COMUNE DI SAN MICHELE DI GANZARIA
Città metropolitana di Catania

DELIBERAZIONE DELLA GIUNTA MUNICIPALE

N° 33 DEL 12/05/2023

OGGETTO:	REGOLAMENTO EUROPEO UE N. 2016/679 SULLA PROTEZIONE DEI DATI PERSONALI – PROCESSO DI GESTIONE DEI RISCHI DEL TRATTAMENTO – APPROVAZIONE DELLA METODOLOGIA DI VALUTAZIONE DEL RISCHIO E DEFINIZIONE DEI CRITERI PER LA CLASSIFICAZIONE DELLA PROBABILITA' E DEGLI INDICI DI GRAVITA' DELL'IMPATTO E DEI CRITERI PER VALUTARE L'EFFICACIA DEL PROCESSO DI TRATTAMENTO DEL RISCHIO.

L'anno duemilaventitre, il giorno dodici del mese di maggio alle ore 12.30 nella sala delle adunanze della Casa Comunale, si è riunita la Giunta Municipale, convocata nelle forme di legge.

Presiede la seduta il Dott. Danilo Parasole nella Sua qualità di Sindaco e sono rispettivamente presenti ed assenti i Signori:

Cognome e nome	Carica	P/A
PARASOLE DANILO	SINDACO	PRESENTE
SAITA LINO	ASSESSORE	PRESENTE
ANZALONE CONCETTA	ASSESSORE	ASSENTE
RUSCICA SALVATORE	ASSESSORE	ASSENTE
SCIBETTA ROCCO	ASSESSORE	PRESENTE
	TOTALE	

X Assiste il SEGRETARIO COMUNALE, Dott.ssa Giuseppina La Morella;
o Assiste il VICESEGRETARIO COMUNALE, Dott. Alberto Gagliano.

Il Presidente, constatato il numero legale degli intervenuti, dichiara aperta la riunione e li invita a deliberare sull'oggetto sopraindicato.

LA GIUNTA COMUNALE

Vista la proposta di deliberazione formulata dall'ufficio proponente ad oggetto: "REGOLAMENTO EUROPEO UE N. 2016/679 SULLA PROTEZIONE DEI DATI PERSONALI – PROCESSO DI GESTIONE DEI RISCHI DEL TRATTAMENTO – APPROVAZIONE DELLA METODOLOGIA DI VALUTAZIONE DEL RISCHIO E DEFINIZIONE DEI CRITERI PER LA CLASSIFICAZIONE DELLA PROBABILITA' E DEGLI INDICI DI GRAVITA' DELL'IMPATTO E DEI CRITERI PER VALUTARE L'EFFICACIA DEL PROCESSO DI TRATTAMENTO DEL RISCHIO."

Ritenutala meritevole di accoglimento;

Dato atto che la stessa risulta corredata dei prescritti pareri di legge;

Visto l'O.A.EE.LL. della Regione Siciliana ed il relativo regolamento di attuazione;

Con votazione unanime e favorevole, resa nelle forme di legge;

D E L I B E R A

Di approvare la proposta di deliberazione formulata dall'ufficio proponente ad oggetto: "REGOLAMENTO EUROPEO UE N. 2016/679 SULLA PROTEZIONE DEI DATI PERSONALI – PROCESSO DI GESTIONE DEI RISCHI DEL TRATTAMENTO – APPROVAZIONE DELLA METODOLOGIA DI VALUTAZIONE DEL RISCHIO E DEFINIZIONE DEI CRITERI PER LA CLASSIFICAZIONE DELLA PROBABILITA' E DEGLI INDICI DI GRAVITA' DELL'IMPATTO E DEI CRITERI PER VALUTARE L'EFFICACIA DEL PROCESSO DI TRATTAMENTO DEL RISCHIO ", allegata alla presente deliberazione per formarne parte integrale e sostanziale e che qui viene richiamata integralmente.

Successivamente,

LA GIUNTA

Ravvisata la necessità di dare immediata attuazione al presente provvedimento per le motivazioni espresse nella proposta come sopra approvata;

Ad unanimità di voti favorevoli espressi nelle forme di legge

D E L I B E R A

Dichiarare, ad ogni effetto di legge, la presente deliberazione immediatamente eseguibile.

Proposta di deliberazione per la Giunta Comunale

OGGETTO: REGOLAMENTO EUROPEO UE N. 2016/679 SULLA PROTEZIONE DEI DATI PERSONALI – PROCESSO DI GESTIONE DEI RISCHI DEL TRATTAMENTO – APPROVAZIONE DELLA METODOLOGIA DI VALUTAZIONE DEL RISCHIO E DEFINIZIONE DEI CRITERI PER LA CLASSIFICAZIONE DELLA PROBABILITA' E DEGLI INDICI DI GRAVITA' DELL'IMPATTO E DEI CRITERI PER VALUTARE L'EFFICACIA DEL PROCESSO DI TRATTAMENTO DEL RISCHIO.

Visti
- il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati - RGDP);
- il D.Lgs. 196 del 30 giugno 2003, recante il "Codice in materia di protezione dei dati personali", come modificato, da ultimo, dal D.Lgs. 10 agosto 2018, numero 101;
- il Regolamento Comunale per la Protezione dei Dati Personali in attuazione del Regolamento UE 2016/679 approvato dal C. C. con delibera n. 3 del 10.02.2021
- le procedure di gestione dei trattamenti approvate dall'amministrazione con delibera G.M. n. 14 del 29.1.2019, in vigore dal 17.2.2019, emendate il 24.12.2019, con delibera G.M. n. 122 del 24.12.2019, in vigore dal 24.12.2019, emendate il 5.4.2022 con delibera G.M. n. 39 del 17.05.2022, in vigore dal 17.5.2022.

Premesso che

Il Reg. Ue n.679/2016 impone ai titolari un obbligo generale di "[tenere] conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche" posti da ciascun trattamento di dati personali, e di "mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento" (Art. 24, paragrafo 2).

Affinché i trattamenti siano conformi al Regolamento è necessario che vengano rispettati i principi del trattamento previsti dall'art. 5 del Regolamento. Ciò impone una preventiva "progettazione" delle operazioni effettuate come dispone l'art. 25 prevedendo che "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati (art. 25, paragrafo 1).

L'art. 32, inoltre, impone di assicurare la sicurezza del trattamento stabilendo che "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio".
In particolare, è necessario garantire

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

L'art. 35, inoltre, prevede che "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.

Il Titolare del trattamento è tenuto a dimostrare il rispetto di tali obblighi e il personale autorizzato al trattamento dei dati personali deve essere istruito e formato riguardo agli adempimenti da compiere in quanto l'Art. 35.4. stabilisce che "Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento....."

Anche il Responsabile della protezione dei dati personali (RPD), nell'eseguire i propri compiti […] considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. (Art. 39, paragrafo 2).

Pertanto, si rende necessario approvare una procedura che descriva la specifica metodologia, adottata dall'amministrazione, che le persone autorizzate al trattamento dovranno seguire ai fini dell'accertamento, della valutazione e del trattamento dei rischi, attraverso la definizione dei criteri per la classificazione della probabilità e degli indici di gravità dell'impatto e dei criteri per il processo di trattamento del rischio e il successivo monitoraggio delle azioni intraprese.

Il personale autorizzato al trattamento dei dati personali è tenuto ad aggiornare le proprie conoscenze e competenze e a rispettare la presente procedura che si aggiunge ed integra le "Istruzioni operative per il personale autorizzato al trattamento" già approvate dall'amministrazione.

Il processo di valutazione e gestione dei rischi del trattamento deve essere effettuato da tutto il personale autorizzato al trattamento addetto agli uffici che trattano dati personali, con la direzione e la responsabilità dei Funzionari/Elevata qualificazione o di un delegato, che sia stato previamente ed espressamente nominato quale responsabile del procedimento di valutazione e gestione dei rischi.

Ritenuto necessario approvare con il presente atto il documento denominato "Processo di gestione del rischio (risk management)" con i relativi allegati;
Visto lo Statuto Comunale;
Visto il D. Lgs. 18.8.2000, n. 267, art. 42, c. 2, lett. a) e ss.mm.ii.;
Visti i pareri favorevoli in ordine alla regolarità tecnica e contabile rilasciati dai Responsabili dei Servizi di cui all'art. 49 del D.Lgs. 18.08.2000, n. 267;
Visto I'O.R.EE.LL. della Regione Siciliana;

PROPONE

1. di assumere la premessa narrativa quale parte integrante e sostanziale della presente deliberazione;
2. di approvare il documento "Processo di gestione del rischio (risk management)" con i relativi allegati, allegato al presente provvedimento a farne parte integrante e sostanziale (Allegato 1);
3. di dare atto che le disposizioni operative sono assoggettate a revisione ogni qualvolta si renderà necessario, anche in funzione di eventuali criticità riscontrate in sede di applicazione;
4. di dare atto che la presente deliberazione non comporta un immediato e diretto impegno di spesa o una maggiore o minore entrata e, pertanto, non assume rilevanza contabile;

5. di disporre che tutti i soggetti autorizzati al trattamento dei dati personali vengano informati del presente provvedimento e osservino le prescrizioni presenti all'interno dello stesso;
6. di disporre che tutti gli adempimenti previsti nel processo di gestione del rischio vengano effettuati con la direzione e la responsabilità dei Funzionari/Elevata qualificazione o di un delegato, che sia stato previamente ed espressamente nominato quale responsabile del procedimento di valutazione e gestione dei rischi.
6. di disporre la pubblicazione del presente provvedimento sul sito istituzionale nella Sezione Privacy e di darne comunicazione al Responsabile della protezione dei dati personali (RPD) del Comune.
7. di dichiarare la presente deliberazione, con successiva votazione unanime, resa in forma palese, immediatamente eseguibile, ai sensi dell'articolo 134, comma 4) del D.Lgs. n. 267/2000 e ss.mm.ii.

Il Responsabile di Area Amministrativa
F.to Dott. Alberto Gagliano

COMUNE DI SAN MICHELE DI GANZARIA
Città metropolitana di Catania

PROPOSTA DI DELIBERAZIONE

DEL RESPONSABILE DELL'AREA AMMINISTRATIVA

OGGETTO: REGOLAMENTO EUROPEO UE N. 2016/679 SULLA PROTEZIONE DEI DATI PERSONALI – PROCESSO DI GESTIONE DEI RISCHI DEL TRATTAMENTO – APPROVAZIONE DELLA METODOLOGIA DI VALUTAZIONE DEL RISCHIO E DEFINIZIONE DEI CRITERI PER LA CLASSIFICAZIONE DELLA PROBABILITA' E DEGLI INDICI DI GRAVITA' DELL'IMPATTO E DEI CRITERI PER VALUTARE L'EFFICACIA DEL PROCESSO DI TRATTAMENTO DEL RISCHIO.

