Linee di indirizzo
in materia di gestione
della valutazione d’impatto
sulla protezione di dati personali

L'Istituzione scolastica
nella persona del Dirigente scolastico

Visti:
- 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 e che abroga la direttiva 95/46/CE (Regolamento Generale sulla protezione dei dati)";
- D.Lgs. n. 196/03 Codice in materia di protezione dei dati personali e s.m.i.
- Li lenea guida della materia del Ministro dell'istruzione;
- il decreto legislativo n° 51 del 18 maggio 2018 recante "Attuazione della direttiva (UE) 2016/680 del
Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché' alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio. Europeo"
- In particolare l'art. 35 del Regolamento europeo rubricato "Valutazione d'impatto sui dati personali" e art. 36 rubricato "Consultazione preventiva" del Regolamento europeo;
- Il Gruppo di Lavoro art. 29, il WP29, del 4 aprile 2017;
- Provvedimento del Garante n° 467 del 11 ottobre 2018 e relativo allegato;
- Sentito il parere favorevole espresso dal Responsabile della protezione dei dati

Emana

le seguenti linee di indirizzo in materia di gestione
della valutazione d'impatto sulla protezione di dati personali

Art. 1
Precisazione sulle premesse

Le premesse che precedono si intendono tutte parte integranti del presente Regolamento.

Art. 2
Oggetto delle linee di indirizzo

La valutazione d'impatto è una procedura prevista dall'art. 35 del Regolamento europeo che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntarne misure idonee ad affrontarli.

Una valutazione d'impatto può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

Art. 3

Finalità della valutazione d'impatto

Le finalità che le presenti linee di indirizzo si prefiggono di evidenziare sono sostanzialmente due:

1. il titolare dei dati è tenuto ad effettuare idonee procedure, quale una valutazione di impatto, per diminuire le probabilità che si verdichino eventi negativi che pregiudichino i diritti e le libertà delle persone coinvolte;

2. La valutazione d'impatto è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali e offre anche un aiuto al titolare che potrà attestare di avere adottato misure idonee a garantire il rispetto delle prescrizioni previste dal regolamento europeo.

Art. 4

Si riporta integralmente l'art. 35 del regolamento europeo
"*Valutazione di impatto sulla protezione dei dati*"

1.Quando un tipo di trattamento, allorché 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 previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

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; o

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

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.

5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

7.La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti. 10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento. 11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Art. 5

Si riporta integralmente l'art. 36 del regolamento europeo
"Consultazione preventiva"

Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

2. Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove

applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:

a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;

b) le finalità e i mezzi del trattamento previsto;

c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;

d) ove applicabile, i dati di contatto del titolare della protezione dei dati;

e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35;

f) ogni altra informazione richiesta dall'autorità di controllo.

4. Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento.

5. Nonostante il paragrafo 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.

Art. 6

Definizioni

Si riportano di seguito le definizioni più significative e più rispondenti all'argomento in esame.

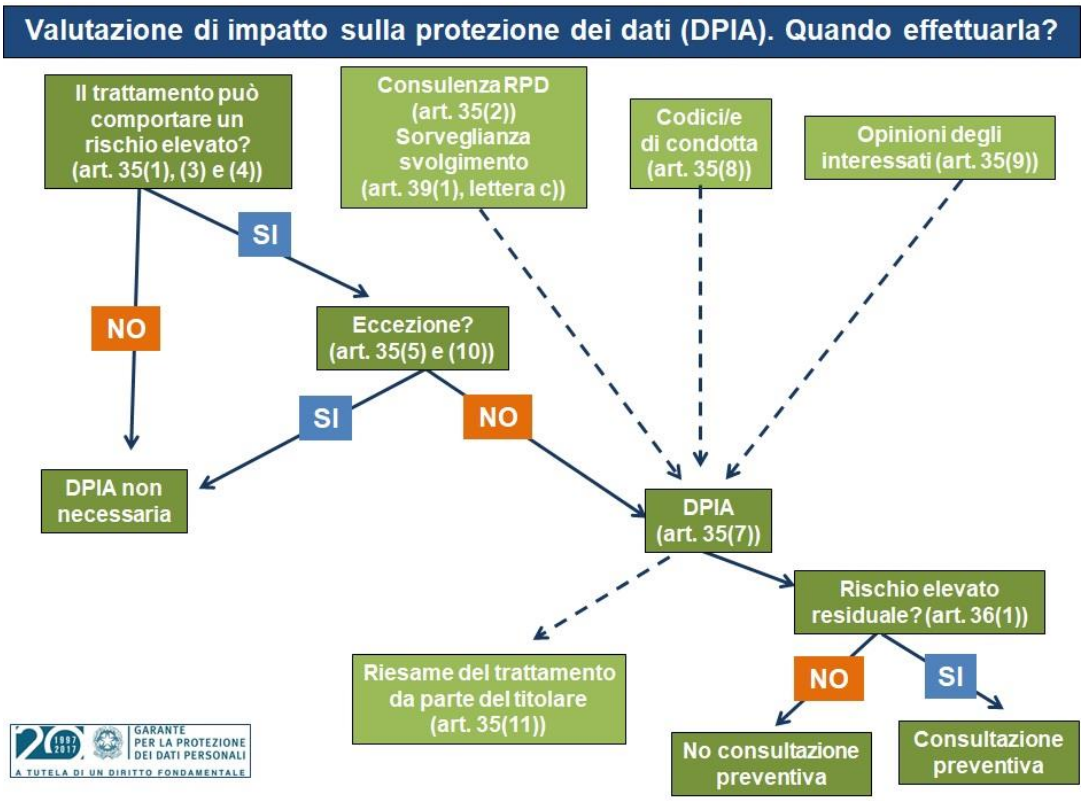
Rischio – Un rischio è uno scenario che descrive un evento e le sue conseguenze stimate in termini di gravità e probabilità. Il rischio da tenere presente non riguarda i dati personali, ma i diritti e le libertà delle persone fisiche, con riferimento al danno reputazionale, discriminazione, furto di identità, perdita finanziaria, perdita di controllo dei dati, altri svantaggi economici e impossibilità di esercitare diritti.

