Camera di Commercio
Gran Sasso d'Italia

PROCEDURA
D.P.I.A.
(*Data Protection Impact Assessment*)

Il presente documento si inserisce nel piano di *accountability* dell'Ente
in linea con i principi di cui al Regolamento (UE) 2016/679 – GDPR

SOMMARIO

INTRODUZIONE AL DOCUMENTO

SCOPO E CAMPO DI APPLICAZIONE

Scopo della presente **procedura** è disciplinare lo svolgimento della DPIA (Data Protection Impact Assessment) e di tutte le azioni/valutazioni a questa preliminari e/o conseguenti.

In particolare, la procedura regola lo svolgimento della preliminare valutazione del rischio finalizzata ad appurare se un dato trattamento o un insieme di trattamenti debba essere soggetto a DPIA (da svolgersi secondo le indicazioni fornite dalle Linee Guida dell'EDPB WP248 e dal Provvedimento dell'Autorità garante per la protezione dei dati personali del 11 ottobre 2018, n° 467); lo svolgimento in concreto della DPIA; gli adempimenti a questa eventualmente conseguenti.

Le valutazioni d'impatto sulla protezione dei dati personali sono strumenti importanti ai fini dell'*accountability* dell'Ente, in quanto sostengono i Titolari del trattamento non soltanto nel rispettare i requisiti fissati dal GDPR, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del Regolamento, tenendo conto (tra l'altro) dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo teso a garantire e a dimostrare la conformità dell'Ente al GDPR, anche sotto il profilo della gestione dei rischi insiti in ciascuna attività di trattamento di dati personali.

La presente procedura è portata a conoscenza mediante trasmissione del presente documento ai Dirigenti e alle P.O. e mediante la pubblicazione sul sito web istituzionale – nella sezione "Amministrazione Trasparente", alla pagina "Altri contenuti" -> Dati ulteriori -> Trattamento dati personali e Responsabile della Protezione dei Dati -> Adempimenti in materia di privacy.

NORMATIVA E LINEE GUIDA DI RIFERIMENTO

La presente procedura risponde ai seguenti requisiti normativi:

1. Regolamento (UE) 2016/679, *General Data Protection Regulation*:
   - artt. 24, 35 e 36;
   - considerando 84, 89, 90, 91, 93, 94, 95 e 96;
2. *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679* (WP248 rev0.1), Gruppo di lavoro *ex* art. 29 per la protezione dei dati (WP29);
3. Provvedimento dell'Autorità garante per la protezione dei dati personali del 11 ottobre 2018, n° 467 e relativo allegato;
4. Linee guida dell'*European Union Agency for Cybersecurity* (ENISA), *Handbook on Security of Personal Data Processing*.

ACRONIMI E DEFINIZIONI UTILIZZATE

GDPR / Regolamento	Regolamento UE 2016/679 (General Data Protection Regulation)
Codice Privacy	D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" come modificato dal D.Lgs. 101/2018
Garante	Autorità Garante per la protezione dei dati personali
WP29 / EDPB	Già *Article* 29 *Working Party*, Gruppo di lavoro *ex* art. 29 per la protezione dei dati, ora EDPB, *European Data Protection Board*
DPIA	*Data Protection Impact Assessment* o Valutazione d'impatto sulla protezione dei dati. È un processo volto a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.
Rischio	Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e di probabilità.

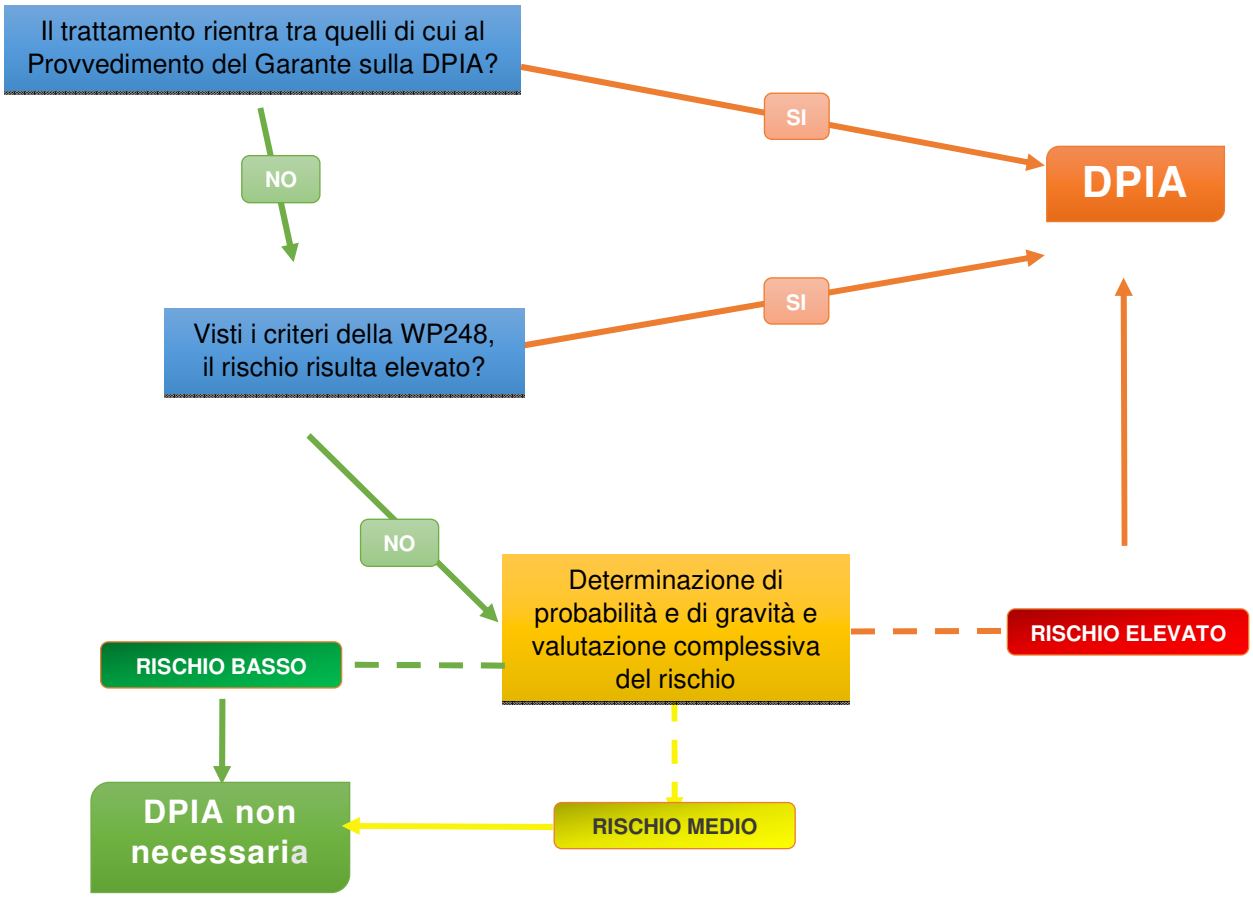
Diritti e Libertà delle persone fisiche	Vengono principalmente tenuti in considerazione i diritti alla protezione dei dati e alla vita privata, ma anche altri diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale
Interessato	La persona fisica cui si riferiscono i dati personali
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4, punto 7 del GDPR)
DPO / RPD	*Data Protection Officer*/ Responsabile della protezione dei dati, ai sensi dell'art. 37 del GDPR
Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento, ai sensi dell'art. 28 GDPR
Referente Privacy	Persona individuata dalla CCIAA per il coordinamento delle attività in ambito di privacy in carico all'Ente
Amministratore di Sistema Interno	Persona fisica incaricata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, ivi comprese le figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi
Delegato del Titolare	Dirigente individuato dall'Amministrazione quale Delegato del Titolare del Trattamento