Ai sensi dell'art. 53 della legge 8 giugno 1990, n. 142, (come recepito con l'art. 1, comma 1, lettera f) della legge regionale 11 dicembre 1991, n. 48) e successivamente modificato dall'art. 12 della L.R. n. 30 del 23.12.2000, sulla proposta di deliberazione i sottoscritti esprimono parere di cui al seguente prospetto:

PARERE DEL SERVIZIO INTERESSATO:

Per quanto attiene la Regolarità tecnica si esprime parere Favorevole

San Michele di Ganzaria, lì 09/05/2023

IL RESPONSABILE
F.to Dott. Alberto Gagliano

PARERE DEL SERVIZIO INTERESSATO:

Per quanto attiene la Regolarità contabile si esprime parere Favorevole
Non investe il bilancio

San Michele di Ganzaria, lì 09/05/2023

IL RESPONSABILE
F.to Dott. Carmelo Brunello

La presente approvata e sottoscritta

IL SINDACO
F.to Dott. Danilo Parasole

L'ASSESSORE ANZIANO
F.to Lino Saita

IL SEGRETARIO COMUNALE
F.to Dott.ssa Giuseppina La Morella

Per copia conforme all'originale
San Michele di Ganzaria, lì _____

IL SEGRETARIO GENERALE

Il sottoscritto SEGRETARIO COMUNALE, visti gli atti d'Ufficio,

ATTESTA

Che la presente deliberazione è divenuta esecutiva il 12/05/2023

Perché dichiarata immediatamente esecutiva (art. 12, comma 2 L.R.44/91)

Dalla Residenza Municipale, lì 12/05/2023

IL SEGRETARIO COMUNALE

F.to Dott.ssa Giuseppina La Morella

Che la presente deliberazione è stata pubblicata per rimanervi 15 giorni consecutivi

Dal al

nel sito informatico di questo Comune (art. 32, comma 1, della legge 18 giugno 2009, n. 69 e s.m.i; Albo on line);

Dalla Residenza Municipale, lì

IL SEGRETARIO COMUNALE

Processo di gestione del rischio

(risk management)

****

metodologia di valutazione del rischio *del trattamento*
definizione dei ***criteri per la classificazione*** *della probabilità e degli indici di gravità dell'impatto e dei* ***criteri per il processo di trattamento del rischio***

***

adottato dal Comune di San Michele di Ganzaria con delibera G.C. n. 33 del 12/05/2023

INDICE

O.	Tool per testare e valutare l'efficacia della procedura prevista per stabilire se sussiste l'obbligo di effettuare la DPIA	
P.	Check list per individuare i trattamenti con obbligo di DPIA	

Premessa

Il Reg. Ue n.679/2016 impone ai *titolari* un obbligo generale di *"[tenere] conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento nonché* ***dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche***" posti da ciascun trattamento di dati personali, e di "*mettere in atto* ***misure tecniche e organizzative adeguate*** *per garantire, ed essere in grado di* ***dimostrare, che il trattamento è effettuato conformemente*** *al presente Regolamento*" (Art. 24, paragrafo 2).

Affinchè i trattamenti siano ***conformi*** al Regolamento è necessario che vengano rispettati i **principi del trattamento** previsti dall'art. 5 del Regolamento. Ciò impone una preventiva "progettazione" delle operazioni effettuate come dispone l'art. 25 prevedendo che "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento,* ***sia al momento di determinare i mezzi*** *del trattamento* ***sia all'atto del trattamento stesso*** *il titolare del trattamento* ***mette in atto misure tecniche e organizzative adeguate****, quali la pseudonimizzazione,* ***volte ad attuare in modo efficace i principi di protezione dei dati,*** *quali la minimizzazione, e a* ***integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati*** (Art. 25, paragrafo 1).

L'art. 32, inoltre, impone di assicurare la **sicurezza del trattamento** stabilendo che "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del* ***rischio*** *di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento* ***mettono in atto misure tecniche e organizzative adeguate*** *per* ***garantire un livello di sicurezza adeguato al rischio".***

In particolare, è necessario garantire

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

L'art. 35, inoltre, prevede che "*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.*

Il Titolare del trattamento è tenuto a **dimostrare** il rispetto di tali obblighi e il personale autorizzato al trattamento dei dati personali deve essere istruito e formato riguardo agli adempimenti da compiere in quanto l'Art. 35.4. stabilisce che "*Il titolare del trattamento e il*

*responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è **istruito** in tal senso dal titolare del trattamento....."*

Anche il RPD, nell'eseguire i propri compiti […] *considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo*. (Art. 39, paragrafo 2).

Pertanto, il presente documento descrive la specifica **metodologia**, adottata dall'amministrazione, che le persone autorizzate al trattamento dovranno seguire ai fini de**ll'accertamento, della valutazione e del trattamento dei rischi**, attraverso la definizione dei **criteri per la classificazione** della probabilità e degli indici di gravità dell'impatto e dei **criteri per il processo di trattamento del rischio** e il successivo monitoraggio delle azioni intraprese.

Il personale autorizzato al trattamento dei dati personali è tenuto ad aggiornare le proprie conoscenze e competenze e a rispettare la presente procedura che si aggiunge ed integra le "**Istruzioni operative per il personale autorizzato al trattamento**" già approvate dall'amministrazione.

Il concetto di **rischio** del trattamento dei dati personali ha una valenza molto ampia.

I rischi oggetto di valutazione non si limitano ai **rischi per la sicurezza** intesa in senso stretto – cioè alla probabilità e all'impatto di una violazione dei dati – ma comprendono anche i **rischi per i diritti e le libertà degli interessati** (e di altre persone fisiche) posti dal trattamento.

Si tratta, infatti, non soltanto dei rischi per i diritti alla riservatezza e alla vita privata e per gli specifici diritti riconosciuti agli interessati, ma anche, a seconda dei casi, dei rischi per i diritti alla **libertà di espressione**, alla **libertà di circolazione**, alla **non-discriminazione**, alla **libertà dagli autoritarismi**, al **diritto di vivere in una società democratica senza indebite attività di sorveglianza** svolte dal proprio o da un altro Paese, e per il **diritto a un rimedio giurisdizionale effettivo**.

Se il trattamento non rispetta i principi del trattamento previsti dal GDPR ciò pone di per sé un "rischio": **rischio di non conformità**

Alcuni trattamenti presentano **rischi intrinseci** che possono manifestarsi in assenza di violazioni dei dati: essi derivano dalle caratteristiche intrinsecamente pericolose dei trattamenti in quanto tali, anche ove svolti in modo conforme alle rispettive disposizioni e senza che si verifichi alcuna violazione dei dati ai sensi del RGPD, come prevede l'Art. 35.3 per i trattamenti che comportano

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

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

In tutti questi casi, e proprio per il fatto che trattamenti di questo tipo comportano rischi intrinsecamente elevati per i diritti e le libertà delle persone, è necessario condurre una **Valutazione di impatto sulla protezione dei dati** (DPIA) e, in determinate circostanze, consultare la o le autorità di controllo competenti.

Tutto questo comporta la necessità di analizzare attentamente **tutti gli aspetti di ogni singolo trattamento o funzionalità di protezione dati** – sia nell'ambito dell'analisi complessiva effettuata in sede di riesame delle attività di trattamento, sia nel quadro della valutazione dei rischi.

Il processo di valutazione e gestione dei rischi del trattamento deve essere effettuato da tutto il personale autorizzato al trattamento addetto agli uffici che trattano dati personali, con la direzione e la responsabilità dei Funzionari/Elevata qualificazione o di un delegato, che sia stato previamente ed espressamente **nominato quale responsabile del procedimento di valutazione e gestione dei rischi**.

Il processo si articola nelle fasi di seguito descritte.

*****

1. Definizione e contesto delle operazioni di trattamento da sottoporre a valutazione

L'accertamento dei rischi deve essere svolto, periodicamente, per ogni trattamento effettuato dall'organizzazione tenendo conto della definizione **dell'inventario delle attività** di trattamento e del **Registro di tali attività di trattamento**, in modo particolare, dell'analisi delle attività stesse che è stata effettuata dall'amministrazione nei precedenti Piani di adeguamento e dal RPD.

La persona nominata responsabile del procedimento di valutazione e gestione dei rischi dovrà annotare la data in cui si effettua la valutazione e il cognome e nome dell'incaricato che la effettua.

Il primo passo da compiere consiste nel definire le operazioni di trattamento svolte e il contesto, alla luce delle risultanze del **Registro dei trattamenti**, **dell'organigramma**, della mappatura del **sistema informatico,** degli **applicativi e delle piattaforme utilizzate,** riportando le informazioni rilevanti come di seguito indicato:

Data della Valutazione	Incaricato che effettua la Valutazione	Definizione e contesto delle operazioni di trattamento										
		codice ID tratt.	Denominazione	Finalità	Autorizzati che effettuano il trattamento	Dati trattati	Catgeorie di interessati	Operazioni eseguite	Destinatari	Mezzi di elaborazione Dispositivi	Elaboratore utilizzato (*Archiviazione interna/esterna; Responsabile*)

La compilazione di tale scheda può essere effettuata utilizzando il tool in Excel denominato "***Tool in Excel per la Valutazione e il trattamento del rischio***" (Allegato B)

Tale fase, che è propedeutica alle operazioni da compiere nelle fasi successive, deve condurre all'individuazione di tutti gli aspetti che assumono rilevanza ai fini dell'individuazione delle minacce e dei fattori di rischio.

Particolare attenzione dovrà essere data alle **categorie di dati** che sono oggetto del trattamento tenendo in considerazione la diversa delicatezza dei dati trattati come indicata nella seguente scheda:

Dati Comuni	Anagrafici Recapiti e dati di contatto	Moderato
	Foto Video	Più elevato
Dati relativi ai lavoratori	Retribuzione Giudizi di idoneità a mansioni specifiche Esposizione a particolari rischi	
Dati Particolari	Origine razziale o etnica Opinioni politiche o filosofiche Appartenenza sindacale Convinzioni religiose Stato di salute Sorveglianza sanitaria Dati diagnostici	Molto elevato
Dati giudiziari	Provvedimenti giudiziari Sentenze di condanna	
Dati genetici	DNA	
Dati biometrici	Firma grafometrica Impronte digitali	

- Analogamente, dovranno essere evidenziati
  - le singole **operazioni di trattamento** effettuate, prestando particolare attenzione ai casi di diffusione e comunicazione di dati;
  - i diversi **dispositivi di elaborazione** dei dati utilizzati, focalizzando l'attenzione sulla sicurezza informatica dei sistemi
  - le **piattaforme** utilizzate, analizzando i protocolli di trasmissione utilizzati
  - le diverse **categorie di interessati** i cui dati vengono trattati tenendo conto che il livello di esposizione al rischio aumenta qualora si trattino i dati relativi ad interessati vulnerabili che si trovano in una situazione di squilibrio di potere rispetto al titolare del trattamento, come ad esempio:
    Persone diversamente abili
    Minori

Dipendenti
infermi di mente
richiedenti asilo
anziani
pazienti, ecc.

2. Valutazione circa la conformità (compliance) del trattamento al GDPR e alla normativa di settore

Un trattamento dei dati personali che non rispetti tutti i principi del trattamento previsti dall'art. 5 del GDPR comporta di per sé dei rischi per gli interessati in quanto tutti i principi sono posti proprio a presidio dei diritti e delle libertà delle persone i cui dati vengono trattati.

Per esempio, se si è rilevato che uno specifico trattamento, per quanto lecito, nel senso di fondato su un'idonea base giuridica e finalizzato a un interesse legittimo, comporta la raccolta e la conservazione di dati non pertinenti ed eccedenti per la specifica finalità, quindi in violazione del principio di "*minimizzazione dei dati*", si può affermare che ciò ponga di per sé un "rischio" – ossia, il rischio di un utilizzo improprio dei dati non pertinenti ed eccedenti. In tal caso, la misura adeguata per evitare il manifestarsi di questo rischio sarebbe l'astenersi dalla raccolta dei dati non pertinenti ed eccedenti, con la cancellazione dei dati di queste tipologie già detenuti. Un altro esempio potrebbe essere l'impiego di dati ancora caratterizzabili come identificativi in un trattamento statistico che possa essere svolto attraverso dati pseudonimizzati o anonimizzati; in tal caso, la misura adeguata sarebbe quella di assicurarsi che i dati utilizzati siano pseudonimizzati correttamente o, meglio ancora, anonimizzati.