Gestione dei rischi – La gestione dei rischi può essere definita come l'insieme delle attività volte a indirizzare l'amministrazione verso una corretta gestione dei rischi.

Diritti e libertà delle persone fisiche - Il riferimento a "diritti e libertà" degli interessati previsto dall'articolo 35 del Regolamento riguarda principalmente i diritti alla protezione dei dati e alla vita privata, , ma include anche altri diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.

Art. 7

Schema utile per la gestione delle valutazioni di impatto
tratto da atti emanati dal Garante su WP29



Il presente schema, se coniugato nella lettura con gli articoli 35 e 36 del regolamento europeo, forniranno a questa istituzione scolastica ineludibili indicazioni su quale migliore strategia sarà da valutare per sviluppare una valutazione di impatto davanti a trattamenti che presentano rischi per i diritti e le libertà di interessati.

Art. 8

I soggetti coinvolti nelle valutazioni

Dirigente scolastico – Al dirigente spetta l'effettuazione della DPIA. La conduzione materiale può essere affidata ad un altro soggetto, interno o esterno alla scuola; tuttavia la responsabilità dell'adempimento ricade, comunque, sul titolare.

Tale assegnazione deve risultare comprovata da lettera che attribuisce al soggetto designato compiti e funzioni operando sotto l'autorità del dirigente scolastico.

Responsabile della protezione dei dati – Il titolare deve consultarsi con l'RPD. Tale consultazione e le conseguenti decisioni assunte dal dirigente devono essere documentate nell'ambito della DPIA.

Codice di condotta – Nel valutare l'impatto il titolare tiene in debito conto dei codici di condotta approvati ai sensi dell'art. 40 del regolamento europeo, se esistenti.

Opinioni degli interessati - Il titolare raccoglie le opinioni degli interessati o dei loro rappresentanti.

Il WP29 raccomanda:

- Per la raccolta delle opinioni in oggetto si possono individuare molteplici modalità, in rapporto al contesto: per esempio uno studio generico relativo a finalità e mezzi del trattamento; un quesito rivolto ai rappresentanti del personale; un questionario inviato ai genitori della scuola;
- Qualora la decisione assunta in ultima analisi dal titolare si discosti dall'opinione degli interessati, è bene che il titolare documenti le motivazioni che hanno condotto alla prosecuzione o meno del progetto;
- Il titolare dovrebbe documentare anche le motivazioni della mancata consultazione degli interessati qualora decida che quest'ultima non sia opportuna.

Art. 9

Metodologia suggerita per eseguire una valutazione di impatto

Il Regolamento europeo consente al titolare del trattamento di individuare la struttura e la forma della valutazione d'impatto più adatta alle attività della istituzione scolastica.

Il Regolamento, quindi, consente al Titolare di avvalersi di una qualsiasi metodologia di gestione e di valutazione del rischio che sia conforme ai principi del Regolamento stesso.

Le presenti linee di indirizzo sono utilizzabili con i dovuti adattamenti in funzione della particolare valutazione di impatto che la scuola intende realizzare.