MATRICE DELLA REDAZIONE E DELLE REVISIONI

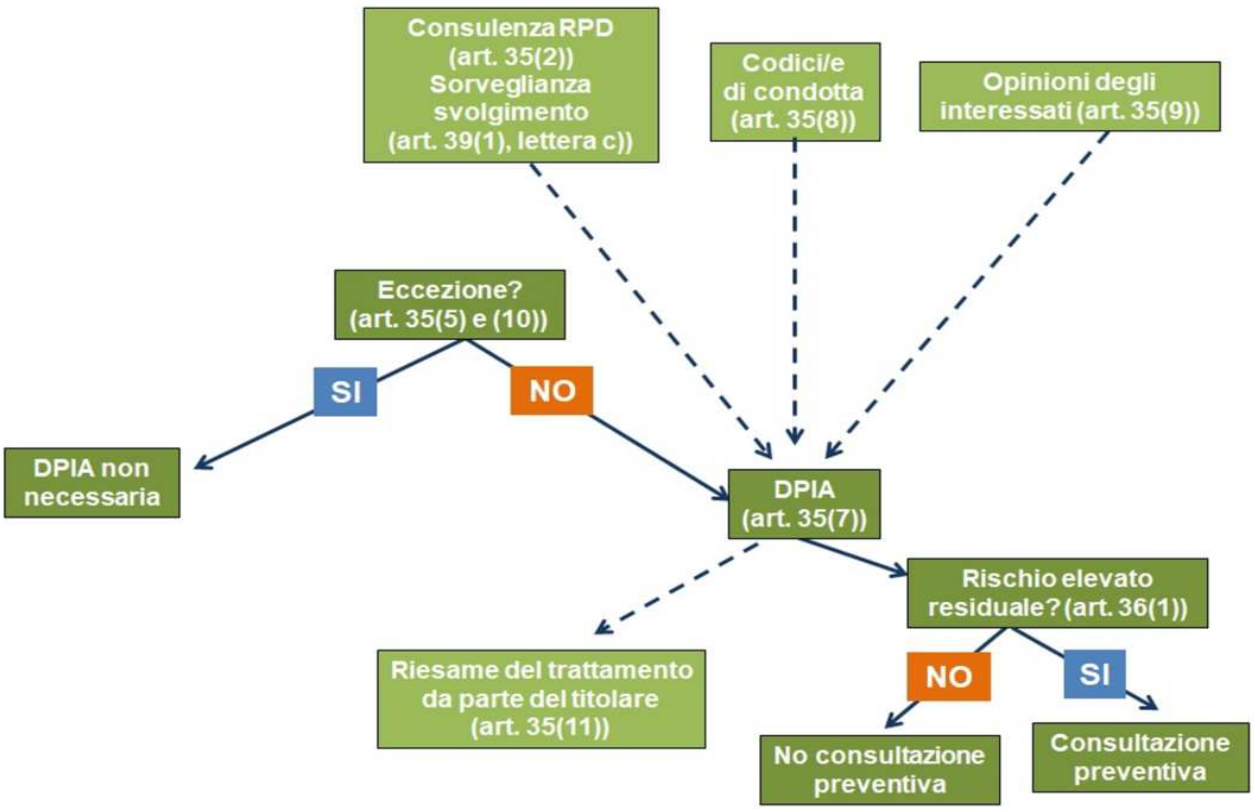
Data	Descrizione	Stato
04/10/2023	Prima versione della Procedura	Determina Dirigente Area IV in veste di Delegato del Titolare n. 275 del 4.10.2023

FASI DEL PROCESSO

La procedura di valutazione, preliminare alla DPIA, può riassumersi nelle fasi di seguito rappresentate.



Lo svolgimento della DPIA può riassumersi nelle ulteriori fasi di seguito rappresentate.



VALUTAZIONI PRELIMINARI IN ORDINE ALL'EFFETTUAZIONE DELLA DPIA

In linea con l'approccio basato sul rischio adottato dal GDPR, non è obbligatorio svolgere una DPIA per ciascun trattamento. È, infatti, necessario realizzare una DPIA soltanto quando la tipologia di trattamento "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (art. 35, par. 1, GDPR).

Ne consegue che, al fine di poter stabilire se, per un dato trattamento o per un insieme di trattamenti, risulta necessaria l'effettuazione di una DPIA, occorre effettuare preliminarmente le tre valutazioni di cui ai successivi paragrafi.

DPIA OBBLIGATORIA AI SENSI DEL PROVVEDIMENTO DEL GARANTE

Il Garante per la protezione dei dati personali **ha provveduto ad individuare, con Provvedimento 11 ottobre 2018, n° 467, l'elenco delle tipologie di trattamenti da sottoporre a valutazione d'impatto**. I trattamenti ivi elencati debbono pertanto essere considerati a priori quali potenzialmente comportanti un rischio elevato per i diritti e le libertà delle persone fisiche.

