AUTOMOBILE CLUB *BOLOGNA*

REGOLAMENTO sulla Metodologia per la

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI
Data Protection Impact Assessment - DPIA
(Regolamento UE 679/2016)

Approvato con Delibera del Consiglio Direttivo n.33 del 27 ottobre 2021

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI
Data Protection Impact Assessment - DPIA
(Regolamento UE 679/2016)

METODOLOGIA

PREMESSA E RIFERIMENTI NORMATIVI

Il presente documento descrive la metodologia adottata **dall'Automobile Club Bologna**, di seguito AC, per effettuare la valutazione d'impatto sulla protezione dati personali connessi ai trattamenti posti in essere in qualità di Titolare così come previsto dall'art. 35 del Regolamento EU n.679/2016 (GDPR).

Per valutazione d'impatto sulla protezione dei dati personali si intende il processo inteso 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 stesso, valutando detti rischi e determinando le misure per affrontarli.

Le principali fonti normative utilizzate per la redazione del presente documento sono:

- ✔ Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR);
- ✔ D.lgs. n.101 del 10 agosto 2018 recante *disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016* che ha modificato il D.lgs. n.196 del 30 giugno 2003 (Codice Privacy);
- ✔ Software PIA – Valutazione d'impatto sulla protezione dei dati: software creato dall'autorità francese per la protezione dei dati personali (CNIL) allo scopo di guidare i Titolari del trattamento dei dati personali nell'adempimento degli obblighi prescritti dal GDPR;
- ✔ 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 - WP 248 Rev. 01;
- ✔ Provvedimento n. 467 dell'11 ottobre 2018 del Garante per la protezione dei dati personali - Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679;
- ✔ Linee guida del Garante per la protezione dei dati personali sulla "Individuazione e gestione del rischio";
- ✔ Manuale RPD - Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europea (Elaborato per il programma "T4DATA" finanziato dall'UE).

METODOLOGIA

La valutazione d'impatto in materia di protezione dei dati personali (DPIA) è uno strumento finalizzato a stimare i potenziali danni che potrebbero derivare agli interessati da una determinata attività di trattamento eseguita dal Titolare. Si tratta di uno degli elementi di maggiore rilevanza nel nuovo quadro normativo di settore, perché esprime chiaramente la responsabilizzazione (*"accountability"*) del Titolare nei confronti dei trattamenti da questi effettuati.

La valutazione d'impatto sulla protezione dei dati personali costituisce, pertanto, parte integrante della complessiva attività di trattamento, poiché è il processo inteso a garantire la conformità del trattamento alla

normativa (*"compliance"*). Il Titolare è, infatti, tenuto non soltanto ad assicurare l´osservanza delle disposizioni del GDPR, ma anche a dimostrare adeguatamente in che modo garantisce tale osservanza: la valutazione d'impatto ne è un esempio.

La DPIA si applica tanto ai nuovi trattamenti in fase di progettazione *("privacy by design")* quanto ai trattamenti che il Titolare ha già posto in essere *("privacy by default")* e riguarda, come più sopra accennato, il rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà delle persone i cui dati sono, appunto, oggetto del trattamento. La valutazione d'impatto deve essere pertanto considerata come un processo soggetto a revisione continua e non come un adempimento che il Titolare del trattamento può eseguire una volta per tutte.

In ambito AC, la valutazione d'impatto è effettuata dal Titolare del trattamento dei dati personali dell'Ente, eventualmente coadiuvato dal Responsabile della protezione dei dati o dai Referenti delegati dal Titolare ai sensi dell'art. 24 co. 1 del GDPR e dell'art. 2- quaterdecies del D.lgs. 101/2018 (Codice Privacy).

In linea con il principio di *accountability*, il Garante italiano ha chiarito che *"quando la raccolta, l´elaborazione, l´utilizzazione, la conservazione e in genere tutte le operazioni relative al trattamento dei dati vengono effettuate nell´ambito di un´amministrazione pubblica, di una società o di un ente, il titolare del trattamento è la struttura nel suo complesso e cioè il soggetto al quale competono le scelte di fondo sulla raccolta e sull´utilizzazione dei dati. Non devono, quindi, essere considerati come "titolari" le singole persone fisiche che l´amministrano o che la rappresentano"*. ("Privacy: chi sono i titolari e i responsabili del trattamento dei dati nelle imprese e nelle amministrazioni pubbliche" – Comunicato, 11 dicembre 1997).

Ciò premesso, l'AC**,** in un'ottica di omogeneità e uniformità nell'azione della Federazione ACI, ha adottato la metodologia individuata e sviluppata dall'Automobile Club d'Italia per la gestione dei rischi in materia di protezione dei dati personali in relazione alle attività di trattamento di cui stabilisce finalità e mezzi.

Tale metodologia prevede un processo DPIA composto di due fasi distinte, essenziali per individuare i rischi e gestire correttamente le risultanze della valutazione, in modo da rendere l'intero processo adattabile e aggiornabile al mutare delle condizioni e delle esigenze organizzative.

FASE 1 - VALUTAZIONE DELLA RISCHIOSITÀ NEI TRATTAMENTI DI DATI PERSONALI IN RELAZIONE AI DIRITTI E ALLE LIBERTA' DEGLI INTERESSATI.

La prima fase della metodologia DPIA adottata dall'AC consiste nel sottoporre i trattamenti di cui è Titolare ad un esame preliminare per valutare se questi presentino dei rischi per i diritti e le libertà delle persone fisiche. Tale valutazione si esplica, in primo luogo confrontando il trattamento in esame con la casistica

individuata dall'Autorità Garante nazionale (*c.d. "Questionario del Garante"*) e assoggettando successivamente il trattamento ad una ulteriore valutazione che tiene conto della probabilità che un determinato rischio si verifichi e della gravità dello stesso per i diritti degli interessati secondo i parametri individuati dal WP 248 Rev.01 nelle *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato".*

FASE 2 - GESTIONE DEI TRATTAMENTI CHE POSSONO COMPORTARE UN "RISCHIO ELEVATO" PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI – MISURE DI MITIGAZIONE.