La valutazione d'impatto sulla protezione dei dati ha la finalità, anche, di "*gestire i rischi*" per i diritti e le libertà delle persone fisiche:

1. **Definizione del contesto** – Si rappresenta il contesto, descrivendo in modo sistematico il trattamento: "*tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio*";
2. **Valutazione dei rischi** - "*valutare la particolare probabilità e gravità del rischio*" ", tenendo conto della finalità, liceità del trattamento, la presenza di dati adeguati, pertinenti e limitati, la previsione di un adeguato periodo di conservazione.
   Vanno valutate le misure per gestire i rischi e le misure per tutelare i diritti e le libertà degli interessati.
3. **Gestione dei rischi** – Vanno trattati i rischi per i diritti e le libertà degli interessati: "*attenuando tale rischio*" e "*assicurando la protezione dei dati personali*", e "*dimostrando la conformità al presente regolamento*";

Il Regolamento definisce gli elementi minimi e necessari per una corretta metodologia di valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 7, e consideranda 84 e 90):

1. *"una descrizione dei trattamenti previsti e delle finalità del trattamento";*
2. *"una valutazione della necessità e proporzionalità dei trattamenti";*
3. *"una valutazione dei rischi per i diritti e le libertà degli interessati";*
4. *"le misure previste per:*
   a. *"affrontare i rischi"*;

b. "*dimostrare la conformità al presente Regolamento*".

Su quanto esposto nell'ultimo paragrafo si invita il lettore a consultare l'**Allegato "A"**

Va evidenziato come il rischio deve essere valutato non solo in termini di sicurezza, ma anche tenendo conto del tipo di dati coinvolti e del tipo di trattamento nel suo complesso.

Va valutata la correttezza complessiva del trattamento avendo riguardo, ad esempio, alle modalità di raccolta del dato e alla qualità del dato [intesa quest'ultima, come rispondente ai requisiti di accuratezza, completezza, coerenza, attendibilità, attualità, precisione].

La raccolta e la conservazione di dati non pertinenti e non eccedenti per una specifica finalità, ad esempio, in violazione del principio di minimizzazione dei dati, pone in sé un rischio, il rischio di un utilizzo improprio dei dati non pertinenti eccedenti. In tal caso la misura adeguata a evitare il manifestarsi di questo rischio, consiste nell'astenersi dalla raccolta di dati non pertinenti e non eccedenti, con la cancellazione dei dati di queste tipologie se già detenuti.

Fondamentale è, quindi, analizzare attentamente tutti gli aspetti di ogni singolo trattamento, ivi inclusi le relative operazioni in esso contenute, sia nell'ambito dell'analisi complessiva sia nel quadro della valutazione dei rischi.

Qualora si preveda di effettuare un trattamento che possa presentare un rischio elevato, il Titolare del trattamento deve scegliere una metodologia per la valutazione d'impatto sulla protezione dei dati che soddisfi i criteri proposti dal Gruppo di lavoro ex articolo 29 (WP29 del 4 aprile 2017), che:

a. sia integrata nei processi in materia di progettazione, sviluppo, cambiamento, rischio e riesame operativo in conformità con i processi, il contesto e la cultura interni;
b. coinvolga le parti interessate appropriate e definisca chiaramente le loro responsabilità (responsabile della protezione dei dati, responsabile del trattamento, ecc.)

Il Titolare deve valutare il rischio attraverso la definizione del trattamento e del relativo contesto come indicato in precedenza.

Tenendo conto delle caratteristiche del trattamento può far seguire a tale tipo di valutazione anche la realizzazione della DPIA avvalendosi:

1. del software di ausilio messo a disposizione dall'Autorità francese per la protezione dei dati.
   Il software è gratuito e liberamente scaricabile dal sito del Garante per la protezione dei dati personali (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8581268), oppure dal sito www.cnil.fr (https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil).
   Per approfondimenti, è disponibile anche un breve tutorial realizzato dal Garante per la protezione dei dati personali accessibile al link:
   https://www.garanteprivacy.it/regolamentoue/dpia/gestione-del-rischio;
2. di qualsiasi metodologia di gestione e valutazione del rischio che sia conforme ai principi del Regolamento.

Art. 10

In quali casi e quando la valutazione deve essere svolta

Per i dirigenti scolastici l'obbligo di effettuare una valutazione d'impatto va ricondotto all'obbligo generale di gestire adeguatamente i rischi presentati dal trattamento di dati personali.

Tali rischi vanno gestiti in base a quanto prevede l'articolo 25 coniugato con l'articolo 5 del Regolamento, integrando *by design* nel trattamento, necessarie garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati.

Fin dalla fase di progettazione di un trattamento deve essere analizzato il contesto, la finalità del trattamento, tenendo in debito conto gli aspetti organizzativi al fine di ridurre i rischi. Fondamentale è il rispetto anche dei principi di *privacy by default* valutando la qualità del dato, la portata del trattamento, il periodo di conservazione, accessibilità a un soggetto autorizzato e accesso graduale per esigenze motivate.

Come già precisato, il Regolamento non richiede una valutazione d'impatto per ciascun trattamento che presenta generici rischi per i diritti e le libertà delle persone fisiche.

La valutazione d'impatto sulla protezione dei dati **è <u>obbligatoria soltanto</u> qualora il trattamento "*possa presentare un <u>rischio elevato</u> per i diritti e le libertà delle persone fisiche*"**.