I trattamenti in questione sono i seguenti:

1.	Trattamenti valutativi o di *scoring* su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché 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.
2.	Trattamenti automatizzati finalizzati 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.	Trattamenti che prevedono 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 di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini 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. effettuati 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.
4.	Trattamenti 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).
5.	Trattamenti effettuati 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).
6.	Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
7.	Trattamenti effettuati 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*) ogni qualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01.
8.	Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
9.	Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. *mobile payment*).

10.	Trattamenti 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.
11.	Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12.	Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

CRITERI DI VALUTAZIONE FISSATI DALLA WP248

Per procedere all'identificazione dei trattamenti che possono presentare un "rischio elevato", la WP248 del Gruppo di lavoro *ex* art. 29 - *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679* - ha individuato i seguenti nove criteri:

1.	**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" (considerando 71 e 91). Esempi di ciò potrebbero includere: un ente finanziario che esamina i suoi clienti rispetto a una banca dati di riferimento in materia di crediti oppure rispetto a una banca dati in materia di lotta contro il riciclaggio e il finanziamento del terrorismo (AML/CTF) oppure contenente informazioni sulle frodi; oppure un'impresa di biotecnologie che offre test genetici direttamente ai consumatori per valutare e prevedere i rischi di malattia o per la salute; oppure un'impresa che crea profili comportamentali o per la commercializzazione basati sull'utilizzo del proprio sito web o sulla navigazione sullo stesso.
2.	**Processo decisionale automatizzato che 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" (articolo 35, paragrafo 3, lettera a). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti delle persone. Il trattamento che non ha effetto o ha soltanto un effetto limitato sulle persone non risponde a questo criterio specifico. Ulteriori spiegazioni in merito a queste nozioni saranno fornite nelle linee guida sulla profilazione che saranno pubblicate prossimamente dal WP29.
3.	**Monitoraggio sistematico**: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" (articolo 35, paragrafo 3, lettera c). Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico).
4.	**Dati sensibili o dati aventi carattere altamente personale**: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10. Un esempio potrebbe essere quello di un ospedale generale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli dei trasgressori. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali documenti personali,

	messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone.
5.	**Trattamento di dati su larga scala**: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. Ad ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala: a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; c. la durata, ovvero la persistenza, dell'attività di trattamento; d. la portata geografica dell'attività di trattamento.
6.	**Creazione di corrispondenze o combinazione di insiemi di dati**, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato.
7.	**Dati relativi a interessati vulnerabili** (considerando 75): il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento.
8.	**Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative**, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc. Il regolamento generale sulla protezione dei dati chiarisce (articolo 35, paragrafo 1 e considerando 89 e 91) che l'uso di una nuova tecnologia, definita "in conformità con il grado di conoscenze tecnologiche raggiunto" (considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi. Ad esempio, alcune applicazioni di "Internet delle cose" potrebbero avere un impatto significativo sulla vita quotidiana e sulla vita privata delle persone e, di conseguenza, richiedono la realizzazione di una valutazione d'impatto sulla protezione dei dati.
9.	Quando **il trattamento in sé** "**impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto**" (articolo 22 e considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto. Un esempio di ciò è rappresentato dal caso in cui una banca esamina i suoi clienti rispetto a una banca dati di riferimento per il credito al fine di decidere se offrire loro un prestito o meno.

Il ricorrere di due o più dei predetti criteri è indice di un trattamento che presenta un rischio elevato per i diritti e le libertà degli interessati e per il quale è quindi richiesta una DPIA. Ciò nonostante, un Titolare può ritenere che un trattamento che soddisfa soltanto uno di questi criteri richieda una DPIA.

Per contro, un trattamento può corrispondere ai casi di cui sopra ed essere comunque considerato dal Titolare un trattamento tale da non "*presentare un rischio elevato*". In tali casi il Titolare deve giustificare e documentare i motivi che lo hanno spinto a non effettuare una valutazione d'impatto sulla protezione dei dati, nonché includere/registrare i punti di vista del DPO (RPD).

INDIVIDUAZIONE DEGLI ULTERIORI TRATTAMENTI CHE PRESENTANO UN RISCHIO ELEVATO

Anche al di fuori delle ipotesi dei paragrafi che precedono, possono comunque sussistere trattamenti che presentano un rischio elevato per i diritti e le libertà delle persone fisiche e che, di conseguenza, richiedono lo svolgimento di una DPIA.
Al fine di individuare tali trattamenti, è necessario procedere ad una valutazione dei rischi ad essi connessi che tenga in considerazione **PROBABILITÀ** di accadimento di una violazione dei dati personali e **GRAVITÀ** dei possibili impatti sugli Interessati, da valutarsi separatamente, per ciascun trattamento, su riservatezza, integrità e disponibilità del dato.
Al fine di poter effettuare detta valutazione, è preliminarmente indispensabile che l'Ente abbia svolto una approfondita analisi dei processi di trattamento operati, da cui trarre le informazioni qui necessarie.

PROBABILITÀ DI ACCADIMENTO

Il Referente *privacy*, di concerto con i Dirigenti dell'Ente e con il supporto dell'Amministratore di sistema interno, procederà alla valutazione della PROBABILITÀ considerando le misure di sicurezza tecniche, organizzative e fisiche adottate dall'Ente, nonché il loro livello di implementazione e di adeguatezza.

In particolare, dovrà valutarsi l'esistenza e l'effettivo livello di implementazione almeno delle seguenti misure:

	Misura	Breve descrizione della misura
Sicurezza tecnica	Gestione *asset* informatici	Esistenza e aggiornamento costante di un registro/ censimento delle risorse e degli apparati IT utilizzati per il trattamento dei dati personali (*hw*, *sw* e rete)
	Gestione modifiche autorizzazioni informatiche	In caso di riorganizzazioni interne o di dismissione di personale o assegnazione ad altro ruolo, l'organizzazione deve prevedere una procedura chiaramente definita per la revoca dei diritti, delle responsabilità e dei profili di autorizzazione e la conseguente riconsegna di materiali e strumenti.
	Gestione e controllo accessi logici e sistema di autenticazione	Esistenza di un sistema di controllo degli accessi applicabile a tutti gli utenti che accedono al sistema IT. Per l'accesso al sistema IT, dovrebbero essere implementate procedure di autenticazione almeno a due fattori (combinazione di nome utente e *password*). Il sistema dovrebbe accettare unicamente *password* con un adeguato livello di complessità. I diritti specifici dovrebbero essere assegnati a ciascun ruolo in base al principio di necessità.
	Antivirus	Presenza di *antivirus* su tutti i dispositivi in uso presso l'Ente (*device* mobili compresi)
	Gestione aggiornamenti applicativi	Gli aggiornamenti critici di sicurezza rilasciati dallo sviluppatore del sistema operativo devono essere installati regolarmente. Gli utenti non dovrebbero essere in grado di disattivare o *bypassare* le impostazioni di sicurezza.
	Sicurezza della rete/ connessioni	Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite idonei protocolli (TLS / SSL).
	Sicurezza del server	I server ove risiedono database e applicazioni devono essere configurati per essere operativi utilizzando un account separato, con i privilegi minimi. Dovrebbero essere adottate idonee misure di crittografia dei dati (*at rest*) e dei dati in transito
	Sicurezza delle postazioni di lavoro	Come minimo, gli utenti non dovrebbero avere i privilegi per installare o disattivare applicazioni software senza autorizzazione. Il sistema dovrebbe attivare il *timeout* di sessione quando l'utente non

		è stato attivo per un certo periodo di tempo.
	Gestione dismissione apparecchiature informatiche	Devono essere definite procedure per la dismissione sicura delle apparecchiature informatiche a fine vita.
	Gestione Log Amministratori di Sistema	Le attività degli amministratori di Sistema devono essere registrate tramite log conservati nel rispetto delle prescrizioni di cui al Provvedimento del Garante del 27 novembre 2008.
	Back-Up e Re-Store	Le procedure di *backup* e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità. L'esecuzione dei *backup* deve essere monitorata per garantirne la completezza. I *backup* completi devono essere eseguiti regolarmente. Le copie del *backup* devono essere conservate in modo sicuro in luoghi diversi.
	Business continuity	L'Ente deve definire le procedure ed i controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema IT mediante il quale si procede al trattamento dei dati personali (in caso di incidente / violazione di dati personali).
	Disaster recovery	Devono essere definiti requisiti per la sicurezza delle informazioni e per la continuità della gestione della sicurezza delle informazioni in seguito a eventi disastrosi.
Sicurezza organizzativa	Definizione ruoli e responsabilità interne	I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con le politiche di sicurezza.
	Gestione modifiche autorizzazioni	cfr. voce presente in misure tecniche.
	Obblighi riservatezza del personale	L'Ente deve garantire che tutti i dipendenti, lavoratori e persone autorizzate al trattamento comprendano le proprie responsabilità e gli obblighi di riservatezza sui dati personali oggetto del trattamento da essi svolto.
	Gestione cessazione rapporto di lavoro	L'Ente provvede a disattivare tutti gli account connessi al personale cessato e a farsi restituire eventuali supporti mobili, documenti etc, contenenti dati personali
	Procedure per la gestione *data breach*	L'Ente deve dotarsi di una procedura che disciplina ruoli e regole per la gestione di una violazione di dati personali (c.d. *data breach*).
	Policy utilizzo sistemi informativi aziendali	L'Ente dovrebbe dotarsi di regole e procedure interne per l'utilizzo dei sistemi informativi e aggiornarle periodicamente.
	Formazione del personale dipendente	L'Ente dovrebbe assicurare formazione continua a tutto il personale dipendente sia sulle tematiche privacy sia sulle specifiche misure di sicurezza (tecniche ed organizzative) adottate.
	Gestione Responsabili del trattamento (selezione, nomina, obblighi contrattuali)	I responsabili del trattamento devono essere scelti sulla base di criteri di affidabilità. Il rapporto con i responsabili del trattamento deve essere disciplinato da un atto/nomina contenente almeno i requisiti di cui all'art. 28 GDPR.
Sicurezza fisica	Controllo e gestione accessi fisici	Dovrebbero essere disciplinate e controllate le modalità di accesso ai locali dell'Ente da parte di: dipendenti/fornitori/manutentori/ visitatori /ospiti/utenti. Adozione di misure quali: servizio di portierato; sistemi di videosorveglianza; sistemi di allarme, etc...
	Sistemi antincendio	Dovrebbero essere predisposto un sistema antincendio e idonee procedure per il loro controllo e manutenzione.

	Sicurezza archivi cartacei (es. armadi, casseforti, etc)	L'accesso agli archivi cartacei dovrebbe essere regolamentato e selezionato. Dovrebbero essere predisposte idonee misure volte a evitare eventi distruttivi quali allagamenti e incendi. Gli archivi cartacei dovrebbero avere almeno le seguenti dotazioni di sicurezza: chiavi (in caso di locali/armadi/cassettiere,etc) non direttamente accessibili a terzi.

La valutazione della probabilità dovrà essere svolta sulla base della seguente scala di valori:

BASSA	*È improbabile che l'evento si verifichi.*
MEDIA	*Ci sono ragionevoli probabilità che l'evento si verifichi.*
ALTA	*È molto probabile che l'evento si verifichi.*

GRAVITÀ DI ACCADIMENTO

Il Referente *Privacy*, di concerto con l'Ufficio / l'Area o gli Uffici / le Aree interessate da ciascun trattamento sottoposto a valutazione, procede quindi alla individuazione del livello di **GRAVITÀ**, considerando tipologie di dati personali trattati, volume di questi dati, operazioni effettuate, nonché categorie di soggetti Interessati.

L'Ente dovrà valutare, per ciascun trattamento, il possibile impatto sulle persone fisiche in caso di violazioni della riservatezza, dell'integrità e della disponibilità dei dati trattati.

A tal fine, l'Ente adotta la seguente scala di valutazione:

BASSO	*Gli individui possono andare incontro a disagi minori o semplici fastidi, che supereranno senza alcun problema.*
MEDIO	*Gli individui possono andare incontro a significativi disagi, che supereranno con alcune difficoltà (es. costi aggiuntivi).*
ALTO	*Gli individui possono andare incontro a conseguenze rilevanti che dovrebbero essere in grado di superare con gravi difficoltà (es. danni economici rilevanti).*
MOLTO ALTO	*Gli individui possono subire conseguenze irreversibili o che non sono in grado di superare (es. danni psicologici).*

Di tutti i valori risultanti dalla valutazione, l'Ente terrà in considerazione il solo valore più alto, corrispondente al valore globale di GRAVITÀ (riferibile sempre alla scala di cui sopra).