Preliminarmente, la persona incaricata di effettuare la valutazione dovrà annotare i dati del Titolare, la data in cui si procede alla valutazione e cognome e nome della persona incaricata di effettuare la valutazione come segue:

Titolare del trattamento	
Data della valutazione	
Incaricato che effettua la valutazione	

La **data della valutazione** deve essere sempre indicata perché da essa decorrono i termini massimi entro i quali è necessario applicare le misure necessarie a rimuovere la difformità.

La valutazione di conformità deve essere effettuata dopo aver individuato il trattamento e raccolto le **informazioni di contesto** necessarie per la valutazione, come indicato nella tabella seguente:

Ambito	Individuazione del trattamento e del contesto	Informazioni sul trattamento rilevanti per la valutazione
Informazioni sul trattamento	**ID del trattamento** *(indicare il codice numerico che identifica il trattamento)*	

	Denominazione del trattamento *(indicare la denominazione data al trattamento)*	
	Altre entità coinvolte *(Contitolari; Responsabili; altri titolari autonomi)*	
	Autorizzati *(indicare gli autorizzati che effettuano il trattamento)*	
	Categorie di dati trattati *(verificare se vengono trattate Categorie particolari di dati o dati concernenti condanne penali, reati e misure di sicurezza o altri dati sensibili e darne evidenza a lato)*	
	FINALITA' del trattamento *(Indicare le finalità del trattamento)*	
	Disciplina di settore applicabile al trattamento *(Indicare la fonte normativa: Legge; D.L.; D.Lgs.; L. R.; ecc.)*	

Sulla base degli elementi raccolti e di eventuali altre informazioni rilevabili dal Registro dei trattamenti, si procederà a rispondere (SI/NO) ai seguenti 16 quesiti volti a verificare il rispetto dei principi del trattamento previsti dall'art. 5 del GDPR.

Se la risposta è NO significa che viene violato uno dei principi del trattamento per cui è necessario **adottare le misure necessarie** per ripristinare la conformità, stabilendo il termine per l'adeguamento e la persona incaricata di provvedere all'attuazione delle misure, come di seguito indicato:

Quesiti per la valutazione della conformità		*Rispondere SI /NO*	**Misure da applicare**	**Incaricato dell'attuazione**	**Termine per l'adeguamento**
1. Liceità	**1.1 Ricorre una delle condizioni ex artt. 6, 9 e 10 ?**				
	1.2 La base giuridica è appropriata e proporzionata ?				
	1.3 E' rispettata la disciplina di settore?				
	1.4 Se i dati sono Comunicati sussiste una base giuridica che consente la Comunicazione dei dati ?				
	1.5 Se i dati sono Diffusi sussiste una base giuridica che consente la Diffusione dei dati ?				
	1.6 I rapporti con i Contitolari e soggetti esterni sono definiti e regolati (dalla legge o ex art. 26 e 28) ?				
	1.7 E' stata fatta la DPIA nei casi in cui è obbligatoria ?				
2. Finalità	**2.1 - Le finalità sono state predeterminate ?**				
	2.2- I dati NON sono utilizzati per altre finalità secondarie ?				
3. Trasparenza	**3. -Viene resa l'informativa ?**				
4. Correttezza	**4. -C'è congruenza tra quanto prospettato all'interessato e il trattamento ?**				

5. Minimizzazione	5. - I dati sono adeguati, pertinenti e limitati a quanto necessario alle finalità ?				
6. Esattezza	6. -Sono state previste tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti o per integrare quelli incompleti rispetto alle finalità ?				
7. Conservazione	7. -I dati sono conservati in una forma che consenta l'identificazione per un arco di tempo non superiore al conseguimento delle finalità ?				
8. Integrità e Riservatezza	8. -Sono state adottate misure organizzative (Policy) adeguate per proteggere i dati da trattamenti non autorizzati o illeciti e dalla perdita, distruzione o dal danno accidentali ?				
	9. -Sono state adottate misure tecniche (Hardware - software - antivirus) adeguate per proteggere i dati da trattamenti non autorizzati o illeciti e dalla perdita, distruzione o dal danno accidentali ?				
	Somma esiti negativi				
	Valutazione della Conformità ai Principi del trattamento	CONFORME			
		NON CONFORME			

Si procede quindi a

Valutare il grado complessivo di conformità, sommando tutti i SI e dividendo per 16 (n. di quesiti) e poi dividendo per 100.

Valutare il grado complessivo di difformità sommando tutti i NO e dividendo per 16 (n. di quesiti) e poi dividendo per 100.

Grado complessivo di conformità	0%
Grado complessivo di difformità	0%

Si tratta solo di un indicatore utile per capire qual è la situazione complessiva di conformità di ogni trattamento, ma va sottolineato, comunque, che è sufficiente un solo NO perché il trattamento sia valutato come "NON CONFORME" con conseguente obbligo di intervenire adottando le misure correttive appropriate al singolo caso.

Per agevolare la valutazione è stato predisposto un tool in un **file Excel denominato "tool_valutazione della conformità" (Allegato E)** nel quale vanno inserite le informazioni sul trattamento per poi rispondere ai quesiti con SI/NO. Al termine della valutazione è necessario conservare il report della valutazione in formato PDF/A.

Il tool propone alcune **misure correttive** e un **termine massimo** entro il quale devono essere messe in atto che varia da 3 a 60 giorni, a seconda della complessità degli adempimenti da

compiere. Tali indicazioni fornite dal tool non sono vincolanti e possono essere variate da chi effettua la valutazione in relazione al singolo caso. Si raccomanda, comunque, di intervenire tempestivamente al fine di rimuovere la causa della difformità.

In alternativa, è possibile compilare la **scheda di valutazione di conformità in word (Allegato D)**, convertirla in formato PDF/A e conservare il file per eventuali successive verifiche.

Il file deve essere firmato digitalmente e conservato.

In alternativa, la scheda di valutazione dovrà essere stampata e firmata dalla persona che effettua la valutazione e dalla persona incaricata di attuare le misure correttive, se diversa dall'autore della valutazione.

Qualora il RPD ne faccia richiesta le schede di valutazione devono essergli trasmesse tempestivamente.

La procedura di valutazione della conformità **deve essere effettuata periodicamente**, almeno una volta all'anno entro il 30 novembre di ogni anno e, in ogni caso, anche prima

- qualora si verifichi un mutamento dei fattori di contesto che caratterizzano il trattamento;
- in caso di richiesta del RPD.

Per verificare la **conformità dell'informativa è disponibile una Check list in Excel** (allegato K).

3. Valutazione circa l'obbligo o meno di effettuare la Valutazione d'impatto (DPIA)

Dopo aver effettuato la valutazione di conformità è necessario verificare, in via prioritaria, quali sono i trattamenti che presentano un **rischio elevato** per i diritti e le libertà delle persone fisiche per i quali è obbligatorio effettuare la Valutazione d'impatto (DPIA).

L'individuazione di tali trattamenti deve essere effettuata sulla base dei **seguenti criteri**:

a) trattamenti, indicati nell'art. 35.3 del Reg. UE 2016 n.679, che comportano:

   i. 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**;

   ii. 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

   iii. la **sorveglianza sistematica su larga scala di una zona accessibile al pubblico**.

b) trattamenti per i quali ricorrono almeno 2 dei 9 criteri previsti dalle Linee guida del Gruppo art. 29 del 4/10/2017 WP 248)

c) trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto in base al Provvedimento del Garante N. 467 DELL'11 ottobre 2018 [doc. web n. 9058979]

d) trattamenti per i quali la **valutazione dei rischi**, di seguito descritta al punto 5), ha evidenziato che il **RISCHIO INERENTE E' ALTO;**

Occorre tener presente che tutti questi rischi possono presentarsi in forma associata con effetti di **reciproco potenziamento**, come nel caso del ricorso alle tecniche di riconoscimento del volto per il monitoraggio di luoghi pubblici da parte delle forze di polizia, allo scopo di "identificare" potenziali delinquenti e prevedere comportamenti scorretti.

Si osservi che i rischi suddetti possono manifestarsi anche in assenza di violazioni dei dati: essi derivano dalle caratteristiche intrinsecamente pericolose dei trattamenti in quanto tali, anche ove svolti in modo conforme alle rispettive disposizioni e senza che si verifichi alcuna violazione dei dati ai sensi del RGPD.

Si tenga presente che spesso il legislatore nazionale ha già tentato una prima gestione dei rischi particolari che si ritengono associati a determinate attività di trattamento, attraverso le norme nazionali. Le **previsioni di legge** devono essere tenute presenti nella valutazione del rischio, per cui non si potrà mai giungere alla conclusione che un determinato rischio sia accettabile pur in violazione delle specifiche disposizioni o limitazioni previste per legge.

Le Autorità nazionali di protezione dati, inoltre, stanno adottando elenchi di trattamenti soggetti al requisito della DPIA sul proprio territorio, e possono adottare elenchi di trattamenti che non sono soggetti a tale requisito; gli elenchi in questione devono essere sottoposti al Comitato europeo della protezione dei dati e possono essere sindacati da altre Autorità attraverso il cosiddetto "meccanismo di coerenza" (Art. 35, paragrafi 4-6).

Per individuare i trattamenti per i quali è obbligatorio effettuare la DPIA occorre procedere, preliminarmente, all'adempimento già descritto al punto 1):

- definire le operazioni di trattamento svolte e il contesto, alla luce delle risultanze del **Registro dei trattamenti**, **dell'organigramma**, delle mappature del **sistema informatico** e degli **applicativi e delle piattaforme utilizzate,** riportando le informazioni rilevanti secondo la seguente tabella:

Data della Valutazione	Incaricato che effettua la Valutazione	Definizione e contesto delle operazioni di trattamento									
		codice ID tratt.	Denominazione	Finalità	Autorizzati che effettuano il trattamento	Dati trattati	Categorie di interessati	Operazioni eseguite	Destinatari	Mezzi di elaborazione Dispositivi	Elaboratore utilizzato (*Archiviazione interna/esterna; Responsabile*)

La compilazione di tale scheda può essere effettuata utilizzando il tool in Excel denominato "***Tool in Excel per la Valutazione e il trattamento del rischio***" (Allegato B)

- Alla luce delle informazioni così raccolte, occorre effettuare le verifiche indicate negli step seguenti rispondendo ai seguenti quesiti utilizzando la **check list contenuta nell'allegato P**:

1° STEP: Verifica sulla sussistenza dei casi previsti dall'art. 35.3

1) Quesiti **per verificare la sussistenza o meno dei casi previsti dall'art. 35 per i quali la Valutazione d'impatto è obbligatoria**	SI/NO
1. Il trattamento comporta 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. E' un 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 ?** ***"Larga scala" è s**i considera il **numero di interessati,** il **volume,** la **durata e l'ambito geografico***	
3. Il trattamento comporta la **sorveglianza sistematica** su **larga scala** di una **zona accessibile al pubblico ?**	

- Se la risposta è SI anche per una sola delle suddette domande, è necessario effettuare la DPIA.

- Se la risposta a tutte e tre le domande è NO occorre procedere agli step successivi.

2° STEP: Verifica sulla base dei 9 criteri previsti dal Gruppo art. 29 WP 248

Le Linee-guida sulla DPIA, riviste e adottate dal WP29 e quindi fatte proprie dal Comitato, individuano **nove criteri** di cui tener conto per stabilire se un trattamento può comportare un "rischio elevato".