Pertanto, è opportuna una valutazione preventiva del trattamento e dei rischi ad esso connesso. Scelta e valutazione preventiva della necessità della valutazione di impatto che devono essere documentate per iscritto alla luce di quanto di seguito rappresentato.

Sebbene una valutazione d'impatto sulla protezione dei dati possa essere opportuna anche in altre circostanze, l'articolo 35, paragrafo 3, individua, in particolare, alcuni casi nei quali un trattamento *"possa presentare rischi elevati"* per i quali essa è richiesta:

1) 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;
2) 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;
3) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La valutazione d'impatto va effettuata <u>"prima del trattamento"</u> (articolo 35, paragrafi 1 e 10, considerando 90 e 93) in coerenza con i principi di *privacy- by design* e *by default* sopra citati (articolo 25 e considerando 78).

La valutazione d'impatto va avviata il prima possibile, fin dalla fase di progettazione del trattamento anche se alcune delle operazioni di trattamento non sono ancora note nello specifico.

Per quanto riguarda lo sviluppo di nuove applicazioni informatiche, il dirigente scolastico, al momento della richiesta, chiederà ad un espetto in materia di visualizzare nella piattaforma di Project and Portfolio

Management (**PPM**) un *alert* per la verifica della sussistenza dei criteri che rendono necessaria la valutazione di impatto.

In tali casi è necessario assicurarsi, prima della fase di approvazione della richiesta di intervento di sviluppo di software e di piattaforme, che vengano previste e rispettate le disposizioni definite dalla *policy* dell'istituzione scolastica in materia di sicurezza di sviluppo delle applicazioni e di trattamento dei dati personali e che queste siano adeguate ai rischi esistenti.

È fondamentale richiedere al Responsabile del trattamento di inserire sempre nella documentazione di intervento di sviluppo di software e di piattaforme un paragrafo dedicato alle misure di sicurezza che devono essere adottate., in quanto la valutazione di impatto deve essere considerata come un processo dinamico e aggiornato.

È opportuno anche prevedere un aggiornamento della valutazione di impatto nel corso dell'intero ciclo di vita del trattamento per assicurare che il livello di protezione dei dati sia garantito o per individuare soluzioni che ne ristabiliscono le conformità.

Tale aggiornamento potrebbe risultare necessario, ad esempio, nel caso in cui si adottino modifiche ad applicazioni/piattaforme. La valutazione di impatto deve essere, infatti, un processo dinamico e aggiornato.

I rischi devono essere valutati e gestiti correttamente, non *una tantum*, ma in modo continuativo, perché i rischi possono evolvere e mutare nel tempo.

Per quanto riguarda i trattamenti di dati personali collegati a procedure già in corso di attuazione, la valutazione d'impatto deve comunque essere effettuata senza ritardo evitando eventuali rinvii.

Una valutazione d'impatto sulla protezione dei dati riguarda solitamente una singola operazione di trattamento dei dati. Tuttavia, l'articolo 35, paragrafo 1, del Regolamento indica che una "singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi".

Il considerando 92 aggiunge che ci "*sono circostanze in cui può essere ragionevole ed economico effettuare una valutazione d'impatto sulla protezione dei dati che verta su un oggetto più ampio di un unico progetto, per esempio quando autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni o quando diversi titolari del trattamento progettano di introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata*".

L'articolo 35, paragrafo 1, del Regolamento indica che una "*singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*". Si potrebbe, quindi, effettuare un'unica valutazione d'impatto sulla protezione dei dati nel caso di più trattamenti simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi.

Si fa presente che, anche in assenza dell'apposita funzionalità e per trattamenti meramente cartacei o che non operano tramite applicativi, deve essere valutata sempre la necessità di procedere o meno alla valutazione di impatto e di essa va conservata documentazione cartacea, rappresentando sempre per iscritto la decisione adottata.

L'articolo 35, paragrafo 4 prevede che ogni autorità nazionale di controllo rediga e renda pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1.

In Italia, il Garante ha definito con il provvedimento 467/2018 l'elenco delle tipologie di trattamento che richiedono una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 4).

Esso è riportato integralmente in **Allegato "B"**

In questa sede ci si limita a riportare l'elenco dei criteri che individuano presenza di rischio elevato:

1) Trattamenti valutativi o di scoring (affidabilità, rendimento, situazione economica)
2) Decisioni automatizzate che producono significativi effetti giuridici o analoghi
3) Monitoraggio sistematico
4) Dati sensibili di natura estremamente personale (vita familiare, dati finanziari, ubicazione)
5) trattamenti di dati su larga scala (numero di interessati, volume, durata e ambito geografico)
6) Combinazione o raffronto di insiemi di dati (diverse finalità, titolari distinti)
7) Dati relativi a interessati vulnerabili (squilibrio di poteri tra titolare e interessato, ad es. minori o disabili)
8) Utilizzi innovativi o applicazioni di nuove tecnologie o organizzative
9) trattamenti che, di per sé, impediscono di esercitare un diritto o di avvalersi di un servizio o di un contratto

Nel caso di trattamento che soddisfi almeno **due dei suddetti criteri** è opportuno che il soggetto che il Titolare del trattamento valuti la necessità di sottoporre il trattamento a una valutazione d'impatto.

