iniziative prese.

Per quale finalità saranno trattati i miei dati personali?	I tuoi dati di contatto verranno custoditi nella banca dati elettronica dell'Istituto Scolastico, residente sull'area del sito internet istituzionale, al solo fine di rendere possibile l'invio periodico di e-mail per i fini già sopra esposti di informazione, commento e promemoria circa le attività svolte dall'Istituto. Unica fonte di legittimazione rispetto a questo trattamento è il tuo consenso, che potrai revocare in ogni momento determinando così la cancellazione dalla newsletter.
Quali garanzie ho che i miei dati siano trattati nel rispetto dei miei diritti e delle mie libertà personali?	Il trattamento avverrà nell'ambito degli uffici di segreteria e dei locali in cui avviene l'attività l'i.t. di Istituto in modalità completamente informatica. A garanzia della riservatezza dei dati saranno applicate misure di sicurezza organizzative ed informatiche adeguate di cui viene data evidenza all'interno del "Documento delle misure a tutela dei dati delle persone" elaborato da questa Istituzione scolastica. Non verrà eseguito su di essi alcun processo decisionale automatizzato (profilazione).
I miei dati entreranno nella disponibilità di altri soggetti?	I Dati personali in questione (indirizzo e-mail) non verranno ceduti a terzi né comunicati a chicchessia. Gli stessi non verranno trasferiti a destinatari residenti in paesi terzi rispetto all'Unione Europea né ad organizzazioni internazionali.
Per quanto tempo terrete i miei dati?	I dati saranno conservati presso l'Istituto per tutto il tempo in cui la prestazione sarà attiva, non appena la scuola dovesse ricevere la revoca del consenso con il conseguente ordine di cancellazione dell'indirizzo e-mail dalla newsletter, lo stesso verrà prontamente eseguito.
Quali sono i miei diritti?	L'interessato ha diritto di chiedere al Titolare del trattamento: - L'accesso ai propri dati, la loro rettifica o cancellazione; - La limitazione e di opporsi al trattamento dei dati personali che lo riguardano; - La portabilità dei dati; L'interessato ha inoltre diritto a proporre reclamo all'Autorità di controllo dello Stato di residenza, nonché a revocare il consenso al trattamento ai sensi dell'Art. 6 del G.D.P.R.
Cosa accade se non conferisco i miei dati?	Il conferimento dei dati non è obbligatorio se non al fine dell'invio delle comunicazioni informative tramite e-mail. L'eventuale rifiuto al trattamento ovvero il mancato, inesatto o parziale conferimento dei dati avrà come conseguenza certa l'impossibilità di una corretta erogazione del servizio.
Chi è il Titolare del trattamento?	L'Istituto Scolastico nella persona del Dirigente Scolastico pro tempore
Responsabile della protezione dei dati (R.P.D. / D.P.O.)	Dottor Ivano Pecis I&P Partners S.r.l. con sede in Falerna (CZ), Via Vittoria 8 - Partita I.V.A. 03735350799 e-mail: amministrazione@ip-privacy.it - PEC dpo.pecis@pec.it

L'atto volontario di iscrizione alla newsletter e sottoscrizione della stessa costituisce accettazione esplicita delle condizioni presenti in questa informativa e viene registrato come dimostrazione di consenso da parte dell'utente.

ISTITUTO DI ISTRUZIONE SECONDARIA SUPERIORE
"Cataldo Agostinelli"
Comprensivo di: Liceo Classico/Scientifico – I.T.E.S. – I.P.S.S.S. – I.P.S.I.A – I.P.S.E.O.A
Via Ovidio – 72013 Ceglie Messapica (BR)
Email: bris006001@istruzione.it – bris006001@istruzione.it
☎ 0831377890 - 🖷 0831379023

INFORMATIVA PRIVACY AI DIPENDENTI – ACCESSO ALLA RETE WIFI

Redatta ai sensi degli Artt. da 13 a 15 del Regolamento U.E. 2016/679 (G.D.P.R.)

Prima che Lei ci fornisca i dati personali che La riguardano, in applicazione del Regolamento Europeo sulla protezione dei dati personali, è opportuno che prenda visione si una serie di informazioni che La possono aiutare a comprendere le motivazioni per le quali i Suoi dati verranno trattati e quali sono i diritti che potrà esercitare rispetto a questo trattamento.