2) Quesiti **Per verificare i Nove criteri previsti dalle Linee guida del Gruppo art. 29 del 4/10/2017 WP 248** - *il **rischio è elevato** se ricorrono **2/9 criteri***	SI/NO
2.1 Il trattamento comporta una **valutazione o assegnazione di un punteggio,** inclusiva di **profilazione** e **previsione**, in particolare in considerazione di "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" **?** *Es.: **profilazione** applicata al personale con riassegnazione automatica delle pratiche*	
2.2 Il trattamento consiste in un **processo decisionale automatizzato c**he ha effetto giuridico o **incide** in modo analogo significativamente: 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" **?** *Es.: trattamento che può portare **all'esclusione** o alla **discriminazione** delle persone – **contrasto dell'evasione** fiscale – contrasto alle **frodi nel welfare – identificazione di minori a rischio***	

2.3 Il trattamento comporta il 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"?

Es*.: **Videosorveglianza** occulta – Videosorveglianza intelligente associata a software di **riconoscimento facciale** – Trattamento di **metadati** (tempo, natura, durata di una transazione bancaria) per ricavarne stime di bilancio*

2.4 E' un trattamento di **dati sensibili o dati aventi carattere altamente personale?**

*Es.: **cartelle sanitarie di pazienti** o **richiedenti sussidi** e **assistenza** conservate dai **Servizi sociali** - Conservazione informazioni su **condanne penali e reati** – **accesso a mail personali dei lavoratori** – accesso a strumenti in contesti **BYOD** (bring your own device)- accesso **ai file di log** – esami sanitari e **verifiche del casellario giudiziale** precedenti l'assunzione – Indagini amministrative e **procedimenti disciplinari** –*

2.5 E' un trattamento di dati su larga scala ?

Si tiene conto dei seguenti fattori:

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;

*Es.: **scambi** di dati su larga scala t**ra titolari del settore pubblico** (ministeri, autorità regionali e locali) su **reti telematiche** – raccolta su larga scala di informazioni genealogiche su famiglie appartenenti a uno specifico gruppo religioso o bisognose –*

2.6 Il trattamento comporta la **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**?**

*Es.: **verifiche incrociate e non trasparenti delle registrazioni sugli accessi** del personale, degli accessi informatici, delle dichiarazioni rese ai fini della compensazione oraria, per individuare casi di assenteismo – **verifiche incrociate dell'Ufficio fiscale** che confronti le dichiarazioni dei redditi con gli atti di proprietà relativi a imbarcazioni di pregio **al fine di individuare potenziali evasori***

2.7 Il trattamento concerne dati relativi a **interessati vulnerabili ?**

Vi è uno **squilibrio di potere tra gli interessati e il titolare del trattamento?**
(Minori, dipendenti, infermi di mente, richiedenti asilo o anziani, pazienti, ecc.)

*Es.: utilizzo di **sistemi di videosorveglianza e geolocalizzazione che consentono la sorveglianza remota dei dipendenti** – trattamenti su larga scala dei **servizi sociali di dati sensibili di soggetti vulnerabili** – trattamenti su larga scala dell'**ufficio personale su dati sensibili dei dipendenti***

2.8 Viene fatto un **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. ?

*Es.: **Nuove tecnologie per tracciare tempi e presenze dei dipendenti** – **Screening di candidati all'impiego** attraverso o social media **– interconnessione dei veicoli***

2.9 E' un trattamento che in sé **"impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" ?** *Ad esempio i trattamenti che mirano a **consentire, modificare o rifiutare l'accesso degli interessati a un servizio** oppure la **stipula di un contratto**.* *Es.: **database negativi di esclusione rispetto a determinate prestazioni utilizzati dai servizi sociali***	

- In presenza di **almeno 2 criteri** che risultino positivi sussiste l'obbligo di effettuare la DPIA.

- In linea di principio, il Gruppo di lavoro ritiene che quanto maggiore è il numero dei criteri soddisfatti da un determinato trattamento, tanto maggiore è la probabilità che esso presenti un rischio elevato per i diritti e le libertà degli interessati e, quindi, che si renda necessaria una DPIA indipendentemente dalle misure che il titolare prevede di adottare.

- il titolare può condurre una DPIA anche se uno solo dei criteri in questione risulta soddisfatto – su base esclusivamente **discrezionale**.

- Se non ricorrono almeno 2 criteri e non si è deciso di effettuare comunque la DPIA, occorre procedere agli step successivi.

3° STEP: Verifica della sussistenza delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto in base al Provvedimento N. 467 DELL'11 ottobre 2018.

3) Quesiti **per la verifica della sussistenza delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto in base al Provvedimento N. 467 DELL'11 ottobre 2018 [doc. web n. 9058979]**	SI/NO
3.1 E' un trattamento valutativo **o di scoring** (affidabilità, rendimento, situazione economica) **su larga scala,** o un trattamento che comporta la **profilazione** degli interessati, o lo svolgimento di **attività predittive** effettuate anche on-line o attraverso app, relativi ad "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" **?**	
3.2 E' un trattamento **automatizzato** finalizzato ad assumere **decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente"** sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere ? *ad es. **screening dei clienti** di una banca attraverso l'utilizzo di dati registrati in una centrale rischi*	

3.3	E' un trattamento che prevede un **utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati,** compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti d servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudin d'uso e ai dati di visione per periodi prolungati? *Rientrano in tale previsione anche i trattamenti di **metadati** ad es. in ambito telecomunicazioni, banche, ecc. effettuat non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.*	
3.4	E' un trattamento su **larga scala di dati aventi carattere estremamente personale** : si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), **o che incidono sull'esercizio di un diritto fondamentale** (quali i dati sull'ubicazione , la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un **grave impatto sulla vita quotidiana** dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti) **?**	
3.5	E' un trattamento effettuato nell'ambito del **rapporto di lavoro mediante sistemi tecnologici** (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un **controllo a distanza dell'attività dei dipendenti ?** *si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8*	
3.6	E' un trattamento **non occasionale di dati relativi a soggetti vulnerabili** (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo) **?**	
3.7	E' un trattamento effettuato attraverso **l'uso di tecnologie innovative,** anche **con particolari misure di carattere organizzativo** (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) **e ricorre anche almeno un altro dei criteri individuati nel WP 248** (vedi punti da 11.1. a 11.9) ?	
3.8	E' un trattamento che comporta lo **scambio tra diversi titolari di dati su larga scala con modalità telematiche ?**	
3.9	E' un trattamento di dati personali **effettuato mediante interconnessione, combinazione o raffronto di informazioni,** compresi i trattamenti che prevedono l'incro cio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment) **?**	
3.10	**E**' un trattamento di **categorie particolari di dati ai sensi dell'art. 9** oppure di **dati relativi a condanne penali e a reati** di cui all'art. 10 **interconnessi con altri dati personali raccolti per finalità diverse ?**	
3.11	E' un trattamento **sistematico di dati biometrici,** tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attiv ità di trattamento ?	
3.12	E' un trattamento **sistematico di dati genetici,** tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attiv ità di trattamento?	

L'elenco non è esaustivo ed è stato adottato applicando il "meccanismo di coerenza", uno strumento volto ad assicurare un'applicazione coerente ed uniforme del Regolamento generale sulla protezione dei dati in tutta l'Unione Europea.

- Se la risposta è SI anche per una sola delle suddette domande, è necessario effettuare la DPIA.

- Se la risposta a tutte e tre le domande è NO occorre procedere agli step successivi.

4 Step: Verificare se sussistono casi nei quali, secondo le linee guida WP248, la Valutazione d'impatto non è necessaria

Qualora l'esito dei passaggi precedenti abbia condotto ad individuare l'obbligo di effettuare la DPIA, può essere effettuata la seguente ulteriore verifica al fine di accertare se sussitono i casi di esonero dall'obbligo previsti dalle linee guida citate.

4) Quesiti **per verificare se sussistono casi nei quali, secondo le linee guida WP248, la Valutazione d'impatto non è necessaria**	SI/NO
4.1 E' un trattamento che **non può comportare un rischio elevato** per i diritti e le libertà delle persone fisiche **?** **Se la risposta e SI, è necessario motivare e documentare la scelta**	
Motivazione:	
4.2 La natura, l'ambito, il contesto e le finalità del trattamento sono **molto simili a quelli del trattamento per cui è già stata condotta la Valutazione d'impatto ?** **Se la risposta e SI, è necessario indicare qual è il trattamento per il quale è già stata condotta la valutazione d'impatto. scelta**	
ID e denominazione del trattamento simile	
4.3 Il trattamento è stato sottoposto a **verifica da parte dell'autorità di controllo prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche ?**	
Indicare gli estremi della verifica	
4.4 E' un trattamento che trova la propria **base legale nel diritto dell'UE o di uno Stato membro** che disciplina lo specifico trattamento, ed è **già stata condotta una Valutazione d'impatto all'atto della sua definizione ?** Se la risposta e SI, è necessario **indicare qual è la base legale e qual è la valutazione d'impatto che è già stata condotta**	
Indicare - *la **base legale** che disciplina il trattamento e* - *la **data o gli estremi della valutazione** d'impatto*	

13.5 E' un trattamento compreso **nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla valutazione d'impatto ?** *Al momento tale elenco non è stato ancora emanato*	

La valutazione d'impatto non è obbligatoria nei casi nei quali, secondo le linee guida WP248, la Valutazione d'impatto è ritenuta non necessaria.

Se, nonostante l'esistenza di uno o più dei presupposti evidenziati dalle verifiche precedenti, NON si ritiene di effettuare la valutazione d'impatto, è necessario **motivare** e **documentare** la scelta allegando o annotando il parere del RPD e la data in cui è stato reso.

Se la necessità dalla valutazione d'impatto non emerge con chiarezza, in caso di dubbio, le linee guida del WP 248 raccomandano di farvi comunque ricorso.

L'esito della valutazione deve essere prontamente **comunicato al RPD** il quale può chiedere di fornire chiarimenti e di trasmettere la documentazione delle valutazioni effettuate

5 Step: Analisi del rischio inerente

Se all'esito delle valutazioni effettuate nelle fasi precedenti risulta che non è obbligatorio effettuare la DPIA, occorre comunque **procedere all'analisi del rischio inerente** - seguendo la metodologia indicata al successivo punto 5) – e se dopo tale valutazione il rischio risulta **ALTO** è necessario **– PRIMA di procedere al trattamento** - effettuare la DPIA.

Il risultato della valutazione deve essere prontamente **comunicato al RPD** il quale può chiedere di fornire chiarimenti e di trasmettere la documentazione delle valutazioni effettuate

4. Definizione delle priorità di analisi dei diversi trattamenti

Considerato che ogni ufficio effettua molteplici trattamenti, è opportuno che prima di procedere alle valutazioni descritte nei punti seguenti, venga effettuata, anche sulla scorta di quanto è emerso dalle valutazioni precedentemente indicate, un'attenta graduazione dei diversi trattamenti dando **priorità** a quelli che presentano caratteristiche tali da poter comportare un **rischio elevato**.

Si tenga presente che spesso è possibile conseguire uno scopo legittimo utilizzando strumenti diversi e meno invasivi, oppure ricorrendo a un minore volume di dati (e a dati meno sensibili), per cui è consigliabile apportare i necessari correttivi alle operazioni di trattamento in modo da ridurre in partenza il livello di impatto.

5. Analisi del rischio inerente

Se all'esito delle valutazioni effettuate nelle fasi precedenti risulta che non è obbligatorio effettuare la DPIA, occorre comunque **procedere all'analisi del rischio inerente,** - seguendo la metodologia di seguito indicata.

L'analisi dei rischi richiede la corretta identificazione delle minacce che possono aver successo sui dati coinvolti nel trattamento.