RISCHIO

Si potrà dunque procedere alla valutazione complessiva del **RISCHIO**, incrociando i valori globali di PROBABILITÀ e di GRAVITÀ così ottenuti, in una matrice tre per tre (3x3):

		VALORE GLOBALE DI GRAVITÀ		
		BASSO	MEDIO	ALTO / MOLTO ALTO
VALORE GLOBALE DI PROBABILITÀ	BASSO			
	MEDIO			
	ALTO			

Il trattamento risulterà dunque cadere in una delle 9 celle colorate:

- in caso di collocazione in una cella rossa, la DPIA risulterà necessaria e dovrà dunque essere condotta;
- in casi di collocazione in una delle 3 celle gialle, pur non risultando necessario effettuare una DPIA, l'Ente dovrà interrogarsi sulla necessità di implementare le misure di sicurezza sino a questo momento adottate, ripetendo almeno ogni 2 anni la valutazione del rischio;
-in caso di collocazione in una delle due celle verdi, la DPIA non sarà necessaria, ma l'Ente dovrà ripetere la valutazione del rischio periodicamente, e comunque ogni 2 anni

Ciò in quanto, come evidenziato dalle Linee guida WP248, "*i Titolari del trattamento devono continuamente valutare i rischi creati dalle loro attività al fine di stabilire quando una tipologia di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche*".
I valori globali di probabilità e di gravità, nonché il valore complessivo del rischio individuato per ciascun trattamento, unitamente alla data di effettuazione dell'ultima valutazione, vengono indicati nel **Registro delle attività di trattamento** dell'Ente.
La documentazione attestante la conduzione della valutazione del rischio e i parametri tenuti in considerazione viene conservata ai fini di *accountability* con allegazione della stessa al Registro.

AVVIO DELLA DPIA – CONSIDERAZIONI PRELIMINARI

L'elenco dei trattamenti da sottoporre a DPIA risultante dalla valutazione di cui ai paragrafi che precedono, dovrà essere rimesso all'attenzione del DPO /RPD affinchè possa formulare eventuali osservazioni e indicare, se del caso, ulteriori trattamenti che necessitano di essere sottoposti a DPIA.
Il parere reso dal DPO /RPD è obbligatorio ma non vincolante. Il Referente interno ne darà pronta comunicazione al Delegato del Titolare e ai Dirigenti dell'Ufficio / Area coinvolta e, ove questi ritengano di discostarsene, documenteranno le motivazioni di tale decisione in apposito documento di *accountability*.
Appurata la necessità di effettuare una DPIA, occorre svolgere due ulteriori considerazioni preliminari, prima di dare avvio alla stessa.

SINGOLO TRATTAMENTO O INSIEME DI TRATTAMENTI

La prima considerazione riguarda la possibilità di effettuare una DPIA non solo su singole operazioni di trattamento dei dati, bensì anche su un insieme di trattamenti, purché gli stessi siano simili e presentino rischi elevati analoghi. Per esempio, è ipotizzabile un'unica DPIA "*quando autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni o quando diversi Titolari del trattamento progettano di introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata*" (considerando 92 GDPR).
Al fine di poter procedere ad un'unica DPIA è tuttavia necessario che i trattamenti multipli presi in considerazione siano simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. Si pensi ad esempio all'utilizzo di una tecnologia simile per raccogliere la medesima tipologia di dati personali e per le medesime finalità, anche laddove i Titolari siano diversi, oppure alla videosorveglianza effettuata presso sedi diverse del medesimo Ente: in tutti questi casi è possibile valutare se risulta opportuno effettuare un'unica DPIA.
Laddove si proceda in tal senso, sarà necessario fornire una giustificazione della scelta di realizzare una singola DPIA.
Qualora il trattamento coinvolga diversi soggetti che operano quali Contitolari, questi ultimi devono aver preliminarmente definito con precisione le rispettive competenze nonché gli obblighi spettanti a ciascuno.

ECCEZIONI EX ART. 35 GDPR

Inoltre, ai sensi dell'art. 35 GDPR, il Garante per la protezione dei dati personali può "*redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati*".
L'Ente dovrà, pertanto, verificare periodicamente le indicazioni fornite sul punto dall'Autorità Garante per la protezione dei dati personali. **Allo stato non risulta che il Garante abbia pubblicato un elenco delle tipologie di trattamenti per i quali risulti esclusa la DPIA**.

SOGGETTI CHE EFFETTUANO E INTERVENGONO NELLA DPIA

L'art. 35 GDPR prevede che la DPIA debba essere effettuata dal **Titolare del trattamento** (art. 35, par. 1 e Considerando 84).

Ove le caratteristiche del trattamento oggetto della DPIA richiedano competenze specialistiche, il Titolare può avvalersi della consulenza di soggetti esterni, ferma restando la sua responsabilità in ordine allo svolgimento della DPIA in tutte le sue fasi.

Qualora la DPIA riguardi trattamenti svolti in tutto o in parte da un Responsabile del trattamento, quest'ultimo - conformemente alle previsioni di cui all'articolo 28, paragrafo 3, lettera f) GDPR e agli obblighi contrattualmente assunti - è tenuto ad assistere il Titolare nell'esecuzione della valutazione d'impatto e a fornire tutte le informazioni a tal fine necessarie.

In base alla specificità del trattamento da esaminare, l'Ente definirà i ruoli e responsabilità interne per lo svolgimento di ciascuna DPIA (Autore/Inseritore; Revisore; DPO (RPD); Interessati; Validatore)

CONTENUTI ESSENZIALI DELLA DPIA

Il GDPR definisce le caratteristiche e i contenuti essenziali di una valutazione d'impatto sulla protezione dei dati. In particolare l'articolo 35, paragrafo 7, e i considerando 84 e 90 prevedono che la valutazione d'impatto debba contenere almeno tutti i seguenti elementi:

- "una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso ove applicabile, l'interesse legittimo perseguito dal Titolare";
- "una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità";
- "una valutazione dei rischi per i diritti e le libertà degli interessati";
- "le misure previste per: affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione".

