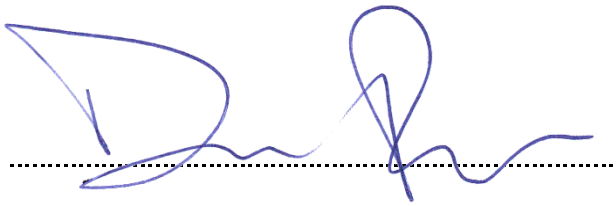
CASA DI CURA GIBIINO S.R.L.

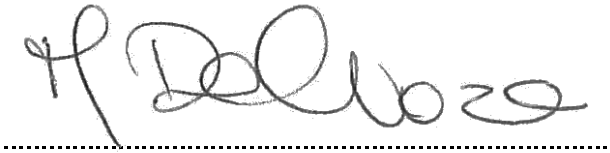
DATA PRIVACY IMPACT ASSESSMENT (DPIA)
WHISTLEBLOWING
EX D.L. 10 MARZO 2023 N. 24 E D.LGS. 8 GIUGNO 2001 N. 231

Relazione del 10.12.2023

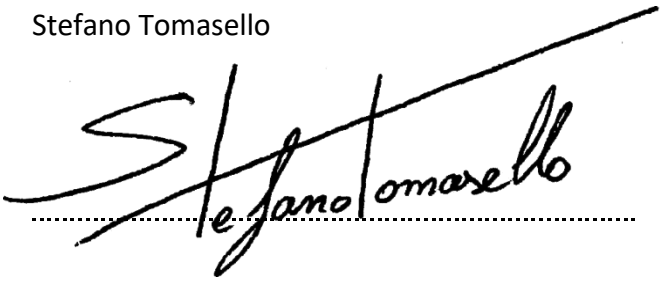
Legale Rappresentante:
Pagano, Dario



DPO:
De Chiara, Manuela



Responsabile dei Trattamenti:
Stefano Tomasello



Indice

1. PREMESSA

Ai sensi dell'art. 35 del Regolamento UE n. 2016/679 (in seguito anche "GDPR"), la DPIA corrisponde alla valutazione d'impatto del trattamento del dato sulla protezione dei dati personali, qualora il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Ciò considerata la natura, il contesto e le finalità del trattamento.

Il GDPR introduce dunque una valutazione di stampo preliminare, che consente al Titolare del trattamento di prendere visione del rischio prima ancora di procedere al trattamento e di attivarsi perché tale rischio possa essere, se non annullato, quantomeno fortemente ridotto.

I principi fondamentali della DPIA risultano pertanto:

- i diritti e le libertà fondamentali dell'interessato, punto cardine dell'intero impianto del GDPR;
- la gestione dei rischi per la privacy, attraverso le misure tecniche ed organizzative di volta in volta adeguate rispetto al rischio.

Una DPIA poggia su due pilastri:

1. i principi e i diritti fondamentali, i quali sono "non negoziabili", stabiliti dalla legge e che devono essere rispettati e non possono essere soggetti ad alcuna variazione, indipendentemente dalla natura, gravità e probabilità dei rischi;
2. la gestione dei rischi per la privacy dei soggetti interessati, che determina i controlli tecnici e organizzativi opportuni a tutela dei dati personali.

La Metodologia di analisi dei rischi adottata nella conduzione delle attività di Data Privacy Impact Assessment è la metodologia di analisi CNIL del Garante Francese (o altra metodologia definita dal Titolare del trattamento).

2. CONTESTO

2.1. Panoramica del trattamento

Il trattamento ha ad oggetto i dati personali dei soggetti che effettuano segnalazioni ai sensi del D.lgs. n. 24/2023.

La gestione delle segnalazioni, di cui al Par. 6.1. (Segnalazioni Interne), viene effettuata affidandosi ad una piattaforma esterna all'azienda, in linea alle disposizioni di cui al D.L. n. 24 del 10 marzo 2023.

Il fornitore del Servizio è Warrant Hub S.p.A. tramite l'applicativo Wallbreakers™, ha fornito indicazioni sulle tecnologie e modalità di trattamento tramite scheda tecnica del servizio che si allega alla presente DPIA (Allegato C: Specifiche di Wallbreakers™).

2.2. Responsabilità Connesse al Trattamento

Ruolo	Nominativo
Titolare del Trattamento	Casa di Cura Gibiino S.r.l.
Responsabile Esterno del Trattamento	Warrant Hub S.p.a.
Amministratore di Sistema	AdS Casa di Cura Gibiino S.r.l.
Responsabili del Trattamento (Data Processors)	OdV
Responsabili del Trattamento (Data Processors)	RDPC

2.3. Riferimenti normativi e Standard applicabili al Trattamento

Al trattamento in materia di segnalazioni e normativa whistleblowing si applicano le seguenti normative e standard:

- Regolamento UE n. 2016/679 (c.d. GDPR)
- D.lgs. n. 196/2003 (c.d. Codice Privacy) così come modificato dal D.lgs. n. 101/2018
- Direttiva UE 1937/2019
- D.lgs. n. 24/2023
- D.Lgs. 231/2001

2.4. Dati oggetti del Trattamento

Di seguito si riportano le tipologie di dati personali che sono oggetto di trattamento a seguito di una segnalazione fatta ai sensi del D.lgs. n. 24/2023

Categorie di Dati	Categoria di Interessati
Dati personali comuni e di contatto	• Dipendenti e Collaboratori che effettuano una segnalazione o che ne sono oggetto. • Fornitori che effettuano una segnalazione o vengono segnalati. • Dati dei Pazienti eventualmente forniti in relazione ad una segnalazione (nei limiti di quanto consentito a norma di legge).

Dati personali particolari (es. dati relativi alla salute, dati relativi all'appartenenza sindacale)	• Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto. • Fornitori che effettuano una segnalazione o vengono segnalati. • Dati dei Pazienti eventualmente forniti in relazione ad una segnalazione (nei limiti di quanto consentito a norma di legge).
Dati giudiziari (es. condanne penali)	• Dipendenti e collaboratori che effettuano una segnalazione o che ne sono oggetto. • Fornitori che effettuano una segnalazione o vengono segnalati.

N.B. L'utilizzo di dati relativi a Pazienti sono da utilizzare nel contesto della Segnalazione solo nel caso in cui gli stessi siano imprescindibili per determinare la validità e le attività seguenti di una Segnalazione.

Si fa specifico obbligo nelle lettere di incarico del Comitato (Vedi Definizioni del PRWHB.00 - Procedura Whistleblowing) di utilizzare questa categoria di dati solo a questa condizione e comunque attenzionarne in maniera particolare la riservatezza, anche limitando gli elementi identificativi (Nome e Cognome) ove non fondamentali per la segnalazione stessa.

2.5. Ciclo di vita del trattamento dei dati (descrizione funzionale)

1. Attivazione e configurazione della piattaforma
2. Utilizzo della piattaforma – invio delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei soggetti autorizzati
3. Dismissione della piattaforma (termini contrattuali o di legge) con conseguente cancellazione sicura dei dati da parte del fornitore/provider del servizio.

3. PRINCIPI FONDAMENTALI

Scopi del Trattamento	Il trattamento è finalizzato esclusivamente alla gestione della segnalazione e all'adempimento degli obblighi legali previsti dalla normativa vigente in materia di whistleblowing.

Base Giuridica del Trattamento	Il trattamento si fonda sulla base giuridica dell'adempimento di un obbligo di legge a cui è tenuto il titolare (Art. 6.1. lett. c) GDPR).
Adeguatezza, pertinenza e limitazione dei dati in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?	I dati personali raccolti sono solo quelli espressamente necessari alla gestione della segnalazione, come normativamente previsto dall'articolo 12 del D.lgs. n. 24/2023. Il perseguimento delle finalità avviene nel rispetto del principio di minimizzazione (art. 5.1. lett. c) GDPR).
Correttezza e Aggiornamento dei Dati.	Il trattamento dei dati personali relativi alle segnalazioni sono costantemente aggiornati in quanto i soggetti incaricati di ricevere e gestire le segnalazioni ne verificano preliminarmente la corrispondenza a verità.
Periodo di Conservazione dei Dati.	Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni, che decorrono dalla data di comunicazione dell'esito finale della procedura di segnalazione, come espressamente previsto dall'articolo 14 del D.lgs. n. 14/2023.

3.1. Misure a tutela dei diritti degli interessati

Informativa al Trattamento	Gli interessati sono informati attraverso una specifica informativa resa ai sensi degli artt. 13-14 GDPR. L'informativa viene resa disponibile secondo le seguenti modalità: • Circolarizzazione della Documentazione tramite il Gestionale Interno della CdC (CareMed) • Comunicazione via E-Mail (Mailing List)

	• Pubblicazione sito internet – Sezione Amministrazione Trasparente: Whistleblowing.
Consenso al Trattamento	Il trattamento dei dati personali relativi la segnalazione da parte dei soggetti espressamente autorizzati al trattamento non necessita di consenso da parte dell'interessato, in quanto la base giuridica del trattamento è l'adempimento di un obbligo di legge (Art. 6.1. lett. c) del GDPR). Nel caso invece ricorra l'ipotesi di comunicazione dei dati personali a soggetti diversi da quelli espressamente autorizzati dal Titolare, il segnalante dovrà prestare il suo consenso specifico alla segnalazione ai sensi degli, tramite piattaforma artt. 6.1. lett. a) e 7 del GDPR.
Esercizio dei diritti degli interessati ex artt. 15 ss. GDPR?	Gli interessati possono esercitare i diritti previsti dagli artt. 15 ss. del GDPR attraverso l'indirizzo di posta elettronica dedicato dpo@casadicuragibiino.it, nei limiti di cui all'articolo 2-undecies del Codice Privacy
Gli obblighi dei Responsabili esterni del trattamento sono definiti con chiarezza e disciplinati da un contratto?	Le terze parti che trattano dati personali per conto del Titolare sono state nominate Responsabili Esterni del trattamento ai sensi dell'art. 28 GDPR, attraverso contratti o altri atti giuridici.
Gli obblighi dei Responsabili del trattamento (Data Processors) sono definiti con chiarezza e disciplinati?	I Soggetti che trattano dati personali per conto del Titolare sono stati nominati Responsabili del trattamento ai sensi dell'art. 28 GDPR, tramite atto specifico di nomina per il contesto di cui alla presente DPIA.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?	Per questa tipologia di trattamento non è previsto un trasferimento di dati personali fuori dall'Unione Europea.

3.2. Misure di Sicurezza Esistenti

Crittografia	Crittografia completa dei dati delle segnalazioni dei segnalatori e delle comunicazioni dei destinatari; Supporto dell'anonimato digitale con l'integrazione di Tor; Supporto HTTPS integrato con lo standard TLS 1.3 (classificazione SSLabs A+);
Controllo degli accessi logici	L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password. Sistema multiutente con ruoli utente personalizzabili (segnalatore, destinatario/ricevitore, amministratore, custode); Supporto dell'autenticazione a due fattori (2FA) conforme allo standard TOTP RFC 6238.
Tracciabilità	Soggetto a continue revisioni tra pari e controlli di sicurezza periodici.
Archiviazione	Database integrato e criptato.
Gestione delle vulnerabilità tecniche	Test di penetrazione multipli con rapporti pubblici completi;

	Conformità agli standard di settore e alle best practice per la sicurezza delle applicazioni (OWASP);
Backup	Back-Up giornaliero. Back-Up eseguito in Automatico. Back-Up Incrementale. Utilizzo 4 Supporti Differenti. Back-Up in Cloud.
Manutenzione	Soggetto a continue revisioni tra pari e controlli di sicurezza periodici;
Sicurezza dei canali informatici	Sandboxing di rete integrato con iptables; Sandboxing dell'applicazione integrato con AppArmor; Protezione completa contro gli invii automatici (prevenzione dello spam); Soggetto a continue revisioni tra pari e controlli di sicurezza periodici.
Sicurezza dell'hardware	I server sono ospitati in un datacenter, situato sul territorio italiano. Il provider è inoltre certificato ISO 27001:2013, ISO 14001:2015, ISO 27017:2015, ISO 27018:2019 e ha ricevuto la Certificazione dell'Agenzia per la Cybersicurezza Nazionale.
Gestire gli incidenti di sicurezza e le violazioni dei dati personali **Lotta contro il malware**	Il prodotto è conforme con le normative GDPR in materia. Gli amministratori e gli sviluppatori del prodotto operano in contesti di sicurezza conformi alle linee guida

	in materia, con firewall e antivirus aziendali al passo con le minacce informatiche di oggi.
Politica di tutela della privacy	La società adotta un Modello Organizzativo sulla protezione dei dati personali.
Gestione dei rischi	L'analisi dei rischi viene condotta secondo metodologia CNIL (o altra metodologia definita dal Titolare).
Gestire gli incidenti di sicurezza e le violazioni dei dati personali	Gli incidenti di sicurezza e le violazioni dei dati personali vengono gestiti secondo la "Procedura Data Breach" adottata dalla Società in conformità a quanto prescritto dagli artt. 33-34 del GDPR.
Vigilanza sulla protezione dei dati	Vigilanza svolta da DPO/Comitato Privacy/funzioni incaricate dal Titolare del trattamento (a seconda di quanto definito nell'organigramma privacy aziendale).

4. ANALISI DEI RISCHI

4.1. Metodologia di Valutazione

Ai sensi della procedura PR.PIA.06.01.03 - Data Protection Impact Assessment e Consultazione Preventiva la Casa di Cura sfrutta un metodo di calcolo del rischio basato su **parametri oggettivi**, al fine di stabilire se esiste un rischio o un rischio elevato per il trattamento specifico. L'Oggettivazione del rischio pertanto passa attraverso un modello di creazione della probabilità e della Gravità in grado di rispecchiare il contesto in cui l'organizzazione opera. Sono state identificate griglie oggettive di calcolo delle Probabilità e Gravità con riguardo ai diritti e libertà dell'interessato.

Matrice Ri = P x G					
	Probabilità	1 - Trascurabile	2 – Limitata	3 – Importante	4 – Massima

Gravità	1 - Trascurabile	1	2	3	4
	2 – Limitata	2	4	6	8
	3 – Importante	3	6	9	12
	4 – Massima	4	8	12	16

Gravità	Significato	Descrizione generica degli impatti (diretti e indiretti)
4	Massima	I soggetti interessati possono incontrare conseguenze irreversibili.
3	Importante	I soggetti interessati possono incontrare conseguenze significative, e difficoltà nella loro risoluzione, ma comunque superabili.
2	Limitata	I soggetti interessati possono incontrare inconvenienti superabili.
1	Trascurabile	Gli interessati non saranno coinvolti o potrebbero incontrare alcuni lievi inconvenienti senz'altro superabili.

Probabilità	Significato	Criterio di scelta
4	Massima	Il verificarsi del danno dipende da condizioni direttamente connesse alla situazione; Il verificarsi del danno non provocherebbe alcuna reazione di stupore; Eventi simili sono già accaduti in azienda o in aziende dello stesso tipo
3	Importante	Il verificarsi del danno dipende da condizioni non direttamente connesse alla situazione ma possibili; Il verificarsi del danno provocherebbe reazioni di moderato stupore; Eventi simili sono stati già riscontrati
2	Limitata	Il verificarsi del danno dipende da condizioni impreviste Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti; Eventi simili si sono verificati molto raramente
1	Trascurabile	Il verificarsi del danno è subordinato a un concatenamento di eventi indipendenti tra loro; Il Verificarsi del danno è creduto impossibile dagli addetti; Non è mai accaduto nulla di simile

Valutazione % delle Misure Esistenti

Rating	Descrizione
1-25%	Non adeguate
26-50%	Minime
51-75%	Adeguate
76-99%	Estremamente Adeguate

Rating rischio residuo (Rr)

Rischio Alto	6,1 - 16
Rischio Medio	3,1 - 6
Rischio Basso	1 - 3

Elementi per la valutazione:

- **Ri** è il Rischio Inerente valore di riferimento su cui effettuare le valutazioni e le operazioni di mitigazione;
- **Rr** è il Rischio Residuo calcolato al netto delle misure di mitigazione del rischio (determinate in via percentuale - % abbattimento);
- L'azienda valuta come Rischio Accettabile (**Ra**) = **3;**
- Se il rischio inerente **Ri** a seguito delle valutazioni oggettive, dovesse risultare superiore ad **Ra;** l'azienda interverrà con mitigazioni opportune tali che **Rr < Ra.**

4.2. Analisi

4.2.1. Accesso illegittimo – Perdita della riservatezza

GRAVITÀ (G)	I soggetti interessati possono incontrare conseguenze significative e probabilmente non risolvibili: difficoltà nella loro risoluzione: Disagio, Diffusione indesiderata dei propri dati, Consultazione dei propri da parte di personale non autorizzato, Ricatto economico, Problematiche di natura giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative, Ritorsioni.
PROBABILITÀ (P)	Il verificarsi del danno dipende da condizioni impreviste Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti; Eventi simili non si sono mai verificati

FONTI DI RISCHIO	Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale) Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker) Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici)
MISURE	Vedi Paragrafi 3.1 e 3.2
CALCOLO DEL RISCHIO RESIDUO	

G	P	Ri	Mitigazione % abbattimento rischio	Rr
4	**2**	**8**	76%	**1,92**

Note: La piattaforma di gestione delle segnalazioni è in linea con i requisiti di Sicurezza di cui al GDPR e Normativi in relazione al Decreto Whistleblowing.

Pertanto le misure di sicurezza, descritte in procedura, la limitatezza dei soggetti coinvolti e la loro integrità a monte della nomina rendono altamente efficaci le misure di mitigazione rendendo il rischio residuo, fondamentalmente risultato di fattori esterni all'organizzazione, trascurabile o comunque tollerabile.

Sebbene il grado di Probabilità 2 preveda che un evento analogo si sia verificato non è stato riscontrato alcun caso nella realtà dell'organizzazione, ad ogni modo – alla luce degli eventi di cybersecurity attuali – non si ritiene adeguato un grado di probabilità inferiore al 2.

Il grado di Rischio applicato è massimo in quanto l'organizzazione ritiene inaccettabile per un Segnalatore o un soggetto Segnalato la perdita di confidenzialità delle informazioni.

4.2.2. Modifiche indesiderate – Perdita dell'integrità

GRAVITÀ (G)	I soggetti interessati possono incontrare conseguenze significative e difficoltà nella loro risoluzione, ma comunque superabili come: Disagio, Diffusione indesiderata dei propri dati, Consultazione dei propri da parte di personale non autorizzato, Ricatto economico, Problematiche di natura giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative.
PROBABILITÀ (P)	Il verificarsi del danno dipende da condizioni impreviste Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti; Eventi simili non si sono mai verificati
FONTI DI RISCHIO	Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale)

	Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker) Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici)
MISURE	Vedi Paragrafi 3.1 e 3.2
CALCOLO DEL RISCHIO RESIDUO	

G	P	Ri	Mitigazione % abbattimento rischio	Rr
3	**2**	**6**	76%	**1,44**

Note: La piattaforma di gestione delle segnalazioni è in linea con i requisiti di Sicurezza di cui al GDPR e Normativi in relazione al Decreto Whistleblowing.

Pertanto le misure di sicurezza, descritte in procedura, la limitatezza dei soggetti coinvolti e la loro integrità a monte della nomina rendono altamente efficaci le misure di mitigazione rendendo il rischio residuo, fondamentalmente risultato di fattori esterni all'organizzazione, trascurabile o comunque tollerabile.

Sebbene il grado di Probabilità 2 preveda che un evento analogo si sia verificato non è stato riscontrato alcun caso nella realtà dell'organizzazione, ad ogni modo – alla luce degli eventi di cybersecurity attuali – non si ritiene adeguato un grado di probabilità inferiore al 2.

Il grado di Rischio applicato è mitigato dal minore impatto di una eventuale perdita di integrità in merito alla tutela del Segnalatore o un soggetto Segnalato non risultando in una perdita di confidenzialità delle informazioni.

4.2.3. Perdita del dato – Perdita della disponibilità

GRAVITÀ (G)	I soggetti interessati possono incontrare inconvenienti superabili.
PROBABILITÀ (P)	Il verificarsi del danno dipende da condizioni impreviste Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti; Eventi simili non si sono mai verificati
FONTI DI RISCHIO	Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale) Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker) Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici)
MISURE	Vedi Paragrafi 3.1 e 3.2

CALCOLO DEL RISCHIO RESIDUO	**G**	**P**	**Ri**	**Mitigazione % abbattimento rischio**	**Rr**
	2	**2**	**4**	76%	**0,96**

Note: La piattaforma di gestione delle segnalazioni è in linea con i requisiti di Sicurezza di cui al GDPR e Normativi in relazione al Decreto Whistleblowing.

Pertanto le misure di sicurezza, descritte in procedura, la limitatezza dei soggetti coinvolti e la loro integrità a monte della nomina rendono altamente efficaci le misure di mitigazione rendendo il rischio residuo, fondamentalmente risultato di fattori esterni all'organizzazione, trascurabile o comunque tollerabile.

I sistemi del Fornitore esterno sono dotati di sistemi di Backup.

L'attento monitoraggio richiesto al Comitato renderebbe comunque ricostruibili gli eventuali dati persi.

Sebbene il grado di Probabilità 2 preveda che un evento analogo si sia verificato non è stato riscontrato alcun caso nella realtà dell'organizzazione, ad ogni modo – alla luce degli eventi di cybersecurity attuali – non si ritiene adeguato un grado di probabilità inferiore al 2.

Il grado di Rischio applicato è mitigato dal minore impatto di una eventuale perdita di disponibilità in merito alla tutela del Segnalatore o un soggetto Segnalato non risultando in una perdita di confidenzialità delle informazioni.

5. Volume dei Dati

Non è stimabile il volume dei Dati relativi a Dati Personali, si evidenzia che comunque gli stessi non potranno configurarsi come trattamento di larga scala.

6. Parere delle parti interessate

Non è stato richiesto un parere alle parti interessate in quanto la finalità del trattamento rappresentano l'adempimento di obblighi di legge.

7. Parere DPO

DPO esprime il proprio parere favorevole alla DPIA effettuata con riferimento alla valutazione di impatto dei dati personali relativi agli adempimenti in materia di whistleblowing, in quanto conformi al dettato normativo. La presente viene firmata per approvazione.

I dati relativi al presente Trattamento e la relativa DPIA saranno trascritti in forma tabellare nei documenti:

- DR.MOP.03.05 - Registro dei Trattamenti Rev. 04 10.12.2023
- DR.MOP.25.05 - DPIA rev. 04 al 10.12.2023

8. Conclusioni

Dall'analisi sull'impatto dei rischi valutati in particolare nell'ambito dei trattamenti individuati aventi l'obbligo di DPIA, emergono "rischi inerenti (Ri)" con impatto sui diritti e libertà degli interessati con stima a valore Medio. Nell'ottica di mitigazione di tali rischi, si evince che, con l'implementazione delle misure tecnico/organizzative pianificate ad integrazione di quelle già messe in atto, il valore di rischio residuo rientra nei parametri accettabili uguali o minori rispetto al Rischio accettato (Ra) dall'organizzazione aventi stima a ***valore Basso,*** valore ritenuto accettabile dall'organizzazione in relazione dai parametri oggettivi considerati.

Si ritiene pertanto che il trattamento in oggetto presenta un grado di rischio sui diritti e libertà dell'interessato rientrante nei parametri accettabili e di conseguenza *non è richiesta una consultazione preventiva all'Autorità Garante.*