La valutazione dei rischi stabilisce il valore delle attività di informazione, identifica le minacce applicabili e le vulnerabilità che esistono (o possono esistere), identifica i controlli esistenti e il loro effetto sul rischio identificato, determina le potenziali conseguenze.

Si prenderanno in considerazione le classi di rischio in relazione all'effetto della minaccia sulle caratteristiche del dato personale.
Le minacce che possono insidiare le tre caratteristiche fondamentali dei dati personali sono: Riservatezza (R); Integrità (I); Disponibilità (D).

A tal fine, in via preliminare, come già descritto al punto 1), si procederà a

- definire le operazioni di trattamento svolte e il contesto, alla luce delle risultanze del **Registro dei trattamenti**, **dell'organigramma**, delle mappature del **sistema informatico** e degli **applicativi e delle piattaforme utilizzate,** riportando le informazioni rilevanti secondo la solita tabella già descritta nei punti precedenti:

Data della Valutazione	Incaricato che effettua la Valutazione	Definizione e contesto delle operazioni di trattamento									
		codice ID tratt.	Denominazione	Finalità	Autorizzati che effettuano il trattamento	Dati trattati	Categorie di interessati	Operazioni eseguite	Destinatari	Mezzi di elaborazione Dispositivi	Elaboratore utilizzato (*Archiviazione interna/esterna; Responsabile*)

La compilazione di tale scheda può essere effettuata utilizzando il tool in Excel denominato "***Tool in Excel per la Valutazione e il trattamento del rischio***" (Allegato B)

Tenuto del contesto in cui avviene il trattamento, effettuare le seguenti tre valutazioni:

- riflettere sull'impatto che una **divulgazione non autorizzata** (perdita di **riservatezza**) dei dati personali potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza

- riflettere sull'impatto che un'**alterazione non autorizzata** (perdita di **integrità**) dei dati personali potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza

- riflettere sull'impatto che una **distruzione o perdita non autorizzata** (perdita di **disponibilità**) dei dati personali potrebbe avere sull'individuo ed esprimere una valutazione/rating di conseguenza

Per agevolare tali valutazioni si possono utilizzare le seguenti **Check list di analisi del rischio reperibile in word nell'Allegato F.**

Accesso illegittimo dei dati (violazione della Riservatezza)	
1) Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?	
2) Quali sono le principali minacce che potrebbero	

concretizzare il rischio?	
3) Quali sono le fonti di rischio?	
4) Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	
5) Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	
6) Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	

Modifiche indesiderate dei dati (violazione dell'Integrità)	
1) Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?	
2) Quali sono le principali minacce che potrebbero concretizzare il rischio?	
3) Quali sono le fonti di rischio?	
4) Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	
5) Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	
6) Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	

Perdita dei dati (violazione della Disponibilità)	
1) Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?	
2) Quali sono le principali minacce che potrebbero concretizzare il rischio?	
3) Quali sono le fonti di rischio?	
4) Quali misure fra quelle individuate contribuiscono a mitigare il rischio?	
5) Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?	
6) Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?	

Per ognuno dei tre aspetti **valutare il livello d'impatto** in base ai criteri di seguito indicati:

Valutazione del Livello di Impatto		
Indicatori del livello di impatto		
Basso	Gli individui possono andare incontro a **piccoli inconvenienti o disagi minori superabili senza particolari problemi** (tempo necessario per re-inserire informazioni, fastidi, irritazione, ecc.)	
Medio	Gli individui possono andare incontro a **inconvenienti o disagi significativi, superabili nonostante alcune difficoltà**	

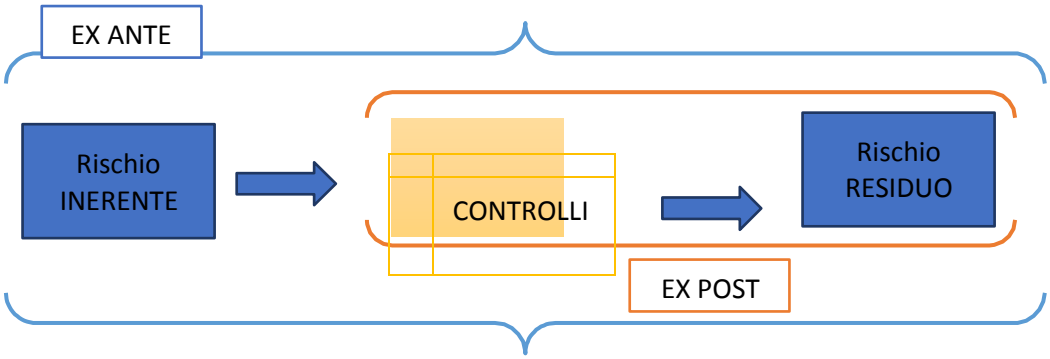
	(costi aggiuntivi, mancato accesso a servizi aziendali, paura, difficoltà di comprensione, stress, disturbi fisici di lieve entità, ecc.)	
Alto	Gli individui possono andare incontro a **conseguenze significative che si dovrebbero poter superare ma con gravi difficoltà** (appropriazione indebita di fondi, sottrazione di liquidità, inserimento in elenchi negativi da parte di istituti finanziari, danni a beni materiali, danni alla proprietà, perdita dell'impiego, ordinanze o ingiunzioni giudiziarie, citazioni in giudizio compromissione dello stato di salute, ecc.)	
Molto alto	Gli individui possono andare incontro a **conseguenze significative o irreversibili, non superabili** (perdita capacità lavorativa, disturbi psicologici o fisici a lungo termine o cronici, decesso, ecc.)	
Perdita di Riservatezza *Motivazione*		
Perdita di Integrità *Motivazione*		
Perdita di Disponibilità *Motivazione*		
Livello d'impatto più elevato		

- Se livello d'impatto più elevato è **ALTO** o **MOLTO ALTO**: è necessario effettuare e documentare la **valutazione d'impatto (DPIA)**

- Se il livello d'impatto è **Medio** o **Basso**
  1) applicare le misure di sicurezza tecniche e organizzative adeguate a ridurre il rischio entro termini accettabili;
  2) effettuare la valutazione del rischio residuo seguendo la procedura di seguito descritta al punto 7).

si tratta di valutazione EX ANTE, fatta in termini di previsione in considerazione dei controlli che si andranno ad applicare tramite le misure di sicurezza pianificate.

Nel periodo successivo verrà fatta la valutazione EX POST considerando l'efficacia delle misure applicate, secondo il seguente schema:



6. I controlli e gli altri fattori di mitigazione del rischio: individuazione delle misure di sicurezza tecniche ed organizzative da applicare al trattamento

Per ridurre il rischio verranno prese in considerazione, come primo punto di riferimento, le misure di sicurezza elaborate da ENISA, riportate nell'**allegato F**.

Tenuto conto del contesto in cui si svolge il trattamento e dei fattori di rischio, chi effettua la valutazione dovrà **selezionare nell'elenco elaborato da ENISA le Misure tecniche e organizzative appropriate da applicare al trattamento,** in modo che il rischio possa essere ridotto ad un livello accettabile.

L'adeguatezza delle misure a specifici livelli di rischio non deve essere percepita come assoluta.

A seconda del contesto del trattamento dei dati personali, i responsabili d'area e i titolari di p.o. possono prendere in considerazione l'adozione di **misure aggiuntive**, anche se assegnate a un livello di rischio più elevato ed anche diverse da quelle elaborate da ENISA.

L'elenco di misure proposto non tiene conto di altri ulteriori requisiti di sicurezza specifici del settore, nonché di obblighi normativi specifici, derivanti ad esempio dalla direttiva ePrivacy o dalla direttiva NIS.

Le misure individuate da ENISA sono ripartite nelle seguenti categorie e sono differenziate in tre livelli

- misure da adottare se il rischio è **basso**: di regola devono essere sempre adottate
- misure da adottare se il rischio è **medio**: di regola devono essere sempre adottate
- misure da adottare se il rischio è **alto**: devono essere sempre adottate come misure aggiuntive

Le misure sono inoltre distinte in tre categorie:

- **obbligatorie**: da applicare sempre a tutti i trattamenti
- **opzionali**: da applicare a discrezione degli incaricati
- **se applicabili**: da applicare solo nei contesti in cui ciò risulti possibile

Di seguito si riportano le categorie delle misure previste da ENISA

Misure organizzative in materia di sicurezza

Id.	Categoria delle misure
A.1	Politica di sicurezza e procedure per la protezione dei dati personali
B.1	Ruoli e responsabilità
C.1	Politica di controllo degli accessi
D.1	Gestione risorse/asset
E.1	Gestione delle modifiche
F.1	Responsabili del trattamento
G.1	Gestione degli incidenti / Personal data breaches
H.1	Continuità operativa
I.1	Obblighi di riservatezza imposti al personale

J.1	**Formazione**
K.1	**Controllo degli accessi e autenticazione**
L.1	**Generazione di file di log e monitoraggio**
M.1	**Sicurezza di Server e Database**
N.1	**Sicurezza delle Postazioni di lavoro**
O.1	**Sicurezza della rete e delle Infrastrutture di comunicazione elettronica**
P.1	**Backup**
Q.1	**Dispositivi mobili / portatili**
R.1	**Sicurezza del ciclo di vita delle applicazioni**
S.1	**Cancellazione / eliminazione dei dati**
T.1	**Sicurezza fisica**

- **Le misure selezionate** da applicare al trattamento dovranno essere **riportate nel dettaglio nella documentazione della valutazione,** compilando la seguente tabella nella quale, per ciascuna misura, verranno indicati**:**
  - **l'obbligatorietà** dell'attuazione della misura;
  - **lo Stato** in cui si trova la misura:
    Misura già adottata
    Attuazione in corso
  - **l'Area/Ufficio** che effettua il trattamento
  - **congome e nome dell'Incaricato dell'attuazione**
  - **il termine** entro il quale la misura dovrà essere attuata
  - **eventuali Responsabili esterni** coinvolti nell'attuazione delle misure

Misure obbligatorie	Stato	Area/ufficio	Incaricato dell'attuazione	Termine per l'attuazione	Responsabili esterni
Obbligatoria					

7. Valutazione del rischio residuo

- Il **livello d'impatto massimo** determinato nella fase precedente (Rischio inerente) deve essere messo in relazione con il **livello di PROBABILITA'** che si verifichi l'evento avverso.
- Preliminarmente, bisogna tener conto del contesto in cui si svolge il trattamento e compilare le seguenti tabelle:

Titolare del trattamento	
Data della valutazione	
Incaricato che effettua la valutazione	

Definizione e contesto delle operazioni di trattamento	
codice ID trattamento	
Denominazione	
Finalità	
Autorizzati	
Dati trattati	
Operazioni eseguite	
Destinatari	
Mezzi di elaborazione /Dispositivi	
Elaboratore utilizzato (*Archiviazione interna/esterna; Responsabile*)	

- Si procede, quindi, a **valutare la probabilità** che si verifichi l'evento avverso tenendo conto delle minacce, dei fattori di rischio e dei criteri di seguito indicati:
- Se la risposta data è NO indicare una sintetica e pertinente motivazione

Valutazione del livello di probabilità

Rispondere ad ogni domanda con SI / NO
Calcolare il punteggio per ogni Area in base alla seguente tabella e motivare brevemente

N. di risposte affermative	Livello	Punteggio
0-1	Basso	1
2-3	Medio	2
4-5	Alto	3

1. Risorse di rete

1. Vi sono parti del trattamento svolte attraverso Internet?	2. E' possibile accedere a un Sistema interno di trattamento dati attraverso Internet (per esempio, riguardo a certi utenti o gruppi di utenti)?	3. Il Sistema di trattamento dati personali è interconnesso a un altro Sistema o Servizio IT interno o esterno all'ente?	4. E' facile per soggetti non autorizzati accedere all'ambiente di trattamento dati?	5. Il Sistema di trattamento dati personali è progettato, implementato o manutenuto senza seguire le migliori pratiche del settore?	Punti
				Livello di probabilità	