DESCRIZIONE DEL TRATTAMENTO

Il primo elemento di valutazione richiesto dall'art. 35, par. 7 GDPR ha carattere descrittivo, essendo teso a rappresentare in modo dettagliato e puntuale il trattamento oggetto della DPIA nel suo insieme.

Nello specifico, occorrerà indicare il nome/ codifica del trattamento, le sue principali caratteristiche, le finalità così come individuate nel Registro/Analisi dei trattamenti e l'eventuale processo nell'ambito del quale si inserisce il trattamento oggetto della DPIA.

L'Ente dovrà, poi, descrivere i soggetti coinvolti nel trattamento definendone ruoli e responsabilità: dovrà pertanto indicare se è l'unico Titolare o se agisce in rapporto di Contitolarità. Dovranno essere elencati gli eventuali Responsabili nominati ai sensi dell'art. 28 GDPR a cui il trattamento medesimo viene affidato in tutto o in parte, nonché i soggetti autorizzati/designati che hanno accesso ai dati.

L'Ente, infine, dovrà fornire ulteriori elementi di dettaglio in ordine al trattamento, utili al fine di valutare il rischio connesso e, in particolare:

- l'indicazione delle categorie dei dati trattati (dati comuni/particolari categorie di dati/dati relativi a condanne penali e reati), con una sommaria descrizione degli stessi;
- l'indicazione della *data retention* per ciascuna finalità indicata;
- l'indicazione degli eventuali destinatari dei dati con specifico riferimento ad eventuali ulteriori Titolari Autonomi che intervengano nel trattamento oggetto della DPIA;
- la descrizione del ciclo di vita dei dati trattati (dalla raccolta alla distruzione, passando per la loro conservazione, i vari step del trattamento, l'archiviazione, ecc.);
- l'indicazione delle modalità e dei principali mezzi impiegati per il trattamento (in via meramente esemplificativa: hardware, software, reti, supporti cartacei, etc).
-

NECESSITÀ' E PROPORZIONALITÀ'

L'Ente, descritto il trattamento, dovrà procedere a valutarne **necessità** e **proporzionalità** in relazione alle finalità perseguite e indicate.

A tal fine, l'Ente dovrà tenere in considerazione i criteri individuati dall'Allegato 2 della WP 248 /2017.

Segnatamente, l'Ente dovrà indicare, motivando le scelte operate:

1) se le finalità del trattamento sono determinate, esplicite e legittime (articolo 5, par. 1, lett. *b*) GDPR);
2) su quali basi giuridiche fonda il trattamento (artt. 6, 9 e 10 GDPR);
3) in che modo il trattamento è conforme al principio di minimizzazione, prestando attenzione a: quantità di dati raccolti, tipologia, stretta necessità rispetto agli obiettivi/ finalità del trattamento (articolo 5, par. 1, lett. *c*) GDPR;
4) in che modo l'Ente garantisce che i dati personali siano esatti e aggiornati indicando, altresì, le misure adottate a tal fine;
5) il tempo di *data retention* e le ragioni per le quali si ritiene che tale periodo sia necessario al raggiungimento delle specifiche finalità indicate (articolo 5, par. 1, lett. *e*) GDPR).

L'Ente è altresì tenuto a valutare le misure adottate al fine di garantire, in ossequio al principio di trasparenza, i diritti degli interessati previsti dal Regolamento, indicando:

a) modalità con le quali vengono fornite le informazioni all'interessato (artt. 12, 13 e 14 GDPR);
b) modalità / procedure per l'esercizio dei diritti da parte degli interessati:
    - diritto di accesso e portabilità dei dati (artt. 15 e 20 GDPR);
    - diritto di rettifica e alla cancellazione (artt. 16, 17 e 19 GDPR);
    - diritto di opposizione e di limitazione di trattamento (artt. 18, 19 e 21 GDPR);
    - revoca del consenso inizialmente prestato (ove il trattamento fondi su tale base giuridica);
c) per ogni Responsabile del trattamento i riferimenti alle clausole contrattuali che delimitano l'ambito delle rispettive responsabilità e disciplinano gli obblighi incombenti per la protezione dei dati personali (art. 28 GDPR);
d) se i dati sono trasferiti verso paesi terzi o organizzazioni internazionali e in caso affermativo i fondamenti di legittimità su cui poggia detto trasferimento (capo V artt. 44 e ss. GDPR).

MISURE

L'Ente dovrà individuare e descrivere tutte le misure tecniche ed organizzative implementate o di cui abbia programmato l'adozione per affrontare/mitigare i rischi per i diritti e le libertà delle persone fisiche.

A tale proposito, in caso di trattamento effettuato da un **Responsabile del trattamento**, l'Ente dovrà acquisire da quest'ultimo le informazioni necessarie a valutare l'adeguatezza delle misure tecniche e organizzative adottate.

Tale passaggio è necessario per la successiva fase della DPIA: la valutazione dei rischi effettivi deve infatti essere svolta anche considerando le misure esistenti o pianificate.

ACCESSO- MODIFICA- PERDITA DEI DATI

L'Ente dovrà quindi procedere, sulla base delle informazioni e delle valutazioni ottenute all'esito delle analisi di cui ai paragrafi precedenti, alla valutazione dei possibili impatti per i diritti e le libertà degli interessati da effettuarsi separatamente per le ipotesi di accesso illegittimo (RISERVATEZZA), modifiche indesiderate (INTEGRITÀ) e perdita dei dati stessi (DISPONIBILITÀ).

In particolare, l'Ente per ciascun ambito di rischio sopra delineato dovrà analizzare ed indicare:

- i potenziali impatti (le ricadute pregiudizievoli) per i diritti e le libertà delle persone fisiche;
- le minacce che possono concretizzare il rischio (ove per minaccia si intende la modalità operativa comprendente una o più azioni individuali sulle risorse che supportano i dati);
- le fonti di rischio umane (persona, interna o esterna all'Ente, che opera in via accidentale o intenzionale ad esempio: amministratore IT, utente, attaccante esterno, concorrente, etc.) o non umane (fenomeni metereologici, materiali infiammabili o pericolosi, virus informatici, etc.) che possono essere all'origine del rischio;
- le misure tra quelle implementate o programmate dall'Ente che possono contribuire fattivamente alla mitigazione di ciascun rischio.