In generale, si ritiene che maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto, indipendentemente dalle misure che il titolare del trattamento ha previsto di adottare.

Tuttavia, il Titolare del trattamento può ritenere che un trattamento che soddisfi soltanto uno di questi criteri richieda comunque una valutazione d'impatto.

Si ricorda che per una maggiore comprensione, la lettura sia continuamente integrata con lo schema previsto dal Garante, consultabile all'art 7 di pag. 4 delle presenti linee di indirizzo.

Art. 11

Analisi dei rischi

L'analisi dei rischi è la fase più delicata ed importante per stabilire, oltre ogni ragionevole dubbio, se il trattamento *de quo* comporta un rischio elevato che può compromettere i diritti e le libertà dell'interessato.

Il Gruppo di Lavoro WP29, nell'intento di supportare anche i dirigenti scolastici nell'identificazione dei trattamenti da sottoporre a valutazione di impatto, ha individuato nove criteri, come indici sintomatici del "rischio elevato". Essi, in dettaglio, sono descritti qui di seguito:

L'analisi dei rischi poggia sulle seguenti quattro macroaree, descrivendo in ciascuna le possibili criticità:

A. Misure esistenti o pianificate

Crittografia: dati sono trattati tramite l'utilizzo di meccanismi di conservazione e comunicazione cifrati, ai fini di garantire la minimizzazione del rischio di acceso agli stessi.

Controllo degli accessi logici: l'accesso alle funzionalità del delle piattaforme utilizzate deve essere regolato da un sistema di attivazione di *account* con permessi specifici, protetti da password, attivabili e disattivabili dall'amministratore del software o da un suo delegato.

Archiviazione: tutta la documentazione relativa all'attività Istituzionale della scuola è regolata dalla normativa vigente in materia di archiviazione nella pubblica amministrazione, contenente indicazioni specifiche per la pubblica istruzione.

Minimizzazione dei dati: I dati vengono trattati e archiviati in forma minima, per quanto previsto dalla normativa vigente.

Lotta contro i malware: I sistemi scolastici sono protetti da malware con modalità di protezione sia hardware che software (firewall e antivirus). È inoltre opportuno fornire agli utilizzatori delle linee guida sull'utilizzo sicuro delle risorse elettroniche e digitali, che includano le istruzioni per una efficace lotta al malware.

Backup: I sistemi di didattica da remoto, e non soltanto questi, utilizzati per il trattamento devono essere provvisti di una modalità di backup. Sono eseguiti copie di riserva con periodicità costante di tutta l'attività degli uffici.

Manutenzione: Viene effettuata regolarmente una attività di manutenzione nei confronti dei sistemi hardware scolastici e degli uffici. Il responsabile del trattamento garantisce inoltre il corretto funzionamento del software cloud di didattica da remoto e degli uffici.

Contratto con i responsabili di trattamento: I responsabili del trattamento devono essere nominati tali tramite la stipula di contratti, ai sensi degli artt. 28 e 29 del Regolamento europeo.

Politica di tutela della *privacy*: la scuola ha messo in atto una serie di misure orientate all'adeguamento della stessa alla normativa vigente. I dipendenti sono stati nominati autorizzati al

trattamento ai sensi dell'Art. 2- quaterdecies del D.Lgs. 196/2003, per l'esercizio delle loro funzioni.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali: la scuola ha emesso un regolamento interno per la gestione dei *data breach*, al cui interno sono specificate le modalità di gestione di tali fenomeni.

Formazione degli autorizzati al trattamento: la scuola ha programmato attività di formazione e informazione per gli autorizzati al trattamento

B. Accesso illegittimo ai dati personali

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Diffusione di dati personali di minori – Diffusione di dati concernenti l'orientamento politico, filosofico, la razza ed etnia – La condizione sanitaria degli interessanti – Cyberbullismo-

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Pubblicazione su piattaforme social di dati personali - Scarsa sensibilità degli studenti alla *privacy* dei compagni - Episodi di Cyberbullismo - Negazione del diritto all'oblio.

Quali sono le fonti di rischio?

Un dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione - Un utente che voglia utilizzare le informazioni per mettere in atto eventi negativi.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Tutte le misure esistenti o pianificate già individuate.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Minima. [*occorre specificare e motivare la stima*]

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Minima. [*occorre specificare e motivare la stima*]

C. Modifiche indesiderate dei dati personali

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Potrebbe limitare le possibilità di intervento della scuola.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Accesso illecito ai dati e modifica degli stessi

Quali sono le fonti di rischio? Errore umano, Fonti umane interne, che intervengano nella modifica dei dati

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Tutte le misure esistenti o pianificate individuate.