Motivazione:	1) 2) 3) 4) 5)

2. Processi e procedure

6. Ruoli e procedure relative al trattamento di dati personali sono definiti in modo incerto o insufficiente?	7. L'utilizzo accettabile delle risorse di rete, di Sistema e fisiche all'interno dell'ente è definito in modo incerto o insufficiente?	8. Ai dipendenti è consentito portare con sé e utilizzare i propri dispositivi collegandoli al Sistema di trattamento dati personali?	9. Ai dipendenti è consentito trasferire, memorizzare o comunque trattare dati personali al di fuori del perimetro dell'ente?	10. Le attività di trattamento dati personali possono essere svolte senza che ciò comporti la creazione di file di registrazione eventi	Puntl

				(log files)?	
				Livello di probabilità	
Motivazione:	6) 7) 8) 9) 10)				

3. Soggetti e persone coinvolte

11. Il trattamento di dati personali è svolto da un numero indefinito di dipendenti?	12. Vi sono parti del trattamento svolte da un agente o da un soggetto terzo (responsabile del trattamento)?	13. Gli obblighi dei soggetti/delle persone coinvolti nel trattamento di dati personali sono fissati in modo incerto o insufficiente?	14. Il personale che partecipa al trattamento di dati personali non ha conoscenze in materia di sicurezza delle informazioni?	15. I soggetti/le persone che partecipano al trattamento di dati personali omettono di conservare in modo sicuro e/o distruggere i dati personali?	Puntl
				Livello di probabilità	
Motivazione:	11) 12) 13) 14) 15)				

4. Settore di attività e scala del trattamento

16. Ritenete che il Vostro settore di attività sia passibile di attacchi cibernetici (cyberattacks)?	17. L'ente ha subito attacchi cibernetici o altre tipologie di violazioni della sicurezza negli ultimi due anni?	18. Sono stati ricevuti notifiche e/o reclami relativamente alla sicurezza dei sistemi IT (utilizzati per il trattamento di dati personali) nell'ultimo anno?	19. Un trattamento riguarda volumi consistenti di dati personali e/o un numero consistente di persone fisiche?	20. Esistono migliori pratiche in materia di sicurezza specifiche del settore di attività dell'ente che non siano state implementate in misura adeguata?	Punti
				Livello di probabilità	
Motivazione:	16) 17) 18) 19) 20)				
				Somma dei punti delle quattro aree di valutazione	

<u>Livello di probabilità</u> del verificarsi di minacce

Somma dei punteggi delle 4 aree	Livello di probabilità
4 - 5	BASSA
6 – 8	MEDIA
9 - 12	ALTA

In base alla somma dei punteggi ottenuti indicare il livello di probabilità tenuto conto della tabella a fianco:

VALUTAZIONE DEL RISCHIO COMPLESSIVO

- *Riportare Il **livello d'impatto** massimo determinato nella fase precedente (Rischio inerente)*
- *Indicare il **livello di probabilità** determinato come sopra*
- *Calcolare il Rischio complessivo in base alla seguente tabella:*

Legenda:
Rischio basso | Rischio medio | Rischio elevato

Impatto	**Probabilità**	**RISCHIO COMPLESSIVO**

Tale fase può essere effettuata utilizzando il file in Excel **Allegato B. Tool in Excel per la Valutazione e il trattamento del rischio o, in alternativa il file in word Allegato C**

8. Decisione da adottare in ordine al trattamento

Sulla base del risultato ottenuto nella fase precedente**, assumere la decisione in ordine al trattamento del rischio** compilando la scheda che segue:

Trattamento del rischio		Decisione adottata	Incaricato dell'attuazione delle misure	Termini previsti per l'attuazione/verifica
Accettazione del rischio	Il rischio viene accettato: non è necessario implementare altre misure			
Riduzione del rischio	Il rischio deve essere attenuato implementando altre misure			
Rifiuto del rischio	Il trattemento viene soppresso			
N/A	Nessun trattamento del rischio è applicabile			

Trattamento del rischio

- Se il **rischio <u>residuo</u>** è **ALTO**: il trattamento <u>deve</u> essere
  - soppresso (RIFIUTO del rischio);
  - o modificato. In questo caso è necessario effettuare la DPIA alla luce delle modifiche apportate
- Se il **rischio <u>residuo</u>** è **BASSO e MEDIO:** il trattamento <u>può</u>
  - essere ACCETTATO (senza adottare altre misure)
  - essere RIDOTTO (adottando altre misure); l**e misure selezionate** da applicare al trattamento dovranno essere **riportate nel dettaglio nella documentazione della valutazione,** compilando la seguente tabella nella quale, per ciascuna misura verranno indicati**:**
    - **l'obbligatorietà** dell'attuazione della misura;
    - **lo Stato** in cui si trova la misura:

      Misura già adottata

      Attuazione in corso

    - **l'Area/Ufficio** che effettua il trattamento

- **congome e nome dell'Incaricato dell'attuazione**
- **il termine** entro il quale la misura dovrà essere attuata
- **eventuali Responsabili esterni** coinvolti nell'attuazione delle misure

Misure obbligatorie	Stato	Area/ufficio	Incaricato dell'attuazione	Termine per l'attuazione	Responsabili esterni
Obbligatoria					

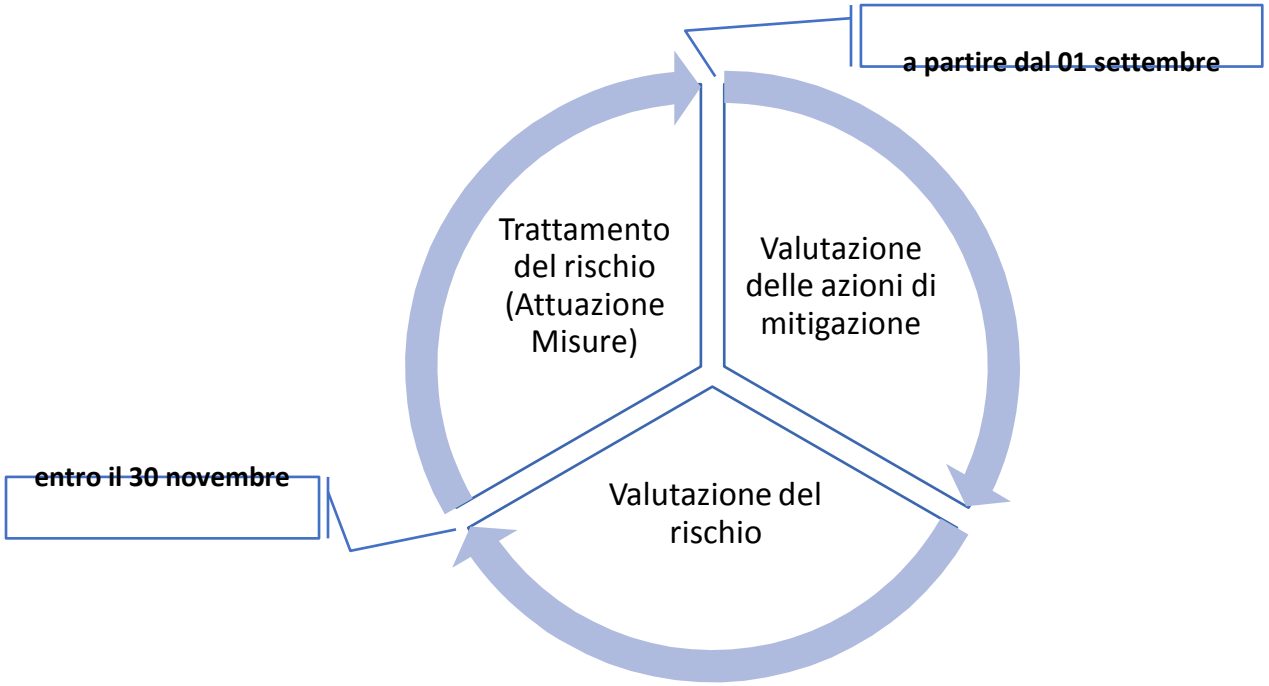
9. Il Trattamento del rischio: attuazione e valutazione delle azioni di mitigazione adottate.

Le misure di sicurezza selezionate dovranno essere attuate a cura della persona incaricata entro i termini previsti nella scheda riportata nel punto precedente.

Successivamente si procederà a **monitorare**, **testare** e **verificare** l'efficacia delle misure adottate e l'efficacia della presente procedura.

Nel periodo successivo a quello di applicazione delle misure, **a partire dal 30 novembre** di ciascun anno, sarà effettuata una nuova valutazione del rischio e l'esito verrà confrontato con quello dell'anno precedente.

L'adeguatezza delle azioni di mitigazione del rischio e l'efficacia della presente procedura saranno monitorate e valutate seguendo la procedura descritta nel punto seguente.

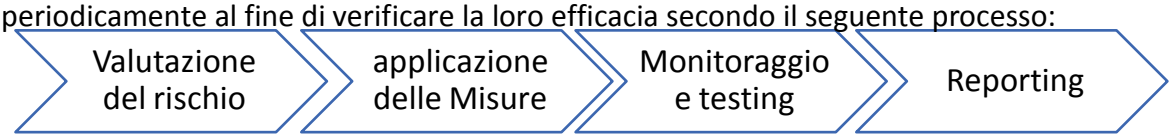


10. Monitoraggio e controllo delle azioni di mitigazione adottate: metodologia e criteri indicatori di rischio

La verifica dell'efficacia delle azioni di mitigazione è essenzialmente oggetto del riesame da parte dell'amministrazione e del DPO.

Di seguito vengono predisposti i processi che dovranno seguire i **responsabili per la rilevazione e il riporto dei dati** che vengono individuati sin da ora nei soggetti designati con specifici compiti, già nominati dall'amministrazione ai sensi dell'art. 2-quaterdecies del D.Lg.s 2033 n.196, salva la facoltà dei dirigenti e/o dei responsabili di p.o. di attribuire tali compiti anche ad altri soggetti specificamente individuati con formale provvedimento di designazione e nomina.

Le azioni di mitigazione adottate devono essere monitorate continuamente e testate periodicamente al fine di verificare la loro efficacia secondo il seguente processo:



Il monitoraggio degli indicatori di rischio può permettere di identificare tendenze anomale e potenziali difformità.

E' uno strumento di controllo a distanza e preventivo che facilita una razionale e completa valutazione del sistema dei controlli interni a presidio dei rischi di non conformità alle norme.

Con "**controllo a distanza**" si intende un'attività di indagine condotta tramite l'estrazione, l'elaborazione e l'analisi continuativa e sistematica di dati provenienti direttamente da diversi archivi dell'ente.

Il monitoraggio degli indicatori di rischi persegue una molteplicità di **obiettivi** quali:

- l'indirizzo dell'azione di controllo della conformità in modo da orientare la pianificazione delle attività sulle aree più critiche;
- l'individuazione e il monitoraggio continui delle aree di maggiore rischio per consentire azioni di intervento tempestive e mirate;
- la ricerca di informazioni predittive a supporto delle valutazioni qualitative derivanti dalle altre attività svolte per assicurare la conformità;
- il miglioramento dell'efficacia e dell'efficienza del processo di valutazione del sistema dei controlli interni a presidio dei rischi di non conformità alle norme.

I test di conformità costituiscono il momento di **verifica ex post** della funzione di compliance ed hanno l'obiettivo di assicurare che effettivamente nel tempo le azioni di mitigazione, che ex ante sono state giudicate adeguate, abbiano effettivamente mitigato i rischi, ossia siano efficaci.