Definiti i potenziali impatti, la loro origine e le misure volte a mitigare il rischio, l'Ente dovrà stimare la probabilità e la gravità degli stessi in relazione a ciascun ambito di rischio.
A tal fine e con riguardo alla GRAVITÀ, l'Ente adotta la medesima scala di valori utilizzata nella valutazione preliminare del rischio e che qui di seguito si riporta per praticità:

BASSO / TRASCURABILE	*Gli individui possono andare incontro a disagi minori o semplici fastidi, che supereranno senza alcun problema.*
MEDIO / LIMITATO	*Gli individui possono andare incontro a significativi disagi, che supereranno con alcune difficoltà*
ALTO / IMPORTANTE	*Gli individui possono andare incontro a conseguenze rilevanti che dovrebbero essere in grado di superare con gravi difficoltà.*
MOLTO ALTO / MASSIMO	*Gli individui possono subire conseguenze irreversibili o che non sono in grado di superare.*

Per quanto concerne, invece la PROBABILITÀ, l'Ente adotta la seguente griglia di valutazione:

BASSO / TRASCURABILE	*Appare impossibile che le fonti di rischio considerate concretizzino una minaccia considerate le misure tecniche ed organizzative adottate*
MEDIO / LIMITATO	*Appare difficile che le fonti di rischio considerate concretizzino una minaccia considerate le misure tecniche ed organizzative adottate*
ALTO / IMPORTANTE	*Appare possibile che le fonti di rischio considerate concretizzino una minaccia considerate le misure tecniche ed organizzative adottate*
MOLTO ALTO / MASSIMO	*Appare molto probabile che le fonti di rischio considerate concretizzino una minaccia considerate le misure tecniche ed organizzative adottate*

REVISIONE

Una volta completata l'attività di inserimento delle informazioni di cui ai paragrafi che precedono, il Revisore provvede a verificare l'operato dell'Autore / Inseritore, individuando le necessarie modifiche da apportare alle informazioni inserite. Il Revisore dovrà inoltre individuare le eventuali misure correttive che l'Ente dovrà adottare al fine di mitigare il rischio e definire il relativo piano di azione con l'indicazione delle tempistiche e delle responsabilità connesse per l'implementazione delle stesse.
Il Revisore dovrà procedere anche alla valutazione delle misure adottate e del rischio residuo, per ciascun ambito di rischio (RISERVATEZZA, INTEGRITÀ e DISPONIBILITÀ), dell'attività di trattamento oggetto della DPIA.

La combinazione dei valori di GRAVITÀ e PROBABILITÀ individuati restituirà la soglia di rischio effettivo secondo la seguente matrice di valutazione:

PROBABILITÀ					
	MOLTO ALTO/ MASSIMO	MEDIO	ALTO	MOLTO ALTO	MOLTO ALTO
	ALTO / IMPORTANTE	BASSO	MEDIO	ALTO	MOLTO ALTO
	MEDIO /LIMITATO	BASSO	MEDIO	MEDIO	ALTO
	BASSO / TRASCURABILE	BASSO	BASSO	BASSO	MEDIO
		BASSO / TRASCURABILE	MEDIO /LIMITATO	ALTO / IMPORTANTE	MOLTO ALTO/ MASSIMO

GRAVITÀ

Dove il Rischio residuo sarà così calcolato:

BASSO	RISCHIO ACCETTABILE - MISURE CORRETTIVE DA PROGRAMMARE E ATTUARE SENZA URGENZA
MEDIO	RISCHIO ACCETTABILE - MISURE CORRETTIVE DA ATTUARE NEL BREVE O MEDIO TERMINE
ALTO	RISCHIO NON ACCETTABILE - L'ENTE NON POTRÀ INIZIARE L'ATTIVITÀ DI TRATTAMENTO SENZA PRIMA AVER IMPLEMENTATO LE MISURE CORRETTIVE INDIVIDUATE. DOVRÀ COMUNQUE PROCEDERE AD UNA NUOVA ANALISI PER VERIFICARE SE IL RISCHIO RESIDUO DOPO L'IMPLEMENTAZIONE DELLE MISURE RIMANE NON ACCETTABILE E, IN QUESTO CASO, PROCEDERE ALLA CONSULTAZIONE PREVENTIVA EX ART. 36 GDPR.
MOLTO ALTO	RISCHIO NON ACCETTABILE –L'ENTE NON POTRÀ INIZIARE L'ATTIVITÀ DI TRATTAMENTO E DOVRÀ PROCEDERE ALLA CONSULTAZIONE PREVENTIVA AI SENSI DELL'ART. 36 GDPR

PARERE DEL DPO /RPD

L'Ente, nel corso di tutte le fasi della DPIA, può sempre interpellare il proprio DPO /RDP che assiste e sorveglia lo svolgimento della DPIA stessa.

L'Ente, dopo l'intervento del Revisore, dovrà ottenere il parere obbligatorio (ma non vincolante) del DPO / RPD.

Il DPO /RPD renderà quindi per iscritto il proprio parere, se del caso, formulando eventuali osservazioni.

Tale Parere dovrà essere allegato o comunque documentato all'interno della DPIA.

CONSULTAZIONE DEGLI INTERESSATI

L'Ente deve, se del caso, "*raccoglie[re] le opinioni degli interessati o dei loro rappresentanti*" (articolo 35, paragrafo 9).

"*Tali opinioni possono essere raccolte attraverso una varietà di mezzi, a seconda del contesto (ad esempio uno studio generico relativo alla finalità e ai mezzi del trattamento, una domanda posta ai rappresentanti del personale oppure indagini abituali inviate ai futuri clienti del Titolare del trattamento)*" (Wp 248/17).

L'Ente dovrà, quindi, valutare se risulti necessario consultare gli interessati e, in caso contrario, documentare la propria scelta in apposito documento di *accountability* da allegare alla DPIA.

Qualora ritenga necessario procedere alla consultazione, l'Ente, nel rispetto del principio di minimizzazione, dovrà valutare le modalità più opportune per lo svolgimento della stessa, tenendo in considerazione che ogni ulteriore trattamento di dati deve essere sorretto da idonea base giuridica.

VALIDAZIONE

Il Delegato del Titolare / Dirigente dell'Ufficio Area Interessata, valutati il parere del DPO /RPD e l'esito dell'eventuale consultazione degli Interessati, valida ed approva formalmente le misure di sicurezza tecniche ed organizzative prescelte, la soglia di accettabilità dei rischi residui nonché il piano di azione indicato.