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Limitata

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Trascurabile, Appare impossibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti, purché si proceda all'alienazione della disponibilità degli stessi agli uffici interessati, alla fine della fase di elaborazione concessa.

D. Perdita di dati personali

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Problematiche.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Distruzione dei server del servizio, Perdita dell'accesso ai documenti, errore umano.

Quali sono le fonti di rischio?

Fonti umane interne, Fonti umane esterne (incaricati del responsabile del trattamento o dei sub responsabili), Eventi naturali che possano influire sui dispositivi fisici di archiviazione.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Tutte le misure esistenti o pianificate individuate.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata. [*occorre specificare e motivare la stima*]

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile. [*occorre specificare e motivare la stima*]

Art. 12
Valutazione dei rischi

Si dà esecuzione all'art. 11 attribuendo a ciascun rischio un codice identificativo.

Si ricorda che il rischio è il prodotto della probabilità che l'accadimento si verifichi per la gravità del danno che questo può comportare sui diritti e le libertà degli interessati.

Il prodotto dei due fattori che, discrezionalmente sono attribuiti dal dirigente scolastico, porta alla valutazione del rischio.

Tabella che conduce alla valutazione del rischio

Codice Rischio	Descrizione rischio "A" Misure esistenti o pianificate	P	G	R
A1	Crittografia			
A2	Controllo degli accessi logici			
A3	Archiviazione			
A4	Minimizzazione dei dati			
A5	Lotta contro i malware			
A6	Backup			
A7	Manutenzione			
A8	Contratto con il responsabile del trattamento			
A9	Politica della tutela della *privacy*			
A10	Gestire gli incidenti di sicurezza e le violazioni dei dati personali			
Codice Rischio	**Descrizione rischio "B"** **Accesso illegittimo dei dati**	**P**	**G**	**R**
B1	Quali potrebbero essere i principali impatti sugli interessati?			
B2	Quali sono le principali minacce che concretizzano il rischio?			
B3	Quali sono le fonti di rischio?			
B4	Quali misure fra quelle note contribuiscono a mitigare il rischio?			
B5	Come stimereste la gravità del rischio alla luce degli impatti ……. ?			
B6	Come stimereste la probabilità del rischio, con riguardo ……. ?			

Codice Rischio	Descrizione rischio "C" Modifiche indesiderate dei dati	P	G	R
C1	Quali sarebbero i principali impatti sugli interessati se il rischio ……. ?			
C2	Quali sono le principali minacce che potrebbero consentire la ……?			
C3	Quali sono le fonti di rischio?			
C4	Quali misure, tra quelle individuate, contribuiscono a mitigare il rischio?			
C5	Come stimereste la gravità del rischio alla luce degli impatti e delle ……?			
C6	Come stimereste la probabilità del rischio con riguardo a minacce, ……?			

Codice Rischio	Descrizione rischio "D" Perdita di dati	P	G	R
D1	Quali potrebbero essere gli impatti principali sugli interessati se ……?			
D2	Quali sono le principali minacce che potrebbero consentire la ……?			
D3	Quali sono le fonti di rischio?			
D4	Quali misure, tra quelle individuate, contribuiscono a mitigare il rischio?			
D5	Come stimereste la gravità del rischio alla luce degli impatti potenziali…?			
D6	Come stimereste la probabilità del rischio con riguardo alle minacce …?			

La probabilità dell'accadimento di un rischio è la possibilità che l'evento/rischio identificato si manifesti in un dato orizzonte temporale. Questo aspetto rimane uno dei più complessi e controversi del processo di analisi del rischio. In assenza di informazioni quantitative precise, che possono provenire dall'analisi dello storico di esperienze simili pregresse o da studi e analisi specifiche dei fenomeni d'interesse, è possibile stabilire la probabilità di accadimento sulla base della sensibilità ed esperienza del personale riguardo a funzioni di loro competenza. Sarà poi possibile determinare e costruire una matrice dei rischi, simile a quella mostrata in figura che segue, ovvero una rappresentazione sintetica del posizionamento relativo dei singoli rischi rispetto al rischio accettabile e al rischio tollerato, consentendo ai vertici di identificare le priorità di azione e le possibili strategie di risposta al rischio.

La valutazione del rischio, data dal prodotto di probabilità di accadimento e gravità dei danni, genera tre livelli di rischio:

Rischio Basso B trascurabile – Non rilevante: il rischio rientra all'interno del rischio accettabile e di conseguenza non sono necessarie misure di controllo o strategie di mitigazione ulteriori;

Rischio Medio M non trascurabile – Monitorare: il rischio supera il primo livello ma rientra nel rischio tollerato. Questa tipologia di rischio solitamente viene sottoposta a costante monitoraggio/gestione da parte dei vertici;

Rischio Alto A elevato – Evitare/Ridurre: Il rischio supera i livelli precedenti. Necessita un'elevata attenzione da parte della direzione che deve quali strategie di trattamento applicare: riduzione/mitigazione del rischio, trasferimento del rischio o eliminazione della fonte di rischio.