La seconda fase della metodologia DPIA interviene qualora dall'esito di una delle due valutazioni condotte nella prima fase si evidenzi un rischio "elevato" per i diritti e le libertà dell'Interessato. L'esecuzione della seconda fase, quindi, ha lo scopo di individuare le misure tecniche, organizzative e IT più idonee per mitigare e/o abbattere il rischio rilevato.

FASE 1 – VALUTAZIONE DELLA RISCHIOSITA' NEI TRATTAMENTI DI DATI PERSONALI IN RELAZIONE AI DIRITTI E ALLE LIBERTA' DEGLI INTERESSATI

Obiettivo della FASE 1 è valutare la rischiosità dei trattamenti di cui l'AC stabilisce finalità e mezzi, ovvero dei quali ha la titolarità, e definire, sulla base di tale valutazione complessiva, se il trattamento possa comportare un *"rischio elevato per i diritti e le libertà delle persone fisiche".*

Il Referente effettua la valutazione della rischiosità di tutti quei trattamenti che non siano già stati sottoposti a verifica da parte dell'Autorità di controllo e che siano in corso di esecuzione antecedentemente a maggio 2018.

Il Referente, inoltre, effettua la valutazione del rischio ogni qualvolta si verifichi:

- ✔ l'introduzione di una nuova attività di trattamento di dati personali;
- ✔ la variazione significativa di uno dei fattori considerati nella valutazione del rischio di un determinato trattamento di dati personali.

Al fine di identificare i trattamenti che presentano un rischio elevato per gli interessati per poi eventualmente determinare la necessità di individuare nella FASE 2 le misure più idonee per mitigare e/o abbattere il rischio rilevato, per ogni trattamento in esame il Referente effettuerà:

A. una preliminare valutazione tramite la procedura informatizzata presente nel Registro elettronico dei trattamenti nella quale è riportato l'elenco delle tipologie di trattamenti da sottoporre a valutazione d'impatto così come identificate dal Garante italiano per la protezione dei dati (All.1 al Provvedimento n.467 dell'11 ottobre 2018);
B. una valutazione del rischio in termini di probabilità e gravità secondo la metodologia definita dal Titolare del trattamento e di seguito descritta, utilizzando l'apposito modello.

A) Valutazione tramite la procedura informatizzata presente nel Registro elettronico delle attività di trattamento nella quale è riportato l'elenco delle tipologie di trattamenti da sottoporre a valutazione d'impatto così come identificate dal Garante italiano per la protezione dei dati.

Nell'Allegato 1 al Provvedimento n. 467 dell'11 ottobre 2018, il Garante italiano identifica le seguenti 12 tipologie di trattamenti - qualificate come trattamenti a rischio elevato – soggette al requisito di una valutazione d'impatto ai sensi dell'art.35 co. 4 del GDPR:

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 (v. WP 248, rev. 01): 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) ogniqualvolta 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.

Il Garante italiano per la protezione dei dati personali ha fornito un chiarimento interpretativo riguardo alle espressioni trattamenti "sistematici" e "non occasionali" indicate nell'elenco ai punti 6,11 e 12 evidenziando che esse sono riconducibili al criterio della "larga scala" così come espressamente indicato al quinto criterio del WP 248 Rev.01:

"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. A 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;"

Nel medesimo chiarimento interpretativo al Provvedimento, l'Autorità ha inoltre evidenziato che il termine "dati biometrici" di cui al punto 11 dell'elenco va inteso come "dati biometrici, trattati per identificare univocamente una persona fisica".

Nell'eseguire la valutazione del rischio dell'attività di trattamento in esame, il Referente avrà cura di individuare se la stessa ricada in una o più tra le tipologie individuate dal Garante italiano spuntando la casella corrispondente del questionario posto all'interno del Registro delle attività di trattamento.

Qualora l'esito della valutazione basata sui parametri sopra descritti risulti "ALTO" (elevato), il Referente dovrà necessariamente passare alla FASE 2 partendo da un livello di rischio "ALTO" (elevato).

Il livello di probabilità iniziale "ALTO" (elevato) sarà dato nei casi in cui, alternativamente:

- ✔ il trattamento presenti le caratteristiche della prima tra le suddette tipologie di trattamento indicate dal Garante Privacy;
- ✔ il trattamento presenti le caratteristiche di almeno due delle altre 11 tipologie di trattamento indicate dal Garante Privacy;

Qualora il trattamento in esame non ricada in nessuna delle tipologie indicate nel provvedimento del Garante italiano, il Referente è comunque tenuto all'esecuzione dell'analisi del rischio nel trattamento di dati personali in termini di probabilità e gravità. Tale valutazione è effettuata sulla base della metodologia adottata dall'Ente in osservanza delle Linee guida del WP 248 REV 1., così come appresso illustrato.

B) Valutazione del rischio, in termini di probabilità e gravità, che si possa verificare un danno per gli interessati derivante dal trattamento di dati personali.

Per ogni tipologia di trattamento effettuato dall'AC in qualità di Titolare deve essere effettuata una valutazione sulla rischiosità, in termini di probabilità e gravità, che si possa verificare un danno per gli interessati derivante dal trattamento di dati personali.
Tale valutazione è eseguita dal Referente secondo la presente metodologia, come di seguito descritto, utilizzando l'apposito modello.

In questa fase il Referente valuta quali siano le fonti potenziali di rischio a cui il trattamento in esame può esporre gli interessati.

Tali fonti di rischio sono state identificate come (fig.1):

- ✔ Violazione della riservatezza: divulgazione o accesso non autorizzato ai dati;
- ✔ Modifica indesiderata dei dati: perdita di integrità o alterazione accidentale o illegale dei dati;
- ✔ Perdita o distruzione dei dati: indisponibilità causata dalla perdita o distruzione accidentale o illegale dei dati.