Per quale finalità saranno trattati i miei dati personali?	Il trattamento dei dati personali necessari, pertinenti e non eccedenti, si rende necessario per consentire ai dipendenti di usufruire del servizio di connessione WIFI dell'Istituto. La **Direttiva del Presidente del Consiglio dei Ministri** del 1 agosto 2015, "*Misure minime di sicurezza ICT per le Pubbliche Amministrazioni*" prevede diversi livelli di attuazione, tra cui la necessità di accesso individualizzato alla rete WIFI. I sistemi informatici e le procedure software preposte al funzionamento della rete WIFI acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet. Si tratta di dati che non vengono accompagnati da alcuna informazione personale aggiuntiva e vengono utilizzati per ricavare informazioni statistiche sul sito, gestire il corretto funzionamento e per fini di sicurezza. I Dati potrebbero essere utilizzati per l'accertamento di Responsabilità in caso di ipotetici reati informatici ai danni del sito. Le informazioni raccolte potrebbero essere ad esempio: indirizzo IP, tipo di browser e parametri del dispositivo usato per connettersi al sito, nome dell'internet service provider (ISP), data e orario di connessione, pagine web visitate. A fini di sicurezza (filtri antispam, firewall, rilevazione virus), i dati registrati automaticamente (come indirizzo IP) potrebbero essere utilizzati, conformemente alle leggi vigenti in materia, al fine di bloccare tentativi di danneggiamento al sito medesimo o di recare danno ad altri utenti, o comunque attività dannose o costituenti reato. Tali dati non sono mai utilizzati per l'identificazione o la profilazione dell'utente, ma solo a fini di tutela del sito e dei suoi utenti e in base ai legittimi interessi del titolare).
Quali garanzie ho che i miei dati siano trattati nel rispetto dei miei diritti e delle mie libertà personali?	Il trattamento avverrà nell'ambito degli uffici di segreteria e dei locali scolastici in genere in modalità sia manuale che informatica. A garanzia della riservatezza dei dati saranno applicate misure minime di sicurezza organizzative ed informatiche di cui viene data evidenza all'interno del "Registro dei trattamenti" elaborato da questa Istituzione scolastica. L'Istituto ha provveduto ad impartire ai propri incaricati istruzioni precise in merito alle condotte da tenere ad alle procedure da applicare per garantire la riservatezza dei dati dei propri utenti. Non verrà eseguito su di essi alcun processo decisionale automatizzato (profilazione).
I miei dati entreranno nella disponibilità di altri soggetti?	I dati forniti non entreranno nella disponibilità di alcuna figura terza esterna all'Istituto o ai suoi incaricati.
Per quanto tempo terrete i miei dati?	I dati saranno conservati presso l'Istituto per tutto il tempo in cui sarà attivo un contratto di prestazione tra l'Istituto e il dipendente ed in seguito, in caso di trasferimento ad altra Istituzione o cessazione del rapporto, verranno trattenuti esclusivamente i dati minimi e per il periodo di conservazione obbligatorio previsto dalla normativa vigente.
Quali sono i miei diritti?	L'interessato ha diritto di chiedere al Titolare del trattamento: - L'accesso ai propri dati, la loro rettifica o cancellazione; - La limitazione e di opporsi al trattamento dei dati personali che lo riguardano; - La portabilità dei dati; L'interessato ha inoltre diritto a proporre reclamo all'Autorità di controllo dello Stato di residenza, nonché a revocare il consenso al trattamento ai sensi dell'Art. 6 del G.D.P.R.
Cosa accade se non conferisco i miei dati?	Il conferimento dei dati personali è necessario se il dipendente intende fare utilizzo della rete WIFI messa a disposizione, gratuitamente e per scopi didattici, dall'Istituto.
Chi è il Titolare del trattamento?	L'Istituto Scolastico nella persona del Dirigente Scolastico pro tempore
Responsabile della protezione dei dati (R.P.D. / D.P.O.)	Dottor Ivano Pecis I&P Partners S.r.l. con sede in Falerna (CZ), Via Vittoria 8 - Partita I.V.A. 03735350799 e-mail: amministrazione@ip-privacy.it - PEC: dpo.pecis@pec.it

ISTITUTO DI ISTRUZIONE SECONDARIA SUPERIORE
"Cataldo Agostinelli"
Comprensivo di: Liceo Classico/Scientifico – I.T.E.S. – I.P.S.S.S. – I.P.S.I.A – I.P.S.E.O.A
Via Ovidio – 72013 Ceglie Messapica (BR)
Email: bris006001@istruzione.it – bris006001@istruzione.it
☎ 0831377890 - 🖷 0831379023

INFORMATIVA COOKIES AGLI UTENTI DEL SITO

Redatta ai sensi degli Artt. da 13 a 15 del Regolamento U.E. 2016/679 (G.D.P.R.)