P - Portabilità del danno

4	**4**	**8**	**12**	**16**
3	**3**	**6**	**9**	**12**
2	**2**	**4**	**6**	**8**
1	**1**	**2**	**3**	**4**
	1	**2**	**3**	**4**

D - Gravità del danno

Pertanto, considerando che è R = P x G, se è:

1) R < 4 (colore verde) il rischio è da considerare basso e quindi accettabile;
2) R > 4 ed anche R< 9 (colore giallo) il rischio è da considerare medio e quindi tollerabile, e comunque deve sottoposto a continui monitoraggi ed a interventi urgenti con misure correttive;
3) R > 9 (colore rosso) il rischio è da considerare **alto** e quindi **dannoso**, pertanto sono richiesti indispensabili interventi a carattere e**mergenzial**i.

Art. 13
Casi nei quali la valutazione di impatto non è obbligatoria

La valutazione d'impatto sulla protezione dei dati non è richiesta nei seguenti casi:

1. quando il trattamento non è tale da "***presentare un rischio elevato per i diritti e le libertà delle persone fisiche***" (articolo 35, paragrafo 1);
2. **quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto**. In tali casi, si possono utilizzare i risultati della valutazione d'impatto già effettuata per un trattamento analogo (articolo 35, paragrafo 11);
3. qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e), trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, che tale base giuridica disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto nel contesto dell'adozione

della base giuridica (articolo 35, paragrafo 10), a meno che uno Stato membro non abbia dichiarato che sia necessario comunque effettuare tale valutazione prima di procedere alle attività di trattamento;

4. qualora il trattamento sia incluso nell'elenco facoltativo (ancora non stabilito dal Garante per la protezione dei dati personali in Italia) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5).

Inoltre, non è necessario realizzare una valutazione d'impatto sulla protezione dei dati per casi (ad esempio operazioni di trattamento in un contesto specifico e per una finalità specifica) che sono già stati esaminati e studiati sotto il profilo dei rischi da altre amministrazioni o altri soggetti. Ciò può essere applicabile anche a trattamenti simili attuati da differenti titolari del trattamento di dati. In questi casi, è necessario condividere o rendere pubblicamente accessibile la valutazione d'impatto dei dati di riferimento, attuare le misure descritte nella stessa e fornire una giustificazione per la realizzazione di una singola valutazione d'impatto.

Infine, non è necessaria una valutazione d'impatto sulla protezione dei dati per i trattamenti che siano stati verificati da un'autorità di controllo, a norma dell'articolo 20 della direttiva 95/46/CE e che vengano eseguiti senza **alcuna variazione rispetto alla verifica precedente**. In effetti, "*[l]e decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate*" (considerando 171).

Diversamente, qualsiasi trattamento di dati le cui condizioni di attuazione (ambito di applicazione, finalità, dati personali raccolti, identità dei titolari del trattamento o dei destinatari, periodo di conservazione dei dati, misure tecniche e organizzative, ecc.) sono mutate rispetto alla prima verifica effettuata dall'autorità di controllo e che possono presentare un rischio elevato devono essere soggette a una valutazione d'impatto sulla protezione dei dati.

Art. 14
Consultazione preventiva

Laddove una valutazione d'impatto sulla protezione dei dati riveli la presenza di **rischi residui elevati**, il di Titolare del trattamento è tenuto a effettuare la consultazione preventiva del Garante in relazione a tale specifico trattamento (articolo 36, paragrafo 1).

Pertanto, ogniqualvolta il Titolare del trattamento **non è in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile (ossia i rischi residui restano comunque elevati) è necessario consultare il Garante.**

L'articolo 36, paragrafo 3, del Regolamento definisce quali siano le informazioni che il soggetto che esercita le funzioni di Titolare o il soggetto Designato deve necessariamente comunicare affinché si possa ottenere il parere del Garante.

Allegato "A"

Il Gruppo di Lavoro WP29 suggerisce diverse metodologie per effettuare una DPIA [es. ISO/IEC 29134 "*Privacy Impact Assesment-Methodology*; ISO 3100025, ed altri ancora], in conformità al regolamento europeo, ed elenca alcuni elementi comuni dei processi di gestione del rischio che devono essere considerati nella effettuazione della DPIA, proponendo i seguenti criteri che i titolari del trattamento devono adattare nell'ambito della DPIA che si vuole effettuare:

- La descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, art. 37 comma 7, lett. a) che prevede:

  - la descrizione della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento; - la registrazione di dati personali, dei destinatari e del periodo di conservazione dei dati personali,
  - la descrizione funzionale del trattamento;
  - l'individuazione delle risorse sulle quali si basano i dati personali (hardware, software, reti, persone,
    canali cartacei o di trasmissione cartacea)
  - considerazione del rispetto degli eventuali codici di condotta.