Al fine di determinare l'esito finale della DPIA dovrà tenersi in considerazione il valore di rischio più alto tra quelli emersi per i tre ambiti di rischio Riservatezza, Disponibilità, Integrità.

Gli esiti delle valutazioni e delle analisi svolte nel corso della DPIA possono essere i seguenti:

A) **ACCETTABILE:** se il valore del rischio rientra nella soglia di accettabilità il trattamento potrà essere iniziato / continuato e le misure correttive implementate senza urgenza, nel caso il valore di rischio sia basso, e con urgenza o comunque nel breve / medio termine ove il valore di rischio risulti medio;

B) **NON ACCETTABILE:** se il valore del rischio risulti alto, quindi superiore alla soglia di accettabilità, il trattamento potrà essere avviato / proseguito solo dopo aver implementato le misure correttive individuate. In tal caso il valore di rischio dovrà essere ricalcolato (svolgendo una nuova DPIA) a seguito dell'implementazione delle misure correttive stesse. Ove anche dopo tale implementazione il rischio permanga alto, prima di iniziare l'attività di trattamento il Titolare dovrà avviare la consultazione preventiva ex art. 36 GDPR;

C) **NECESSARIA CONSULTAZIONE PREVENTIVA:** ove il valore di rischio risulti Molto Alto, il Titolare prima di avviare il trattamento, dovrà consultare il Garante, ai sensi dell'art. 36 GDPR, seguendo la procedura di seguito indicata. Tale adempimento deve essere considerato parte integrante del processo di DPIA.
Alternativamente, il Titolare potrà semplicemente scegliere di non iniziare o di non continuare il trattamento in questione.

CONSULTAZIONE PREVENTIVA

Qualora l'esito della valutazione d'impatto restituisca, anche dopo l'eventuale adozione di misure correttive, un livello di rischio superiore alla soglia di accettabilità, il Titolare del trattamento - non avendo individuato misure idonee e sufficienti ad attenuare il rischio – dovrà procedere alla consultazione preventiva del Garante ai sensi dell'art 36 GDPR.

Il Delegato del Titolare / in collaborazione con il Referente Privacy interno e sentito il DPO avvia la fase di consultazione preventiva procedendo all'invio della richiesta al Garante.

Come previsto all'art. 36, par. 3, GDPR, con la richiesta di consultazione preventiva devono essere comunicati al Garante almeno i seguenti elementi:

a. ove applicabile, le rispettive responsabilità del Titolare del trattamento, dei contitolari del trattamento e dei Responsabili del trattamento;
b. le finalità e i mezzi del trattamento previsto;
c. le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati;
d. i dati di contatto del responsabile della protezione dati;
e. la valutazione d'impatto eseguita.

Nel corso della procedura di consultazione, l'Ente dovrà fornire tempestivamente ogni altra informazione richiestagli dal Garante.

Ai sensi dell'art. 36, par. 2, GDPR il Garante, ove ravvisi che il trattamento sottoposto a consultazione violi la normativa in materia di tutela dei dati personali, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, "(…) *fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al Titolare del trattamento e, ove applicabile, al Responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della*

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

Al riguardo, l'art. 154, comma 5, D.Lgs. n. 196/2003, stabilisce che "*Fatti salvi i termini più brevi previsti per legge, il parere del Garante, anche nei casi di cui all'art. 36, par. 4, del Regolamento, è reso nel termine di quarantacinque giorni dal ricevimento della richiesta. Decorso il termine, l'amministrazione può procedere indipendentemente dall'acquisizione del parere. Quando, per esigenze istruttorie, non può essere rispettato il termine di cui al presente comma, tale termine può essere interrotto per una sola volta e il parere deve essere reso definitivamente entro venti giorni dal ricevimento degli elementi istruttori da parte delle amministrazioni interessate*".

L'Autorità Garante non avrà il compito di "*autorizzare*" il trattamento, bensì dovrà indicare al Titolare le ulteriori misure necessarie al fine di ridurre il livello del rischio ad una soglia di accettabilità e potrà, ove necessario, esercitare tutti i poteri attribuitigli dall'art. 58 GDPR: dall'ammonimento fino alla limitazione o al divieto di procedere al trattamento stesso.

Ove con il Parere del Garante, anche nell'esercizio dei poteri di cui all'art. 58 GDPR, si limiti a indicare le misure correttive da adottare, il Delegato del Titolare, in collaborazione con il Referente interno privacy e il Dirigente dell'Ufficio Area Interessata, individuerà le responsabilità per l'implementazione di tali misure e verificherà che il trattamento abbia effettivamente inizio e/o riprenda solo dopo la completa adozione delle stesse. Analogamente dovrà procedersi nel caso in cui il Garante prescriva eventuali modifiche al trattamento, assicurandosi che lo stesso non sia avviato o continuato se non in conformità alle prescrizioni impartite.

Ove il Garante, nell'esercizio dei poteri di cui all'art. 58 GDPR, imponga la limitazione provvisoria o definitiva del trattamento, l'Ente dovrà conformarvisi e quindi non procedere all'attività di trattamento.

AGGIORNAMENTO E REVISIONE PERIODICA DELLA DPIA

La DPIA non deve intendersi come un'attività da effettuarsi *una tantum*, ma è un processo che deve essere ciclicamente revisionato, tutte le volte che si renda necessario in base alle modifiche apportate all'attività di trattamento.
In via meramente esemplificativa, si indicano di seguito le principali ipotesi in cui è opportuno considerare una revisione della DPIA:

1) **Cambiamento sulle attività di trattamento**, in termini di:
   - contesto;
   - finalità del trattamento;
   - tipologia di dati personali trattati;
   - destinatari (ad eccezione di quelli che rientrano nella definizione di «terzo» ai sensi dell'art. 4, num. 10, del GDPR);
   - modalità di raccolta dei dati personali;
   - trasferimento di dati all'estero.

2) **Modifica ai rischi con impatto sui diritti degli interessati** derivati da:
   - presenza di nuove minacce;
   - variazione dei sistemi informativi a supporto del trattamento;
   - nuove ipotesi di danno per gli interessati;
   - variazione delle misure di sicurezza tecniche ed organizzative applicate ai trattamenti.

3) **Modifica delle modalità attraverso cui gli interessati possono esercitare i loro diritti**