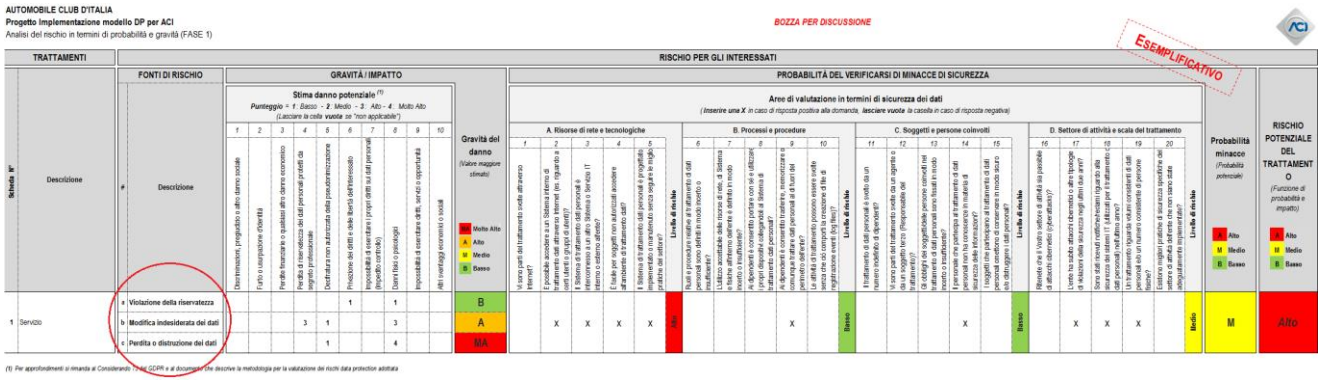


fig.1

Per ciascun trattamento indicato nel campo “Descrizione” del modello e relativa fonte di rischio è necessario (fig.2):

1) identificare primariamente la gravità del danno potenziale che potrebbe ricadere sull’Interessato, utilizzando un valore da 1 (il danno procurabile all’Interessato è basso) sino a 4 (il danno procurabile all’Interessato è molto alto);
2) successivamente, stimare la probabilità del verificarsi di minacce di sicurezza, tenuto conto delle quattro “aree di valutazione” indicate nel prospetto.

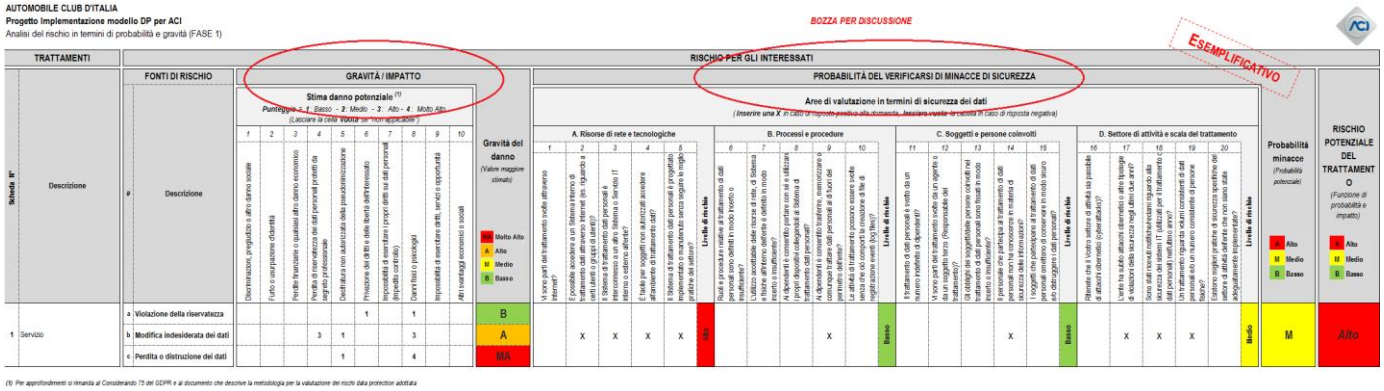


fig.2

1) Gravità del danno potenziale per gli interessati derivanti dal trattamento (GRAVITA’/IMPATTO).

La gravità del danno per gli interessati è stata individuata nei 4 livelli di impatto riportati nel seguente schema.

GRAVITA' / IMPATTO		
§	**Livello**	**Descrizione**
1	**Basso**	**Piccoli inconvenienti superabili senza particolari problemi** *(tempo necessario per re-inserire informazioni, irritazione, ecc.)*
2	**Medio**	**Conseguenze significative, superabili con alcune difficoltà** *(costi aggiuntivi, mancato accesso a servizi aziendali, timori, difficoltà di comprensione, stress, piccoli disturbi fisici, ecc.)*
3	**Alto**	**Conseguenze significative che si dovrebbero poter superare ma con gravi difficoltà** *(sottrazione di liquidità, inserimento in elenchi negativi da parte di istituti finanziari, danni a beni materiali, perdita dell’impiego, ordinanze o ingiunzioni giudiziarie, compromissione dello stato di salute, ecc.)*
4	**Molto Alto**	**Conseguenze significative o irreversibili, non superabili** *(perdita capacità lavorativa, disturbi psicologici o fisici cronici, decesso, ecc.)*

Tale valutazione deve essere effettuata per ognuna delle seguenti categorie di danni procurabili agli interessati (fig.3):

1. Discriminazioni, pregiudizio o altro danno sociale;
2. Furto o usurpazione d'identità;
3. Perdite finanziarie o qualsiasi altro danno economico;
4. Perdita di riservatezza dei dati personali protetti da segreto professionale;
5. Decifratura non autorizzata della pseudonimizzazione;
6. Privazione dei diritti e delle libertà dell'interessato;
7. Impossibilità di esercitare i propri diritti sui dati personali (impedito controllo);
8. Danni fisici o psicologici;
9. Impossibilità di esercitare diritti, servizi o opportunità;
10. Altri svantaggi economici o sociali.

