CAMERA DI COMMERCIO FROSINONE LATINA

SCHEDA GENERALE **Valutazione di impatto sulla protezione dei dati**

Descrivere l'attività (come da Registro dei trattamenti)

Raccolta e gestione, tramite una piattaforma informatica, delle segnalazioni di illecito (whistleblowing) ai sensi del DLgs. n. 24 del 10 marzo 2023 entrato in vigore il 15 luglio 2023 che ha recepito la Direttiva UE 2019/1937. Il trattamento oggetto della presente DPIA concerne l'acquisizione e la gestione del trattamento dei dati personali nell'ambito della procedura di gestione delle suddette segnalazioni.

Riassumere i motivi che hanno portato a individuare la necessità di una Valutazione di Impatto (DPIA)

L'art. 13 co. 6 del DLgs 24/2023 prevede espressamente la definizione di un modello di ricevimento e gestione delle segnalazioni interne prevedendo misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai possibili rischi derianti dai trattamenti effettuati sulla base di una valutazione d'impatto sulla protezione dei dati. Il Titolare, trattandosi di adempimenti connessi a obblighi di legge che trovano dettagliata disciplina nella vigente normative e in specifiche Linee Guida ANAC; non ha ritenuto necessario chiedere il parere degli interessati. Tuttavia, come previsto dalla normativa, la CCIAA ha informato le rappresentanze sindacali dell'adozione della Piattaforma e delle procedure di segnalazione.

Descrivere la NATURA del trattamento e dei dati: come raccogliamo i dati; quali sono le categorie di dati trattati (specificare se sono presenti categorie particolari di dati ex artt. 9 e 10 del GDPR); dove e per quanto conserviamo i dati; che tipo di trattamento effettuiamo sui dati.

Ad oggi i dati personali trattati sono acquisiti direttamente dal soggetto che effettua la segnalazione avvalendosi del canale informatico del fornitore Whistleblowing PA appositamente nominato come Responsabile del trattamento ai sensi dell'art. 28 GDPR. E' in corso di implementazione anche la possibilità di raccogliere la segnalazione "oralmente" mediante registrazione della stessa su casella vocale associata ad un numero telefonico. I dati trattati sono: ordinari nonchè particolari ai sensi degli articoli 6, 9, 10 del GDPR. I dati sono conservati a norma dell'articolo 14 Dlgs. 24/2023: 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura. Le segnalazioni anonime sono conservate a norma dell'art. 3 Dlgs. 24/2023 per i 5 anni successivi dalla data di ricezione.

Descrivere lo SCOPO del trattamento: qual è la condizione che rende il trattamento lecito (base giuridica); perché eseguo il trattamento (finalità); se noti, quali sono gli eventuali benefici (per la Camera) attesi dal trattamento; se note, quali sono le conseguenze attese dal trattamento per gli interessati.

il trattamento è effettuato in adempimento a un obbligo di legge e l'esecuzione di un compito di interesse pubblico, ai sensi dell'art. 6, par. 1, lett. c) ed e) del GDPR. I dati forniti vengono trattati esclusivamente per l'istruttoria della segnalazione ai sensi del D.Lgs.n.24/2023. Al fine di garantire la riservatezza del segnalante, l'identità dello stesso è nota solo al RPCT. Salvo i casi in cui sia configurabile una responsabilità penale o a norma dell'art.2043 c.c ovvero per esigenze di indagini penali tributarie o amministrative, ovvero ispettive, l'identità del segnalante non può essere rivelata, senza il suo consenso e tutti coloro che ricevono o sono coinvolti nella gestione della segnalazione sono tenuti a tutelare la riservatezza di tale informazione. Il consenso degli interessati costituisce la base giuridica unicamente per la comunicazione dell'identità del segnalante al segnalato, ove la stessa sia necessaria alla difesa dell'incolpato nel procedimento disciplinare (art. 12, commi 2 e 5 del D.Lgs. n. 24/2023).

Descrivere il CONTESTO del trattamento: chi sono i soggetti interessati al trattamento (specificare se sono inclusi minori o altre soggetti vulnerabili); qual è la natura del nostro rapporto con gli interessati; qual è la misura del controllo degli interessati sui dati.

I soggetti interessati al trattamento in questione sono il segnalante nonché le persone indicate come responsabili della condotta illecita e le altre persone a vario titolo coinvolte nelle vicende segnalate. Le condotte segnalate sono riconducibili a vicende maturate nel contesto lavorativo del segnalante. Agli Interessati sono riconosciuti i diritti di cui agli artt. 15 e seguenti del GDPR. Quanto al diritto di accesso, si segnala che tale diritto non appare immediatamente esercitabile poiché limitato ai sensi e per gli effetti dell'art. 2 undecies, co. 1, lett. f) D.lgs. 196/03 a norma del quale: "1. I diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto (...) f) alla riservatezza dell'identità della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte, ai sensi del decreto legislativo recante attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione, ovvero che segnala L'interessato può comunque avanzare la richiesta ai dati di contatto indicati dal Titolare del trattamento nell'informativa fornita ai sensi degli artt. 13 e 14 oppure contattando direttamente il Data Protection Officer nominato dalla Società. La CCIAA effettuerà
(i) Comunicazione a tutti i dipendenti sull'esistenza del canale di segnalazione interno (canale informatico);
(ii) Pubblicazione sito web istituzionale – sezione dedicata al Whistleblowing;
(iii) Viene inoltre pubblicata nella intranet la Procedura adottata;

Descrivere l'AMBITO del trattamento: chi ha accesso ai dati; con chi condividiamo i dati (destinatari); ci sono contitolari e/o responsabili del trattamento (interni e/o esterni - specificare); indicare se e quali altri soggetti - interni e/o esterni all'amministrazione - sono stati consultati per la redazione della presente DPIA, e riassumere i loro pareri.

I dati personali del segnalante sono accessibili solo dal RPCT, mentre il contenuto della segnalazione e l'eventuale documentazione ad essa allegata può essere accessibile ad altri dipendenti camerali formalmente all'uopo autorizzati per esigenze istruttorie. Inoltre, i dati possono essere trattati da soggetti esterni formalmente nominati dalla Cciaa quali Responsabili del trattamento (esempio fornitore della piattaforma). I trattamenti analizzati con la presente DPIA non comportano comunicazione né diffusione dei dati. Sono fatte salve specifiche e puntuali comunicazioni della segnalazione, in conformità alla legge, all'Autorità Giudiziaria, Corte dei Conti e/o l'A.N.AC, che opereranno ciascuno nell'ambito delle rispettive competenze, in qualità di Titolari autonomi del trattamento.
I dati personali raccolti con la segnalazione, inoltre, potranno essere comunicati ai soggetti segnalati, solo in caso di consenso espresso del segnalante e nelle ipotesi previste dal D. Lgs. n. 24/2023. In particolare, nell'ambito dei procedimenti disciplinari, l'identità del segnalante potrà essere rivelata laddove concorrano, insieme, i seguenti tre presupposti: (1) che la contestazione si fondi, in tutto o in parte, sulla segnalazione; (2) che la conoscenza dell'identità del segnalante sia indispensabile per la difesa

Valutazione della necessità e proporzionalità del trattamento in relazione alle finalità	Valore
Esistenza di una, o più, **basi giuridiche** del trattamento	Si
Le finalità del trattamento sono **determinate, esplicite** e **legittime?**	Si
I dati personali sono trattati in modo **compatibile** con le finalità?	Si
I dati personali sono **adeguati, pertinenti** e **limitati** a quanto necessario rispetto alle finalità per le quali sono trattati?	Si
I dati personali sono **esatti** e **aggiornati?**	Si
E previsto un **periodo di conservazione** dei dati?	Si
Gli interessati sono **informati** del trattamento?	Si
E' data la possibilità agli interessati di esercitare i loro **diritti?**	Si
Il trattamento include **categorie particolari di dati personali** di cui all'art. 9 del GDPR?	Si
Il trattamento include dati personali relativi a **condanne penali e reati** di cui all'art. 10 del GDPR?	Si
Il trattamento è relativi a **soggetti vulnerabili** (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)?	No
Sono presenti **codici di condotta** approvati ai sensi dell'art. 40 del GDPR?	No
Se presenti, sono rispettati i **codici di condotta** approvati ai sensi dell'art. 40 del GDPR?	No
Il trattamento è stato sottoposto a **meccanismi di certificazione** ai sensi dell'art. 42 del GDPR?	No

RISCHIO: Accesso illegittimo ai dati	Probabilità del rischio	improbabile
Incapacità di esercitare diritti (compresi, ma non limitati, ai diritti sulla privacy)	**Gravità del danno**	nessun impatto
Incapacità di accedere a servizi o opportunità	**Gravità del danno**	nessun impatto
Perdita di controllo sull'uso dei dati personali	**Gravità del danno**	marginale
Discriminazione	**Gravità del danno**	marginale
Furto d'identità o frode	**Gravità del danno**	marginale
Perdita finanziaria	**Gravità del danno**	nessun impatto
Danno alla reputazione	**Gravità del danno**	marginale
Danno fisico	**Gravità del danno**	nessun impatto
Perdita di riservatezza	**Gravità del danno**	marginale
Reidentificazione di dati pseudonimizzati	**Gravità del danno**	marginale
Qualsiasi altro significativo svantaggio economico o sociale	**Gravità del danno**	marginale

Rischio complessivo: (Non rilevante-Basso-Medio-Alto)	**Valore finale**	**#N/D**

RISCHIO: Modifica indesiderata dei dati	Probabilità del rischio	improbabile
Incapacità di esercitare diritti (compresi, ma non limitati, ai diritti sulla privacy)	Gravità del danno	nessun impatto
Incapacità di accedere a servizi o opportunità	Gravità del danno	nessun impatto
Perdita di controllo sull'uso dei dati personali	Gravità del danno	marginale
Discriminazione	Gravità del danno	marginale
Furto d'identità o frode	Gravità del danno	marginale
Perdita finanziaria	Gravità del danno	nessun impatto
Danno alla reputazione	Gravità del danno	marginale
Danno fisico	Gravità del danno	marginale
Perdita di riservatezza	Gravità del danno	marginale
Reidentificazione di dati pseudonimizzati	Gravità del danno	marginale
Qualsiasi altro significativo svantaggio economico o sociale	Gravità del danno	marginale

Rischio complessivo: (Non rilevante-Basso-Medio-Alto)	Valore finale	#N/D

RISCHIO: Perdita indesiderata dei dati	Probabilità del rischio	improbabile
Incapacità di esercitare diritti (compresi, ma non limitati, ai diritti sulla privacy)	**Gravità del danno**	nessun impatto
Incapacità di accedere a servizi o opportunità	**Gravità del danno**	marginale
Perdita di controllo sull'uso dei dati personali	**Gravità del danno**	marginale
Discriminazione	**Gravità del danno**	marginale
Furto d'identità o frode	**Gravità del danno**	marginale
Perdita finanziaria	**Gravità del danno**	marginale
Danno alla reputazione	**Gravità del danno**	marginale
Danno fisico	**Gravità del danno**	nessun impatto
Perdita di riservatezza	**Gravità del danno**	nessun impatto
Reidentificazione di dati pseudonimizzati	**Gravità del danno**	marginale
Qualsiasi altro significativo svantaggio economico o sociale	**Gravità del danno**	marginale

Rischio complessivo: (Non rilevante-Basso-Medio-Alto)	**Valore finale**	**#N/D**

MISURA ***(descrivere la misura nella maniera più dettagliata possibile)***	**La misura incide sul rischio di:**		
	Accesso	***Modifica***	***Perdita***
Gestione dell'eventuale documentazione cartacea è effettuata mettendo in atto le seguenti politiche di sicurezza: protocollazione riservata; conservazione in armadi/cassetti chiusi a chiave accessibili al solo RPTC.			
Gestione delle postazioni informatiche si rinvia: alle Politiche di sicurezza del fornitore della piattaforma informatica pubblicate sul relativo sito web.			
Il Titolare ha adottato uno specifico Disciplinare per regolamentare la procedura di gestione delle segnalazioni interne. Ha proceduto con la nomina a Responsabile del trattamento del fornitore della piattaforma; ha redatto l'informativa per gli Interessati; ha aggiornato il Registro dei trattamenti e ha svolto le attività di valutazione d'impatto ai sensi dell'art. 35 del GDPR. In aggiunta ha formato il personale autorizzato al trattamento e ha dedicato una sezione specifica del sito all'interno dell'Amministrazione Trasparente denominata Whistleblowing.			
Rispetto alla gestione dei rischi il Titolare ha censito il trattamento in REGI e ha usufruito dell'analisi del rischio (adr) fornita dall'applicativo. Inoltre, è stata effettuata la DPIA.			
Vulnerabilità e Crittografica si rinvia alle politiche di sicurezza del fornitore della piattaforma.			
La piattaforma attraverso la crittografia garantisce l'anonimato del segnalante.			
Controllo degli accessi logici: vedasi paragrafo 5 del Documento (trattamento dati relativi alle segnalazioni di condotte illecite) pubblicato sul sito Whistleblowing.it e costantemente aggiornato.			
Tracciabilità (Vedasi paragrafo 5 del Documento trattamento dati relativi alle segnalazioni di condotte illecite) pubblicato sul sito Whistleblowing.it e costantemente aggiornato.			
Archiviazione (Vedasi paragrafo 5 del Documento trattamento dati relativi alle segnalazioni di condotte illecite) pubblicato sul sito Whistleblowing.it e costantemente aggiornato.			
Sicurezza dei canali informatici: tutte le connessioni sono protette tramite protocollo TLS1.2+			

Legenda delle misure (elenco non esaustivo)	**Codice**
Sicurezza dei documenti cartacei: 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.	01
Gestione postazioni: 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.). Definizione di logging: Meccanismo che consente di registrare le operazioni effettuate sul sistema informatico al fine di identificare un accesso abusivo ovvero un utilizzo abusivo di dati personali, oppure per stabilire la causa di un incidente. È opportuno tenere traccia di alcune delle operazioni effettuate sui sistemi informatici; a tale scopo, occorre implementare un meccanismo di gestione dei log (le tracce) e degli incidenti che sia in grado di registrare gli eventi pertinenti e garantire l'inalterabilità di tali registrazioni. In ogni caso, si deve evitare di conservare queste informazioni per un periodo eccessivo.	02
Controllo degli accessi fisici: 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.	03
Protezione contro fonti di rischio non umane: 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, ecc.) che potrebbero influire sulla sicurezza dei dati personali (misure preventive, di rilevamento, protezione, ecc.)	04

Gestione delle politiche di tutela della privacy: 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, formazione, ecc.). Questa misura comprende: - la gestione del personale (autorizzazione al trattamento, misure di sensibilizzazione, formazione) - la gestione dei terzi che accedono ai dati (identificazione soggetti terzi, nomina responsabili esterni o autorizzazione al trattamento, contratto di outsourcing, ecc.) - la vigilanza sulla protezione dei dati (visione globale e aggiornato sullo stato di protezione dei dati e delle conformità al GDPR) - integrazione della privacy sin dalla progettazione	05
Gestione dei rischi: 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.)	06
Vulnerabilità: 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.). Questa misura comprende anche: - la lotta contro il malware, cioè le misure volte a proteggere l'accesso a reti e le postazioni e server contro malware che potrebbe compromettere la sicurezza dei dati personali; - le politiche di backup tali da assicurare la disponibilità e/o integrità dei dati personali, tutelandone la confidenzialità; - la sicurezza dei canali informatici a seconda del tipo di rete sul quale il trattamento è effettuato (firewall, sonde anti-intrusione, ecc.); - sicurezza dell'hardware (server, postazioni fisse, portatili, periferiche, dispositivi di comunicazione, supporti rimovili, ecc.) - manutenzione fisica dei dispositivi	07
CRITTOGRAFIA: 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.). Definizione di cifratura: La cifratura di un messaggio permette di garantire che solo il mittente e il/i destinatari(o) di tale messaggio ne conosca(no) il contenuto. Si tratta di una sorta di busta digitale sigillata. Una volta cifrato, se non si dispone della chiave specifica, il messaggio resta inaccessibile e illeggibile sia per le persone sia per le macchine.	08
Anonimizzazione: Indicare i meccanismi di anonimizzazione implementati, le garanzie da essi introdotte contro l'eventuale reidentificazione e per quali finalità sono implementati. Definizione di Anonimizzazione: L'anonimizzazione mira a eliminare il carattere identificativo dei dati personali. L'approccio all'anonimizzazione deve essere definito caso per caso in rapporto agli utilizzi previsti. 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? Pertanto: 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.	09
Controllo degli accessi logici: 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.). Definizione di controllo degli accessi logici: Consiste nel limitare i rischi di accesso di persone non autorizzate ai dati personali in forma digitale. Per fare ciò è consigliabile definire profili di autorizzazione nei sistemi separando le attività e le aree di responsabilità per limitare l'accesso degli utenti ai soli dati strettamente necessari per portare a termine i rispettivi compiti. - rimuovere le autorizzazioni di accesso non appena un utente cessi di essere abilitato ad accedere a una risorsa locale o IT, ovvero allo scadere del contratto - Realizzare una revisione annuale delle abilitazioni per identificare ed eliminare gli account non utilizzati e riallineare i privilegi concessi alle funzioni di ciascun utente.	10
Tracciabilità: 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.).	11
Archiviazione: 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.). Definizione di Archiviazione: I dati che non sono più di utilizzo corrente, ma il cui periodo di conservazione non è ancora terminato, per esempio poiché sono conservati in previsione di eventuali contenziosi, dovrebbero essere archiviati. Gli archivi devono essere protetti in particolare se i dati archiviati sono dati sensibili ovvero se possono comportare gravi effetti negativi per gli interessati.	12
Sicurezza dei siti web: 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.), rispetto delle Linee Guida Garante Privacy 2014	13

PANORAMICA ED ESITO FINALE DPIA

PANORAMICA DEI RISCHI	VALORE	ESITO
RISCHIO: *Accesso illegittimo ai dati*	*#N/D*	#N/D
RISCHIO: *Modifica indesiderata dei dati*	*#N/D*	#N/D
RISCHIO: *Perdita indesiderata dei dati*	*#N/D*	#N/D

PANORAMICA DELLA NECESSITA' E PROPORZIONALITA'	VALORE	ESITO
Esistenza di una, o più, basi giuridiche del trattamento	*Si*	ok
Le finalità del trattamento sono determinate, esplicite e legittime?	*Si*	ok
I dati personali sono trattati in modo compatibile con le finalità?	*Si*	ok
I dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati?	*Si*	ok
I dati personali sono esatti e aggiornati?	*Si*	ok
E previsto un periodo di conservazione dei dati?	*Si*	ok
Gli interessati sono informati del trattamento?	*Si*	ok
E' data la possibilità agli interessati di esercitare i loro diritti?	*Si*	ok
Il trattamento include categorie particolari di dati personali di cui all'art. 9 del GDPR?	*Si*	cautela
Il trattamento include dati personali relativi a condanne penali e reati di cui all'art. 10 del GDPR?	*Si*	cautela
Il trattamento è relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)?	*No*	ok
Sono presenti codici di condotta approvati ai sensi dell'art. 40 del GDPR?	*No*	-
Se presenti, sono rispettati i codici di condotta approvati ai sensi dell'art. 40 del GDPR?	*No*	necessità di intervento
Il trattamento è stato sottoposto a meccanismi di certificazione ai sensi dell'art. 42 del GDPR?	*No*	-

PANORAMICA DELLE MISURE	VALORE	ESITO
Misure per contrastare il rischio di *Accesso illegittimo ai dati*	*0*	Assente
Misure per contrastare il rischio di *Modifica indesiderata dei dati*	*0*	Assente
Misure per contrastare il rischio di *Perdita indesiderata dei dati*	*0*	Assente

ESITO FINALE DPIA		
	Rischi	#N/D
	Neces./Prop.	Negativo
	GENERALE	Negativo

Indicare il soggetto che ha effettuato la Valutazione di impatto (nome, cognome e ruolo ricoperto all'interno dell'ente)
Responsabile dell'Ufficio Legale dell'Ente. Avv. Annalisa Di Giulio, con il supporto del Responsabile dell'Ufficio Servizi Informatici e Tecnologici dell'Ente

Parere del Responsabile della protezione dei dati (riassumere il parere e indicare nome e cognome del RPD)
Il Responsabile della Protezione dei Dati (RPD) dell'Ente, dott. Enzo Maria Tripodi, preso atto dello svolgimento della DPIA sulla base della metodologia adottata dall'Ente esprime il suo parere positivo al riguardo

Specificare se il parere del RPD è stato accettato. In caso negativo riassumerne le ragioni
il parere dell'RPD è stato accettato.