Per valutare l'efficacia occorre necessariamente avere dei riferimenti numerici, in termini di obiettivi e di risultati. A tal fine si prevede lo sviluppo di almeno tre tipologie di **indicatori di rischio** come di seguito indicati:

INDICATORI DI RISCHIO	
indicatori di esposizione al rischio:	**n. di minacce** che insidiano il trattamento

	n. di eventi formativi non effettuati o non effettuati nelle scadenze programmate **n. di elementi del piano di miglioramento non effettuati** nei tempi programmati
indicatori di anomalia:	**n. di reclami ricevuti**; **n. di incidenti di sicurezza (data breach)** **n. di incidenti della sicurezza (anche se non c'è stato data breach)** es.: n. di incidenti a seguito di virus o malware; eventi riscontrati di mancato rispetto delle policy e procedure per la sicurezza; n. di **data breach non registrati nel registro** delle violazioni **n. di reclami o lamentele degli interessati** **n. di riscontri agli interessati inevasi o non evasi** nei termini di legge **n. di violazioni del tempo massimo** di conservazione dei dati **n. di non conformità riscontrate negli audit e non risolte** nei tempi programmati n. di **violazioni sugli obblighi di informativa** n. di **nuovi trattamenti non registrati sul registro** o comunque prima di effettuare il trattamento
indicatori di perdita:	**n. di provvedimenti sanzionatori**

FREQUENZA dei controlli: la tempistica di estrazione dell'indicatore è in relazione al livello del rischio. Più è alto il **rischio inerente** maggiore sarà la frequenza con cui si dovrà verificare che sia andato tutto bene, secondo la seguente tempistica:

VALUTAZIONE RISCHIO INERENTE	FREQUENZA COMPLIANCE TEST
BASSO	ANNUALE
MEDIO	SEMESTRALE
ALTO	TRIMESTRALE

ELEMENTI DEL COMPLIANCE TEST:

Le verifiche, che saranno effettuate nei tempi indicati dalle persone designate con tale specifico compito, dovranno indicare i seguenti elementi:

DESCRIZIONE/OBIETTIVO: breve descrizione delle verifiche che verranno effettuate.

DATA e FREQUENZA: indicazione della data, del periodo di riferimento e della periodicità del test.

METODOLOGIA: Il test può essere performato utilizzando metodologie diverse:

interviste, check list
inchieste
esame della documentazione
riesecuzione dell'attività
produzione di specifici report di controllo
simulazioni di incidenti di sicurezza o di richieste di esercizio dei diritti

POPOLAZIONE: indicazione di tutti gli oggetti che costituiscono l'area di interesse. Es. Numero di trattamenti verificati nell'ultimo quadrimestre. Nel test è necessario fornire una descrizione della popolazione ed indicare il numero di oggetti che la compongono.

CAMPIONE: descrizione della tecnica utilizzata per la selezione degli oggetti della popolazione da sottoporre a verifica e numerosità di tali oggetti rispetto alla popolazione.

TESTER: nome, cognome e ruolo di colui che esegue i test. Può far parte della funzione di compliance o può appartenere all'unità in cui vengono eseguite le azioni mitiganti, ma – in questo caso – dovrà essere persona differente rispetto a quella che pone in essere tali azioni e non potrà essere il responsabile d ell'unit à/ ufficio che effettua il trattamento.

ESITO: inidcazione dei risultati dei test effettuati, includendo il numero e il tipo delle eventuali anomalie riscontrate.

TECNICHE DI CAMPIONAMENTO:

Deve essere descritto il criterio di selezione utilizzato (una terza persona deve essere in grado di replicare il test)

Deve essere fornito una giustificazione per la scelta della tecnica di campionamento tra quelle di seguito descritte:

Tecniche di campionamento	Modalità	Criterio di selezione
Random	selezione **casuale** degli elementi della popolazione da sottoporre a verifica che assegna a tutti gli elementi della popolazione la stessa probabilità di essere inclusi nel campione. Il campione selezionato possiede approssimativamente le stesse caratteristiche in una porzione della popolazione. Tale selezione permette di estendere i risultati delle verifiche sul campione all'intera popolazione.	Selezione **casuale** semplice.
Totale	Gli elementi della popolazione che verranno verificati (campione) coincidono con la popolazione.	**Tutti** gli elementi inclusi nella popolazione
Judgemental	Gli elementi inclusi nel campione soddisfano alcuni **requisiti stabiliti dal Tester**, che quindi consapevolmente influenza il processo di selezione per ottenere certi obiettivi. In questo modo non si intende rappresentare con il campione l'intera popolazione.	Chiara descrizione del criterio usato
Sistematica	individuare il campione da gruppi di elementi che hanno determinate caratteristiche in comune.	Chiara descrizione delle caratteristiche prese a riferimento per **segmentare la popolazione in sottoinsiemi**. Indicazione del criterio di selezione utilizzato all'interno dei sottoinsiemi della popolazione.

NUMEROSITA DEL CAMPIONE: indicazione del numero degli elementi selezionati dalla popolazione.

MO DA LI T A ' DI SVO LGI MEN T O : la persona designata con tale specifico compito dovrà

- **pianificare** l'attività con un congruo anticipo

- **Registrare** le attività svolte: aree interessate; obiettivi delle verifiche; metodologia impiegata; esiti delle verifiche; eventuali misure correttive dottate

- **Conservare** accuratamente la documentazione

Ogni test dovrà essere documentato mediante compilazione di una **scheda di sintesi** come di seguito indicato:

COMPLIANCE TEST: FORMALIZZAZIONE

Scheda compliance test			
Rif. Test			
Data del test			
Periodo di riferimento			
Obiettivo del test			
INDICATORI DI RISCHIO UTILIZZATI			
Indicatori di esposizione al rischio	Indicatori di esposizione anomalia		Indicatori di perdita
Frequenza (periodicità)			
Popolazione	descrizione		
	#elementi		
Campione	Tecnica		
	Criterio di selezione		
Metodologia			
Tester: Cognome, nome e ruolo/ufficio di appartenenza			
ESITO			

La compilazione della scheda, che dovrà essere datata e firmata dall'incaricato, potrà essere effettuata utilizzando **l'allegato L Scheda Compliant test in word** o **l'allegato M Tool in Excel per il Compliant test**

11. Valutazione del rischio residuale dopo l'applicazione delle misure

L'attività di monitoraggio e verifica sopra descritta dovrà condurre ai seguenti esiti:

ESITO COMPLIANCE TEST:

POSITIVO	NEGATIVO
Non sono state rilevate anomalie o le anomalie rilevate sono giudicate non significative	Le anomalie rilevate dimostrano che le azioni poste a mitigazione non stanno mitigando il rischio
VALIDAZIONE DEL RISCHIO RESIDUO	APERTURA **PIANO DI ADEGUAMENTO**
	VALUTAZIONE RISCHIO RESIDUO

In caso di esito POSITIVO, si procederà alla VALIDAZIONE del rischio residuo (ex post) redigendo il seguente report:

VALIDAZIONE DEL RISCHIO RESIDUALE					
Descrizione	**Frequenza**	**Tester**	**Metodologia**	**Esito**	**Rischio RESIDUO (EX POST)**

In caso di esito NEGATIVO, si procederà a

- attivare un **PIANO DI ADEGUAMENTO** che descriva le criticità rilevate e indichi le azioni da mettere in atto per rimuoverle e i tempi di attuazione in base ad un cronoprogramma
- VALUTARE nuovamente il rischio inerente applicando le misure adeguate a mitigarlo seguendo la procedura descritta al punto 5).

All'esito di tali verifiche **le misure adottate**, oggetto di monitoraggio, **saranno così classificate**:

VALUTAZIONE EX POST SULLE AZIONI DI MITIGAZIONE	
NON ADEGUATA	non esiste alcuna mitigazione.
PARZIALMENTE ADEGUATA	la misura presidia solo in parte il rischio
PREVALENTEMENTE ADEGUATA	la misura presidia una parte rilevante del rischio
ADEGUATA	la misura presidia integralmente il rischio

12. Adozione di un Piano di adeguamento correttivo

In caso di esito negativo del compliance test, occorre procedere alla definizione di **un piano di azione correttivo** al fine di:

sanare le anomalie e criticità riscontrate,
definire e attuare nuove azioni di mitigazione.

Il **Piano di adeguamento** sarà costituito almeno dai seguenti **elementi**:

Tipologia di anomalia/criticità riscontrata (inadeguatezza del controllo, superamento del limite accettabile)
Descrizione dell'anomalia/criticità
Azione proposta
Data definita per la realizzazione dell'azione proposta
Definizione delle **priorità** di intervento secondo un **CRONOPROGRAMMA**
Incaricato della **realizzazione**
Incaricato della **verifica dell'attuazione dell'azione**

Il Piano di adeguamento dovrà essere approvato dall'amministrazione con un formale atto deliberativo.

13. Procedura per testare, verificare e valutare l'efficacia delle misure adottate (Audit)

L'efficacia delle misure adottate e l'efficacia della presente procedura di gestione devono essere monitorate costantemente, testate e verificate periodicamente, di regola a partire dal 01 settembre di ogni anno, in modo da consentire a tutti gli uffici di riesaminare le loro analisi e valutazioni entro il 30 novembre.

13.1 Verifica delle misure adottate per assicurare la conformità

Per **valutare l'efficacia delle misure adottate** si prenderà in considerazione l'Indice medio di conformità registrato nelle valutazioni effettuate nel periodo considerato, fermo restando il fatto che ogni difformità del trattamento deve essere immediatamente rimossa perché costituisce di per sé un rischio per gli interessati.

La **valutazione circa l'efficacia delle misure adottate** sarà quindi effettuata sulla base dei seguenti criteri minimi di valutazione:

Variazione dell'Indice medio di conformità registrato nell'anno	**Le misure adottate sono**	
> 1%	Efficaci	
< 1 %	Neutre/Parzialmente efficaci	
< 0%	Inefficaci	

I suddetti criteri di valutazione costituiscono solo la base di partenza per la valutazione dell'efficacia delle misure adottate e dell'efficacia della presente procedura. Essi potranno essere modificati o integrati con altri criteri individuati di volta in volta dall'amministrazione o suggeriti dal RPD sulla base dei risultati registrati nel periodo considerato. A titolo esemplificativo, ma non esaustivo, si terrà conto anche dei seguenti ulteriori criteri:

- **Incidente di sicurezza** (data breach) verificatosi nell'anno precedente;
- **diritti esercitati** dagli interessati nell'anno precedente;
- **Suggerimenti o segnalazioni del RPD**;
- **Richieste di chiarimenti o provvedimenti formulati dal Garante** per la protezione dei dati personali;

Qualora ricorra anche uno solo di detti criteri la valutazione dell'efficacia delle misure e della procedura sarà negativa, salvo che sussistano specifici elementi idonei ad escludere tale valutazione.

Nel caso in cui le misure adottate risultassero "*inefficaci*" o "*parzialmente efficaci*" l'amministrazione, acquisito il parere del RPD, provvederà ad adottare le necessarie misure correttive, modificando se del caso anche la procedura di valutazione, ridefinendo i tempi di

intervento, i ruoli e le responsabilità adottando ove necessario un Piano di adeguamento con l'indicazione delle azioni correttive da mettere in atto.