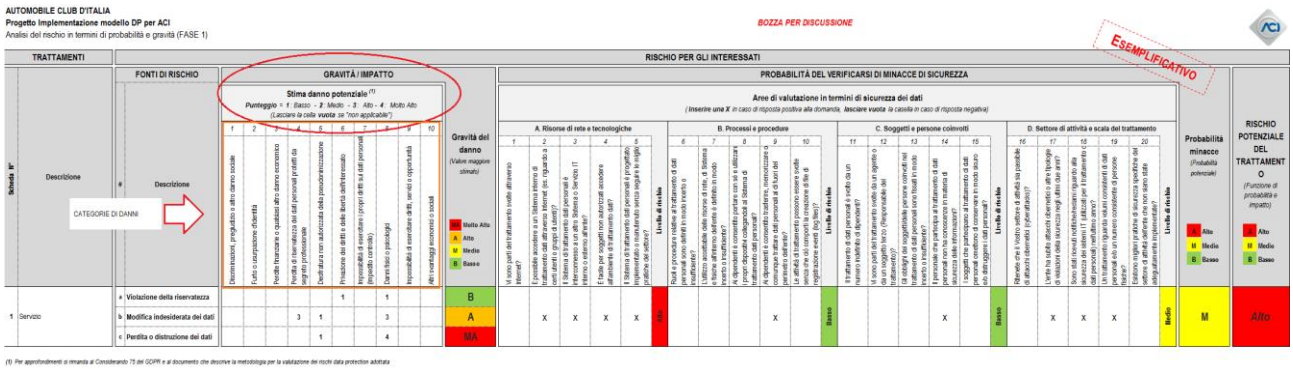


fig.3

In fase di valutazione è opportuno considerare che il livello di gravità del danno per gli interessati tende ad essere più elevato quando il trattamento presenta caratteristiche quali, a titolo esemplificativo e non esaustivo:

- ✔ la profilazione degli interessati;
- ✔ il trattamento di categorie particolari di dati;
- ✔ la minore età o la condizione di vulnerabilità degli interessati;
- ✔ l'elevato volume dei dati trattati;
- ✔ l'elevato numero di interessati.

Ad esito della valutazione inerente al rapporto tra gravità/impatto, ciascuna fonte di rischio sarà identificata con un livello di gravità del danno per l'Interessato da "basso" (colore verde) a "molto alto" (colore rosso).

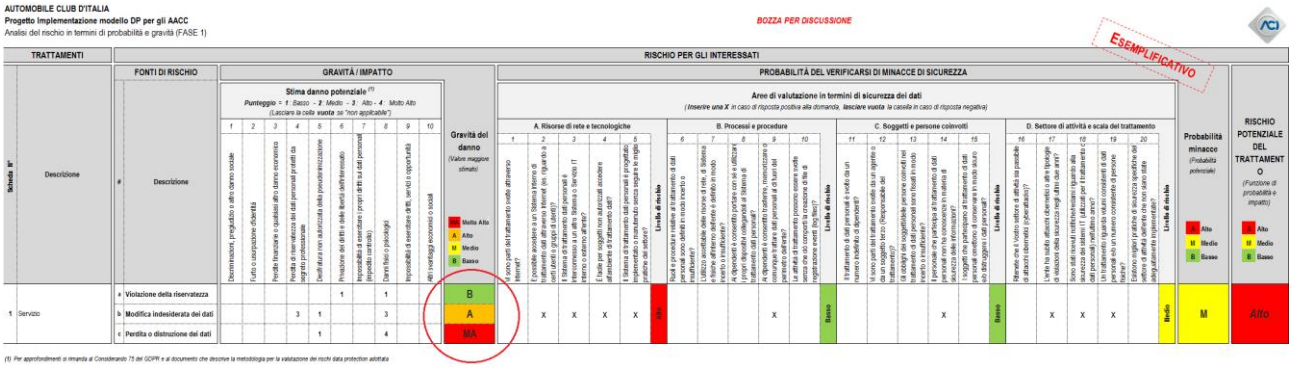


fig.4

2) Probabilità del verificarsi di un evento di minaccia per la sicurezza dei dati personali trattati.

Per valutare la probabilità del verificarsi di una minaccia di sicurezza nel trattamento di dati personali, il Referente dovrà rispondere ad una lista di domande relativamente all'attività di trattamento, suddivise nelle seguenti quattro aree di valutazione (fig. 4):

- ✔ Risorse di rete e tecnologiche (hardware e software)
- ✔ Processi/procedure connessi al trattamento
- ✔ Soggetti e persone coinvolti nel trattamento
- ✔ Settore di attività e scala del trattamento

Sulla base del numero di risposte affermative (indicate con il segno X) e negative (nessun segno) indicate nel modello viene determinato dal sistema un punteggio al quale è associata una determinata probabilità del verificarsi di minacce per la sicurezza dei dati, classificata secondo tre livelli riportati nel seguente prospetto:

PROBABILITA'		
#	**Livello**	Descrizione
1	**Basso**	Appare impossibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti
2	**Medio**	Appare difficilmente possibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti
3	**Alto**	Appare facile per le fonti di rischio considerate concretizzare una minaccia basandosi sulle caratteristiche dei supporti

La combinazione dei risultati così ottenuti in termini di "livelli di impatto" e di "probabilità del verificarsi di minacce" alla sicurezza dei dati permette di ottenere un'indicazione del **LIVELLO DI RISCHIO COMPLESSIVO** secondo il seguente schema:

LIVELLO RISCHIO COMPLESSIVO *(Potenziale)*		LIVELLO GRAVITÀ / IMPATTO		
		Basso (1)	Medio (2)	Alto (3) / Molto Alto (4)
LIVELLO PROBABILITÀ MINACCE	Basso (1)	Basso	Medio	Alto
	Medio (2)	Basso	Medio	Alto
	Alto (3)	Medio	Alto	Alto

Nel caso in cui l'analisi del rischio in termini di probabilità e gravità dia come esito un livello di rischio "ALTO" sarà necessario eseguire una valutazione più approfondita sulla protezione dei dati che prende in esame le misure di contenimento del rischio adottate, corrispondente alla FASE 2 della metodologia, come di seguito descritto.

FASE 2 –GESTIONE DEI TRATTAMENTI CHE POSSONO COMPORTARE UN "RISCHIO ELEVATO PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI – MISURE DI MITIGAZIONE

La seconda fase della metodologia (fig. 5) prevede l'analisi del livello di copertura delle misure di sicurezza idonee a mitigare il livello di rischio potenziale, identificato nella FASE 1, in relazione alle diverse fonti di rischio. Tale valutazione si può eseguire utilizzando il modello allegato al presente manuale.

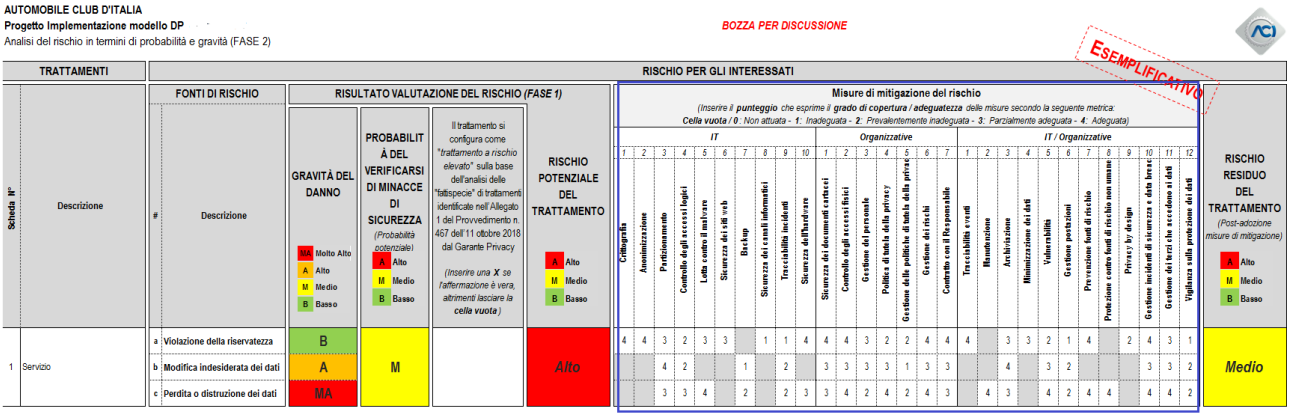


fig.5

Le tipologie di misure di sicurezza applicabili al trattamento oggetto di valutazione sono suddivise in tre ambiti secondo quanto di seguito indicato: IT, Organizzative e IT/Organizzative.

MISURE DI MITIGAZIONE					
TIPOLOGIA		*AMBITO*			
#	*Descrizione*	IT	ORG	IT / ORG	*DESCRIZIONE MISURA*
1	***Crittografia***	*X*			I mezzi implementati per assicurare la confidenzialità dei dati archiviati (in database, file, backup ecc.), così come le procedure per gestire chiavi crittografiche (creazione, archiviazione, aggiornamento in caso di sospetta compromissione ecc.). Specificare i mezzi crittografici impiegati per i flussi di dati (VPN, TLS, ecc.) implementati nel trattamento.

2	***Anonimizzazione***	*X*			Indicare qui i meccanismi di anonimizzazione implementati, le garanzie da essi introdotte contro l'eventuale reidentificazione e per quali finalità sono implementati. Per meglio valutare la bontà di un approccio di anonimizzazione, il G29 propone tre criteri : - Individuazione: resta possibile distinguere un individuo all'interno di un gruppo? - Correlabilità: è possibile collegare reciprocamente insiemi di dati distinti riferiti a uno stesso individuo? - Deduzione: è possibile dedurre informazioni su un determinato individuo? Un insieme di dati rispetto ai quali non siano possibili né l'individuazione né la correlazione o la deduzione è, a priori, un insieme anonimo. Un insieme di dati rispetto ai quali non sia rispettato anche solo uno dei tre criteri suddetti potrà essere considerato anonimo solo in base a un'analisi dettagliata dei rischi di reidentificazione.
3	***Partizionamento***	*X*			Metodi utilizzati per il partizionamento del trattamento: metodiche che riducono la possibilità di correlazioni fra i dati personali e di una compromissione a carico della totalità dei dati. Per esempio, si potranno identificare i dati specifici per ogni attività separandoli logicamente, ecc.
4	***Controllo degli accessi logici***	*X*			Descrivere in che modo sono definiti e attribuiti i profili degli utenti. Specificare i mezzi di autenticazione implementati precisando, ove applicabile, le regole per le password (lunghezza minima, caratteri richiesti, durata della validità, numero di tentativi prima del blocco dell'account, ecc.).
5	***Lotta contro il malware***	*X*			Misure volte a proteggere l'accesso a reti pubbliche (Internet) o non controllate (di partner) nonché postazioni e server contro malware che potrebbe compromettere la sicurezza dei dati personali.
6	***Sicurezza dei siti web***	*X*			Metodi e strumenti implementati per ridurre il rischio che le caratteristiche di un sito web siano sfruttate al fine di pregiudicare dati personali (disciplinare generale di sicurezza, cifratura TLS dei flussi di dati, politica di rilascio dei cookie, audit di sicurezza, ecc.) .
7	***Backup***	*X*			Esistenza di politiche di backup tali da assicurare la disponibilità e/o l'integrità dei dati personali, tutelandone la confidenzialità (periodicità dei backup, cifratura del canale di trasmissione dati, test di integrità, ecc.).
8	***Sicurezza dei canali informatici***	*X*			A seconda del tipo di rete sulla quale il trattamento è effettuato (isolata, privata o Internet), il titolare del trattamento deve implementare sistemi di protezione adeguati: firewall, sonde antintrusione o altri dispositivi (attivi o passivi) volti a garantire la sicurezza della rete.
9	***Tracciabilità incidenti***	*X*			Esistenza di misure messe in atto per rilevare tempestivamente incidenti relativi a dati personali e disporre di elementi utilizzabili per studiarli o per fornire prove nel contesto di indagini (politica di registrazione eventi, rispetto degli obblighi di protezione dei dati ecc.)
10	***Sicurezza dell'hardware***	*X*			Esistenza di misure adottate per ridurre il rischio che le caratteristiche delle apparecchiature (server, postazioni fisse, portatili, periferiche, dispositivi di comunicazione, supporti rimovibili ecc.) siano utilizzate per danneggiare i dati personali (inventario, compartimentalizzazione, ridondanza, limiti per l'accesso ecc.)
11	***Sicurezza dei documenti cartacei***		*X*		Politiche relative ai documenti cartacei contenenti dati personali utilizzati nell'ambito del trattamento. Tali politiche descrivono come i documenti sono stampati, archiviati, distrutti e condivisi.
12	***Controllo degli accessi fisici***		*X*		Esistenza di un controllo degli accessi fisici ai locali che ospitano il trattamento (zonizzazione, accompagnamento di visitatori, assegnazione di badge, porte chiuse, e così via). Indicare se sono in atto procedure di allarme in caso di irruzione.
13	***Gestione del personale***		*X*		Esistenza di un piano che preveda le misure di sensibilizzazione adottate al momento della presa in carico di un dipendente, e di una procedura che descriva le misure adottate una volta cessato il rapporto di lavoro con i soggetti che accedono ai dati .
14	***Politica di tutela della privacy***		*X*		Esistenza di un'organizzazione idonea a guidare e verificare la protezione dei dati personali all'interno della struttura (designazione di un DPO/RPD, creazione di un organo di monitoraggio, ecc.)
15	***Gestione delle politiche di tutela della privacy***		*X*		Il titolare del trattamento deve disporre di una base documentale che formalizzi gli obiettivi e le regole da applicare nel campo della protezione dei dati (piano d'azione, revisione periodica delle politiche in materia di protezione dati, ecc.)
16	***Gestione dei rischi***		*X*		Esistenza di una politica che definisce i processi volti a controllare i rischi che i trattamenti comportano per i diritti e le libertà degli interessati (censimento dei trattamenti di dati personali, dei dati trattati, dei supporti utilizzati, valutazione del rischio, definizione di misure esistenti o previste ecc.)

17	***Contratto con il responsabile del trattamento***		*X*		I dati personali comunicati a / o gestiti da responsabili del trattamento devono beneficiare di garanzie sufficienti. Utilizzare esclusivamente responsabili del trattamento che offrono garanzie sufficienti (in particolare quanto a conoscenze specialistiche, affidabilità e risorse). Esigere che il responsabile comunichi la propria politica di sicurezza dei sistemi informativi. Adottare e documentare misure (audit di sicurezza, visite agli impianti, ecc.) che consentano di assicurare l'effettività delle garanzie offerte dal responsabile del trattamento in materia di protezione dei dati. Tali garanzie comprendono, in particolare,: - la cifratura dei dati in base alla loro sensibilità ovvero, in assenza di cifratura, l'esistenza di procedure tali da garantire che il responsabile del trattamento non acceda ai dati affidatigli - la cifratura delle trasmissioni dei dati (p.es.: connessioni tipo HTTPS, VPN, ecc.) - garanzie in materia di protezione della rete, tracciabilità (log, audit), gestione delle autorizzazioni, autenticazione, ecc. Prevedere un contratto con i responsabili del trattamento ove siano definiti tutti gli aspetti previsti dal GDPR. Qualora si ricorra a un fornitore di servizi di cloud computing: 1. Specificare con chiarezza quali dati e quali trattamenti si collocheranno nel cloud; 2. Definire le rispettive esigenze di sicurezza tecnica e giuridica; 3. Effettuare uno studio dei rischi al fine di individuare le misure di sicurezza adeguate; 4. Individuare il tipo di cloud idoneo al trattamento previsto; 5. Scegliere un fornitore che dia garanzie sufficienti; 6. Riesaminare la politica di sicurezza interna; 7. Monitorare gli sviluppi nel tempo.
18	***Tracciabilità eventi***			*X*	Politiche che definiscono la tracciabilità degli eventi e la gestione dei relativi log.
19	***Manutenzione***			*X*	Esistenza di una politica di manutenzione fisica dei dispositivi, specificando l'eventuale ricorso all'outsourcing. Dovrà comprendere la manutenzione remota, ove autorizzata, e specificare i metodi di gestione dei materiali difettosi.
20	***Archiviazione***			*X*	Politiche di conservazione e gestione di archivi elettronici contenenti dati personali, finalizzate a tutelarne, in particolare, la validità giuridica per tutto il periodo necessario (versamento, conservazione, migrazione, accessibilità, eliminazione, politiche di archiviazione, protezione della confidenzialità, ecc.).
21	***Minimizzazione dei dati***			*X*	Si possono utilizzare i seguenti **metodi**: > Filtraggio e rimozione. Quando i dati sono importati, possono essere raccolti involontariamente vari tipi di metadati (come dati EXIF allegati ad una immagine); tali metadati devono essere identificati ed eliminati se non sono necessari per le specifiche finalità. > Riduzione del potenziale identificativo attraverso trasformazione. Dopo aver ricevuto dati sensibili, in quanto parte di un set di informazioni generali ovvero trasmessi solo a fini statistici, questi possono essere convertiti in un modulo meno sensibile oppure essere pseudonimizzati, per esempio: - se il sistema raccoglie l'indirizzo IP per determinare la posizione dell'utente a fini statistici, l'indirizzo IP può essere eliminato una volta dedotti la città o il quartiere; - se il sistema riceve dati video da telecamere di sorveglianza, può riconoscere le persone immobili o in movimento nella scena e sfocarle; - se il sistema è un contatore intelligente, può aggregare i dati sul consumo energetico lungo un determinato arco temporale senza registrarli in tempo reale. > Riduzione della natura identificativa del dato. Il sistema può consentire che l'utente: - utilizzi una risorsa o un servizio senza rivelare la propria identità (dati anonimi); - utilizzi una risorsa o un servizio senza rivelare la propria identità, ma rimanendo identificabile e responsabile di tale utilizzo (dati pseudonimi); - effettui molteplici utilizzi di risorse o servizi senza che tali utilizzi siano reciprocamente correlati (dati non correlabili); - utilizzi una risorsa o un servizio senza che altri, in particolare terze parti, siano in grado di osservare che la risorsa o il servizio è in uso (non osservabilità). La scelta di un metodo fra quelli sopra elencati deve dipendere dalle minacce identificate e, per alcuni tipi di minacce alla riservatezza, la pseudonimizzazione sarà più idonea dell'anonimizzazione (ad esempio se vi sono esigenze di tracciabilità). > Riduzione dell'accumulazione dei dati. Il sistema può essere strutturato in parti (partizioni) indipendenti con funzioni distinte di controllo degli accessi. I dati possono anche essere distribuiti tra questi sottosistemi indipendenti ed essere controllati da ciascun sottosistema utilizzando diversi meccanismi di controllo degli accessi; in questo modo, se un sottosistema subisce una compromissione, possono essere ridotti gli impatti sul set complessivo di dati. > Limitazione dell'accesso ai dati. Il sistema può: - limitare l'accesso ai dati in base al principio detto 'need to know';