Per quale finalità saranno trattati i miei dati personali?	I cookies sono piccoli file di testo che possono essere utilizzati dai siti web per rendere più efficiente l'esperienza per l'utente. La legge afferma che possiamo memorizzare i cookie sul suo dispositivo se sono strettamente necessari per il funzionamento di questo sito. Per tutti gli altri tipi di cookie abbiamo bisogno del suo permesso. Questo sito utilizza diversi tipi di cookie. Alcuni cookie sono collocati da servizi di terzi che compaiono sulle nostre pagine. In qualsiasi momento è possibile modificare o revocare il proprio consenso sul nostro sito Web. I cookies utilizzati sul sito hanno la finalità di eseguire autenticazioni informatiche o il monitoraggio di sessioni e la memorizzazione di informazioni tecniche specifiche riguardanti gli utenti che accedono al nostro server. In tale ottica, alcune operazioni sul sito non potrebbero essere compiute senza l'uso dei cookies, che in tali casi sono quindi tecnicamente necessari. A titolo esemplificativo, l'accesso ad aree riservate del sito e le attività che possono essere ivi svolte sarebbero molto più complesse da svolgere e meno sicure senza la presenza di cookies che consentono di identificare l'utente e mantenerne l'identificazione nell'ambito della sessione. I cookies "tecnici", a norma di legge, possano essere utilizzati anche in assenza del consenso dell'interessato. Il nostro Istituto informa dunque in primo luogo che sul sito sono operativi cookies tecnici necessari per navigare all'interno del sito stesso ed altri cookies utilizzati per analizzare statisticamente gli accessi/le visite al sito (cookies cosiddetti "analytics") che perseguono esclusivamente scopi statistici (e non anche di profilazione o di marketing) e raccolgono informazioni in forma aggregata senza possibilità di risalire alla identificazione del singolo utente. In questi casi, dal momento che la normativa vigente prescrive che per i cookies analytics sia fornita all'interessato l'indicazione chiara e adeguata delle modalità semplici per opporsi (opt-out) al loro impianto (compresi eventuali meccanismi di anonimizzazione dei cookies stessi), specifichiamo che è possibile procedere alla disattivazione dei cookies analytics come segue: aprire il proprio browser, selezionare il menu impostazioni , cliccare sulle opzioni internet, aprire la scheda relativa alla privacy e scegliere il desiderato livello di blocco cookies. Qualora si voglia eliminare i cookies già salvati in memoria è sufficiente aprire la scheda sicurezza ed eliminare la cronologia spuntando la casella "elimina cookies".
I miei dati entreranno nella disponibilità di altri soggetti?	No, nessun dato verrà trasmesso a terzi da parte nostra.
Quali sono i miei diritti?	L'interessato ha diritto di chiedere al Titolare del trattamento: - L'accesso ai propri dati, la loro rettifica o cancellazione; - La limitazione e di opporsi al trattamento dei dati personali che lo riguardano; - La portabilità dei dati; L'interessato ha inoltre diritto a proporre reclamo all'Autorità di controllo dello Stato di residenza, nonché a revocare il consenso al trattamento ai sensi dell'Art. 6 del G.D.P.R.
Chi è il Titolare del trattamento?	L'Istituto Scolastico nella persona del Dirigente Scolastico pro tempore
Responsabile della protezione dei dati (R.P.D. / D.P.O.)	Dottor Ivano Pecis I&P Partners S.r.l. con sede in Falerna (CZ), Via Vittoria 8 - Partita I.V.A. 03735350799 e-mail: amministrazione@ip-privacy.it - PEC: dpo.pecis@pec.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Scheda aggiornata in base alla versione delle Linee guida del WP29 emendata e adottata il 4 ottobre 2017

Valutazione di impatto sulla protezione dei dati (DPIA) – Art. 35 del Regolamento UE/2016/679

COSA È?

È una procedura prevista dall'**articolo 35 del Regolamento UE/2016/679 (RGPD**) che mira a descrivere un trattamento di dati per **valutarne la necessità e la proporzionalità nonché i relativi rischi**, allo scopo di approntare misure idonee ad affrontarli. Una DPIA **può riguardare un singolo trattamento oppure più trattamenti** che presentano **analogie** in termini di natura, ambito, contesto, finalità e rischi.

PERCHÉ?

La DPIA è uno strumento importante in termini di responsabilizzazione *(accountability)* in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, **la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali.** Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego **per tutti i trattamenti**, e **non solo** nei casi in cui il Regolamento la prescrive come obbligatoria.

IN CHE MOMENTO?

La DPIA deve essere condotta **prima** di procedere al trattamento. Dovrebbe comunque essere previsto un **riesame continuo** della DPIA, **ripetendo la valutazione a intervalli regolari.**

CHI?

La **responsabilità** della DPIA spetta al **titolare**, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare **ne monitora** lo svolgimento **consultandosi** con il **responsabile della protezione dei dati** (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del **responsabile della sicurezza dei sistemi informativi** *(Chief Information Security Officer, CISO)* e **del responsabile IT**.

QUANDO LA DPIA E' OBBLIGATORIA?

In tutti i casi in cui un trattamento può presentare un **rischio elevato per i diritti e le libertà** delle persone fisiche.
Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:
- trattamenti valutativi o di *scoring*, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

QUANDO LA DPIA NON E' OBBLIGATORIA?

Secondo le Linee guida del Gruppo Art. 29, la DPIA **NON è necessaria** per i trattamenti che:
- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento. Per un quadro completo: www.garanteprivacy.it/regolamentoue