13.2 Verifica d el l ' efficacia della procedura di valutazione della conformità

Per testare e valutare l'efficacia della procedura di valutazione della conformità descritta al punto 2), al termine di ogni valutazione periodica effettuata dagli uffici **la persona designata** con questo specifico compito provvederà a **raccogliere i seguenti dati** risultanti dalle valutazioni dei singoli trattamenti effettuate dai diversi uffici nell'anno in corso:

Monitoraggio delle valutazioni di conformità effettuate nell'anno			
ID trattamento	**Ufficio/Area**	**Data della valutazione**	**Grado complessivo di conformità %**

I valori del **grado complessivo di conformità** (espressi in percentuale) registrati nei vari trattamenti oggetto di valutazione saranno sommati e il risultato sarà diviso per il numero dei trattamenti oggetto di valutazione ottenendo così **l 'in di ce med i o d i co nf ormi tà co mp l essi va .**

I dati ottenuti saranno **confrontati con quelli relativi all'anno precedente** compilando la seguente tabella:

Criteri	anno 1	anno 2	Variazioni**
n. di trattamenti censiti nel Registro dei trattamenti			
n. complessivo di valutazioni effettuate dai vari uffici			
% di valutazioni effettuate dai vari uffici			
Indice medio di conformità complessiva*			

* *sommare di tutti gli **indici di conformità relativi a ciascun trattamento** e dividere per il numero dei trattamenti oggetto di valutazione;*

** riportare nella colonna Variazioni, le variazioni registrate nei due periodi per ogni singola voce

I dati così raccolti saranno **trasmessi all'amministrazione, ai responsabili d'area e ai titolari di P.O.** che sulla base di tali informazioni effettueranno la valutazione in ordine all'efficacia/inefficacia della procedura di valutazione adottata incrociando i dati ottenuti secondo i seguenti criteri:

		Variazione dell'**Indice medio di conformità**		
		Diminuisce	Invariato	Aumenta
Variazione della **% di valutazioni effettuate**	Diminuisce			
	Invariata			
	Aumenta			

Legenda: la procedura di valutazione è		
Inefficace	Invariata	Efficace

Il **report** finale dei dati raccolti sarà trasmesso al RPD per le sue valutazioni

Nel caso in cui la procedura di valutazione della conformità risultasse "*inefficace*" o "Invariata", l'amministrazione, acquisito il parere del RPD, provvederà ad apportare le necessarie modifiche volte a rimuovere le criticità rilevate.

Le verifiche descritte ai punti 13.1 e 13.2 possono essere effettuate utilizzando il **tool in Excel per testare e valutare l'efficacia delle misure adottate e della procedura di valutazione della conformità Allegato N.**

13.3 Verifica del l'efficacia della procedura di valutazione cir ca l'obbl igo di effet tuar e una DPIA

Per testare e valutare l'efficacia della procedura prevista per stabilire se sussiste l'obbligo di effettuare la DPIA si considereranno i seguenti **criteri**:

<table>
<tr><th colspan="3">CRITERI PER VALUTARE L'EFFICACIA DELLA PROCEDURA DI VALUTAZIONE CIRCA L'OBBLIGO DI EFFETTUARE LA DPIA</th></tr>
<tr><td colspan="2">% dei trattamenti peri quali è stata fatta la Valutazione
> o = al 90%</td><td>% dei trattamenti peri quali è stata fatta la Valutazione
< al 90%</td></tr>
<tr><td colspan="2">Effettuare controlli a campione sulle verifiche effettuate</td><td rowspan="2"></td></tr>
<tr><td>valutazioni esatte e corrette
= 100%</td><td>valutazioni esatte e corrette
< 100%</td></tr>
<tr><td rowspan="2">LA PROCEDURA E' EFFICACE</td><td colspan="2">LA PROCEDURA E' INEFFICACE</td></tr>
<tr><td colspan="2">revisionare e modificare la procedura o effettuare altre azioni di adeguamento.</td></tr>
</table>

- Se la **percentuale di trattamenti** per i quali è stata **effettuata la valutazione** nel periodo considerato è **superiore o uguale al 90%,** si effettueranno controlli A CAMPIONE sulle valutazioni effettuate:

  Se il 100% delle valutazioni controllate sono esatte e corrette, la procedura è EFFICACE;

  altrimenti la procedura è INEFFICACE: è necessario revisionare e modificare la procedura o effettuare altre azioni di adeguamento.

- Se la **percentuale di trattamenti** per i quali è stata effettuata la valutazione nel periodo considerato **è inferiore al 90%** la procedura è considerata INEFFICACE: occorre revisionare e modificare la procedura o effettuare altre azioni di adeguamento

- **Successive verifiche anche a campione** sono effettuate dai responsabili o dai titolari di P.O. al fine di verificare se le valutazioni effettuate siano esatte e corrette.

Le verifiche sopra descritte possono essere effettuate utilizzando il **tool in** per testare e valutare l'efficacia della procedura prevista per stabilire se sussiste l'obbligo di effettuare la DPIA **Allegato O.**

14. La valutazione d'impatto: metodologia

Se la valutazione preliminare del rischio condotta nei termini indicati mostra effettivamente che un determinato trattamento può comportare un "**rischio elevato**", il titolare è tenuto a condurre una **valutazione di impatto sulla protezione dei dati** (DPIA) prima di procedere al trattamento e a mettere in atto adeguate **misure di mitigazione o opzioni alternative**.

La valutazione sarà condotta secondo quanto è previsto nelle Linee guida Gruppo di lavoro Articolo 29 - WP 248 - in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" - adottate il 4 aprile 2017 -come modificate e adottate da ultimo il 4 ottobre 2017, nelle altre linee guida adottate dall'EDPB e dal Garante per la protezione dei dati personali.

La valutazione viene effettuata da un TEAM di persone designate dall'amministrazione ai sensi dell'art. 2-quaterdecies Codice privacy con tale specifico compito. Il Dirigente o responsabile di p.o. può inserire nel TEAM anche altri dipendenti al fine di effettuare una specifica valutazione su uno o pià trattamenti, assicurando la partecipazione di persone di genere diverso.

"Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi" (Art. 35, paragrafo 1, ultimo periodo).

La valutazione d'impatto deve essere effettuata prima di procedere al trattamento.

Nel condurre la valutazione si potranno utilizzare le metodologie elaborate dal CNIL, secondo il **modello allegato con la lettera I,** o secondo modelli o standard approvati da altre autorità, evitando in ogni caso di utilizzate schemi standard e semplificazioni che rischiano di comprometterne l'efficacia.

La struttura della valutazione d'impatto sarà la seguente:

1) Dati del Titolare, Denominazione / contatti, dati del DPO
2) Descrizione sistematica del trattamento anche mediante un diagramma di flusso
3) Valutazione circa l'osservanza principi del trattamento e sulla necessità e proporzionalità del trattamento in relazione alle finalità
4) Valutazione dei rischi per i diritti e le libertà degli interessati
5) Gestione dei rischi: indicazione delle misure tecniche e organizzative da applicare
6) Stima del Rischio residuo
7) Decisione in ordine al trattamento
8) Eventuale consultazione preventiva del Garante ai sensi dell'art. 36 del Reg. Ue 2016 n.679

La valutazione dovrà

- tener conto di tutti i rischi anche di quelli non riferibili agli incidenti informatici;

- esaminare i diversi scenari di rischio e i possibili impatti al fine di individuare misure adeguate ad affrontarli per annullarli o ridurli ad un livello accettabile;
- non focalizzarsi solo su aspetti meramente tecnici del trattamento;
- evitare di utilizzare schemi standard o semplificazioni che potrebbero comprometterne l'efficacia rendendola generica e inadeguata rispetto ai rischi effettivi del trattamento;
- essere fatta in concreto e in **modo adeguato e puntuale**, avendo cura **che le misure previste siano inerenti ai rischi** previsti, evitando di riportare giudizi di adeguatezza estremamente sintetici, privi di idonea motivazione che non individuino, in relazione ai profili esaminati, appropriate misure "per affrontare i rischi" e per attenuare gli stessi, astenendosi dal prevedere misure inconferenti per la mitigazione del rischio
- assicurare l'applicazione dei principi del trattamento individuando degli "indicatori di prestazione", fissando delle "metriche" che consentano di "misurare" e rendere disponibili per tutti le valutazioni fatte;
- tener conto dello "stato dell'arte" (innovazioni tecnologiche);
- tener conto dei costi (efficienza economica)

La valutazione sarà condotta con il coinvolgimento

- delle figure rilevanti dell'organizzazione (Responsabile per la transizione digitale, Responsabile della gestione documentale e della conservazione, Responsabile della prevenzione della corruzione e della trasparenza, Responsabile della sicurezza informatica, ecc.);
- dei Responsabili del trattamento e dei Contitolari
- ove possibile, degli interessati o loro rappresentanti, mediante test, questionari o sondaggi che raccolgano le loro opinioni;

Sulla valutazione dovrà essere chiesto obbligatoriamente il parere del Responsabile della protezione dei dati personali.

La valutazione potrà essere **pubblicata** nel sito web dell'ente anche in forma sintetica.

Sarà effettuato poi il **monitoraggio** al fine di verificare l'adeguatezza ed efficacia delle misure previste seguendo la metodologia indicata al precedente punto 13.

Periodicamente, ad intervalli regolari (almeno una volta all'anno o comunque ogni qualvolta se ne ravvisi la necessità) si procederà alla sua **revisione** con eventuale modifica e/op integrazione delle misure previste e della decisione adottata per iniziare quindi un nuovo ciclo.

15. Conservazione della documentazione

Tutti i documenti elaborati per effettuare le valutazioni previste nella presente procedura dovranno essere conservati adeguatamente, sotto la cura e la responsabilità dei dirigenti responsabili d'area o di p.o., nel rispetto delle norme

- sulla protocollazione,
- sulla gestione documentale,
- sulla conservazione degli atti e documenti amministrativi.

A tal fine i file dovranno essere salvati in formato aperto interoperabile, nei formati previsti dalle Linee Guida AGID sulla gestione documentale e dovranno essere applicati i metadati obbligatori previsti da dette linee guida oltre ai metadati facoltativi che possano risultare utili a reperire anche a distanza di tempo i singoli documenti o fascicoli.

16. Rapporti con il Responsabile della protezione dei dati personali (DPO)

Il Responsabile della protezione dei dati personali dovrà interpellato tempestivamente ogni qualvolta sorgano dubbi riguardo alle operazioni descritte nella presente procedura o in ordine ai rischi del trattamento. In tali casi dovrà essergli trasmessa immediatamente tutta la documentazione necessaria per consentirgli di esprimere il proprio parere.

Il Responsabile della protezione dei dati personali potrà in qualsiasi momento richiedere al personale che è autorizzato al trattamento dei dati la trasmissione di atti o documenti relativi alle operazioni compiute in base alla presente procedura e potrà fornire all'amministrazione eventuali suggerimenti indicando i correttivi da apportare alla presente procedura, alle azioni di mitigazione implementate e ai piani di adeguamento approvati e potrà proporre egli stesso l'approvazione di piani di miglioramento e l'applicazione di ulteriori misure correttive necessarie per mitigare i rischi entro limiti accettabili.

Tutte le richieste e comunicazioni formulate dal RPD, sia di persona sia tramite posta elettronica devono essere prontamente riscontrate come previsto nelle Linee guida per i rapporti con il RPD già approvate dall'amministrazione alle quali si rimanda.

Quando il RPD richiede la compilazione di questionari, check list, schede, tabelle, ecc., bisognerà provvedere tempestivamente avendo cura di fornire sempre dati esatti, completi e aggiornati.

Il parere del RPD deve ricevere sempre la dovuta considerazione.

In caso di disaccordi, occorre documentare le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal RPD.

Il RPD deve consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente, come previsto nel Piano di risposta per la gestione delle violazioni al quale si rimanda.

Data _____

Il Sindaco
F.to Dott. Danilo Parasole