					- separare i dati sensibili e applicare politiche specifiche di controllo degli accessi; - crittografare i dati sensibili per proteggerne la riservatezza durante la trasmissione e l'archiviazione; - proteggere l'accesso ai file temporanei nascosti che vengono generati durante l'elaborazione dei dati.
22	***Vulnerabilità***			*X*	Politiche volte a limitare la probabilità e la gravità dei rischi per le risorse utilizzate durante l'operatività (documentare le procedure operative, inventariazione e aggiornamento di software e hardware, correzione di vulnerabilità, duplicazione dei dati, limitazioni all'accesso fisico al materiale, ecc.).
23	***Gestione postazioni***			*X*	Misure adottate per ridurre la possibilità che le caratteristiche del software (sistemi operativi, applicazioni aziendali, software per ufficio, impostazioni ecc.) vengano sfruttate per danneggiare i dati personali (aggiornamenti, protezione fisica e accessi, lavoro su uno spazio di rete protetto, controlli di integrità, logging, ecc.).
24	***Prevenzione delle fonti di rischio***			*X*	Esistenza di misure per evitare che fonti di rischio, umane o non umane, anche se scarsamente probabili, arrechino pregiudizio ai dati personali (merci pericolose, aree geografiche pericolose, trasferimento dati al di fuori dell'UE, ecc.)
25	***Protezione contro fonti di rischio non umane***			*X*	Esistenza di misure per ridurre o evitare i rischi connessi a fonti non umane (fenomeni climatici, incendi, danni provocati dall'acqua, incidenti interni o esterni, animali, ecc.) che potrebbero influire sulla sicurezza dei dati personali (misure preventive, di rilevamento, protezione, ecc.)
26	***Integrare la protezione della privacy nei progetti***			*X*	Esistenza di procedure che descrivono i metodi volti a tenere conto della protezione dei dati personali in ogni nuovo trattamento (certificazioni, specifiche di riferimento, gestione del rischio per la persona interessata secondo una metodologia interna o indicata dall'autorità di controllo, ecc.)
27	***Gestire gli incidenti di sicurezza e le violazioni dei dati personali***			*X*	Esistenza di un'organizzazione operativa per rilevare e gestire eventi che possono influire sulle libertà e sulla riservatezza degli interessati (definizione delle responsabilità, piano di reazione, caratterizzazione delle violazioni ecc.)
28	***Gestione dei terzi che accedono ai dati***			*X*	Esistenza di una procedura volta a ridurre i rischi per le libertà e la vita privata degli interessati potenzialmente conseguenti all'accesso legittimo ai dati da parte di terzi (identificazione dei soggetti terzi, contratto di outsourcing, convenzione, BCR, ecc.)
29	***Vigilanza sulla protezione dei dati***			*X*	Esistenza di misure che consentano una visione globale e aggiornata dello stato di protezione dei dati e della conformità con il GDPR (verifica della conformità dei trattamenti, obiettivi e indicatori, responsabilità, ecc.).

La valutazione dell'efficacia della singola misura sul grado di copertura di ciascuna fnte di rischio viene effettuata dal Referente secondo la seguente metrica:

0 = Non attuata: *la misura non è stata implementata (inesistente grado di copertura della fonte di rischio e dei dati oggetto di trattamento – nessuna ponderazione);*

1 = Inadeguata: *la misura è stata implementata ma non è adeguata a mitigare il rischio (scarso grado di copertura della fonte di rischio e dei dati oggetto di trattamento – ponderazione stimata del 30%);*

2 = Prevalentemente inadeguata: *la misura implementata non è sufficientemente adeguata a mitigare il rischio (parziale grado di copertura della fonte di rischio e dei dati oggetto di trattamento - ponderazione stimata del 50%);*

3 = Parzialmente adeguata**:** *la misura implementata non è pienamente adeguata a mitigare il rischio (incompleto grado di copertura della fonte di rischio e dei dati oggetto di trattamento - ponderazione stimata del 70%);*

4 = Adeguata**:** *la misura implementata dovrebbe essere adeguata a mitigare il rischio (quasi completo grado di copertura della fonte di rischio e dei dati oggetto di trattamento - ponderazione stimata del 90%).*

La valutazione del grado di copertura delle misure di sicurezza adottate restituisce come risultato un *Tasso di mitigazione del rischio* che viene applicato al livello di rischio complessivo del trattamento calcolato nella Valutazione del rischio in termini di probabilità e gravità.

Tale operazione permette di calcolare il **livello residuo di rischio del trattamento** (fig. 6):

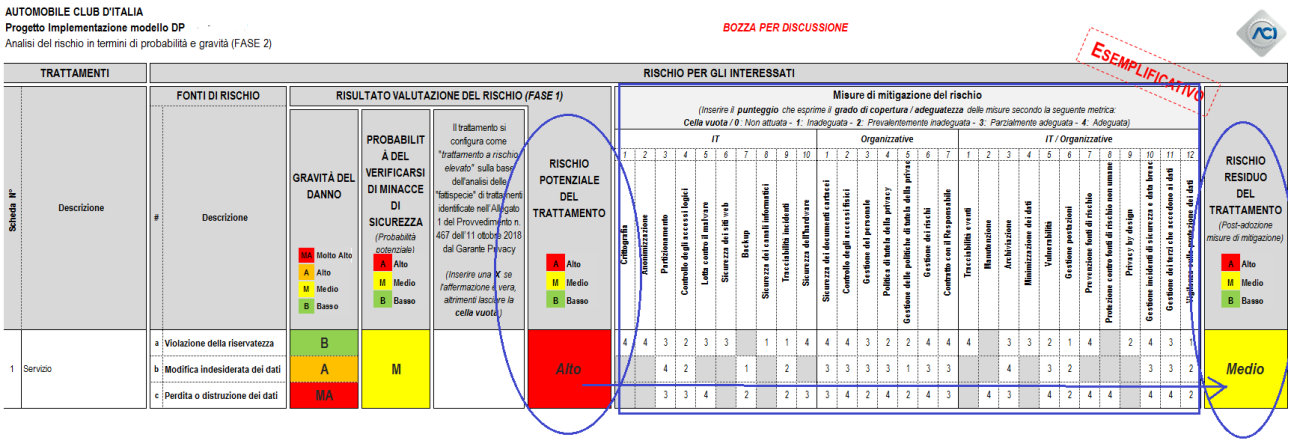


fig.6

Il **livello residuo di rischio del trattamento si intende al netto delle misure di sicurezza implementate**, associando il punteggio finale al seguente schema**:**

LIVELLO RISCHIO COMPLESSIVO *(Residuo)*		LIVELLO GRAVITÀ / IMPATTO		
		Basso (1)	Medio (2)	Alto (3) / Molto Alto (4)
LIVELLO PROBABILITÀ MINACCE	Basso (1)	Basso	Medio	Alto
	Medio (2)	Basso	Medio	Alto
	Alto (3)	Medio	Alto	Alto

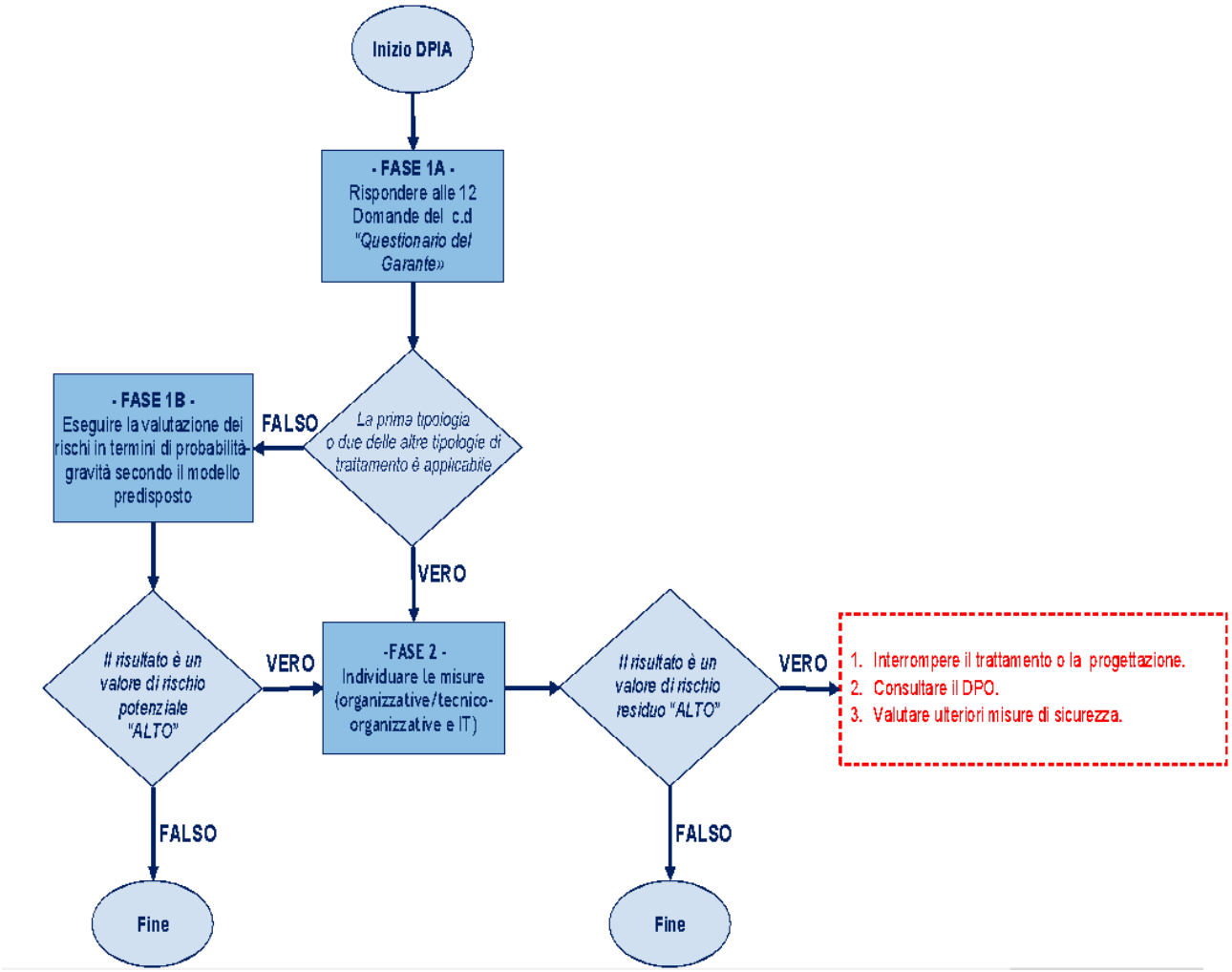
L'analisi del rischio in termini di probabilità e gravità è effettuata dal Referente ogni qualvolta si realizzano delle variazioni del rischio rappresentato dalle attività relative al trattamento.

Nel caso in cui il livello di rischio finale risulti "**ALTO**" sarà necessario:

1) sospendere immediatamente il trattamento dei dati personali, qualora già in atto;
2) identificare ed implementare ulteriori misure di sicurezza tecniche e organizzative per la mitigazione del rischio e ripetere la FASE 2 della presente metodologia al fine di verificare che il livello complessivo di rischio non risulti ancora "**ALTO**".

Qualora il livello di rischiosità del trattamento dovesse risultare ancora "**ALTO**" a seguito dell'adozione delle ulteriori misure di sicurezza, il Titolare o il Referente delegato, consultato il Data Protection Officer, potranno valutare se:

- ✔ sospendere definitivamente la progettazione del nuovo trattamento o il trattamento precedentemente già in essere;
- ✔ procedere alla "Consultazione preventiva" del *Garante per la protezione dei dati personali* (Garante Privacy), ai sensi dell'art. 36 del Regolamento UE 2016/679, in merito al trattamento di dati personali che si intende effettuare.

Per la conduzione della DPIA (Fase 1 e Fase 2) possono essere utilizzati i modelli predisposti.

RAPPRESENTAZIONE PROCESSO DATA PROTECTION IMPACT ASSESTMENT - DPIA