- La valutazione della necessità e proporzionalità dei trattamenti, art. 37 comma 7, lett. b) che prevede
  indicazioni ed esplicitazioni ai sensi di diversi articoli del regolamento europeo in ordine a:
  - finalità determinate, esplicite e legittime;
  - liceità del trattamento;
  - dati personali adeguati, pertinenti e limitati a quanto necessario;
  - limitazione della conservazione;
  - misure che contribuiscono ai diritti degli interessati;
  - informazioni fornite all'interessato;
  - diritto di accesso e portabilità dei dati;
  - diritto di rettifica e alla cancellazione;
  - diritto di opposizione e di limitazione di trattamento;
  - rapporti con i responsabili del trattamento;
  - garanzie riguardanti trattamenti internazionali;
  - consultazione preventiva.

- la valutazione dei rischi per i diritti e le libertà degli interessati, deve considerare:

  - la tipologia dei dati trattati, la loro appetibilità, nonché la loro pericolosità per la *privacy* dei soggetti

cui essi si riferiscono;

- i comportamenti degli operatori;
- gli strumenti utilizzati per il trattamento dei dati;
- gli eventi relativi al contesto;
- l'origine, la natura, la particolarità e la gravità dei rischi;
- le fonti di rischio;
- la stima della probabilità e della gravità;
- le minacce che potrebbero determinare l'accesso illegittimo, la modifica indesiderata e la scomparsa

dei dati;

- le aspettative degli interessati con particolare riguardo agli impatti potenziali per i diritti e le libertà

degli interessati stessi in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata

e la scomparsa dei dati.

❖ <u>le misure previste per affrontare i rischi e dimostrare la conformità al presente regolamento</u>

Allegato "B"

Il Gruppo di Lavoro WP29, nell'intento di supportare anche i dirigenti scolastici nell'identificazione dei trattamenti da sottoporre a valutazione di impatto, ha individuato nove criteri, come indici sintomatici del "rischio elevato". Essi sono di seguito riportati:

1. **valutazione o assegnazione di un punteggio**, trattamento valutativo o di *scoring* compresa la profilazione e le attività predittive, in particolare con riguardo a "*aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato*" (considerando 71 e 91);
2. **processo decisionale automatizzato,** trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "*hanno effetti giuridici*" o che "*incidono in modo analogo significativamente su dette persone fisiche*" (articolo 35, paragrafo 3, lettera a)). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti delle persone coinvolte. Il trattamento che non ha effetto o ha soltanto un effetto limitato sulle persone non risponde a questo criterio specifico;
3. **monitoraggio sistematico,** trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "*la sorveglianza sistematica su larga scala di una zona accessibile al pubblico*" (articolo 35, paragrafo 3, lettera c)). In questo tipo di monitoraggio i dati personali sono raccolti anche in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà oppure può essere impossibile per gli interessati evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);
4. **dati sensibili o dati aventi carattere altamente personale**: questo criterio include categorie particolari di dati personali così come definite all'articolo 9, nonché dati personali relativi a condanne penali o reati di cui all'articolo 10 in quanto esse possono aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati sensibili perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta), perché influenzano l'esercizio di un diritto fondamentale (come, ad esempio, i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione), perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi, ad esempio, a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi;
5. **trattamento di dati su larga scala:** Il Regolamento non definisce la nozione di "larga scala", tuttavia fornisce un orientamento in merito nel considerando 91. Ad ogni modo, si raccomanda di tenere conto, in particolare, dei fattori di seguito elencati al fine di stabilire se un trattamento sia effettuato su larga scala;

a) il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
b) il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
c) la durata, ovvero la persistenza, dell'attività di trattamento;
d) la portata geografica dell'attività di trattamento;

6. **creazione di corrispondenze o combinazione di insiemi di dati**, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato;
7. **dati relativi a interessati vulnerabili** (considerando 75): il trattamento di questo tipo di dati è un criterio collegato all'aumento dello squilibrio di potere tra gli interessati e il soggetto che esercita le funzioni di Titolare. In questi casi le persone possono non essere in grado di acconsentire, di opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori, i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e tutti i casi in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del Titolare del trattamento;
8. **uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative**, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc. Il Regolamento chiarisce (articolo 35, paragrafo 1 e considerando 89 e 91) che l'uso di una nuova tecnologia, definita "*in conformità con il grado di conoscenze tecnologiche raggiunto*" (considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il soggetto che esercita le funzioni di Titolare del trattamento a individuare e trattare tali rischi;
9. **quando il trattamento in sé "*impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto*"** (articolo 22 e considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto.