

 CITTÀ DI BRA	MODELLO ORGANIZZATIVO WHISTLEBLOWING		
	VALUTAZIONE DI IMPATTO PRIVACY	Edizione 01 Revisione 00	Pag. 1
01-PRI	Estratto della versione integrale	N° di pagine 30	19/02/2025

Relazione di valutazione d'impatto sulla protezione dei dati personali (DPIA)

Attività di trattamento

Trattamento dei dati personali acquisiti in relazione alle segnalazioni - da parte di dipendenti o collaboratori dell'ente (fornitori, consulenti, stagisti), o di altro ente, o di un qualunque soggetto - di illeciti o irregolarità o comportamenti fraudolenti o comunque difforni dalle procedure poste in essere presso l'ente, o dalle norme di condotta professionale e/o dai principi di etica richiamati dalla normativa vigente interna ed esterna, riferibili a dipendenti, membri degli organi sociali o a terzi (clienti, fornitori, consulenti, collaboratori), e che possono determinare in modo diretto o indiretto un danno economico, patrimoniale e/o di immagine all'ente (c.d. WHISTLEBLOWING).

Titolare del trattamento	Città di Bra, Piazza Caduti per la libertà, 14 - 12042 Bra (CN), Codice Fiscale: 82000150043, P. Iva: 00493130041, Telefono: 0172.438111, Email: urp@comune.bra.cn.it, Pec: comunebra@postecert.it
Referente per la DPIA	Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) <i>pro tempore</i>
Data prima emissione	19/02/2025

 CITTÀ DI BRA	MODELLO ORGANIZZATIVO WHISTLEBLOWING	VALUTAZIONE DI IMPATTO PRIVACY	Edizione 01	Pag. 3
			Revisione 00	
01-PRI		N° di pagine 30		19/02/2025

Indice:

1. INTRODUZIONE	4
1.1. Nozione di valutazione d'impatto	4
1.2. Quadro normativo di riferimento	4
1.3. Valutazione di necessità della DPIA	4
1.4. Soggetti coinvolti nell'elaborazione della DPIA	5
1.5. Consultazione degli interessati	5
1.6. Valutazione del rispetto della normativa in materia di protezione dei dati personali	5
1.7. Metodologia per la valutazione di impatto	6
1.8. Elenco dei trattamenti oggetto di valutazione	9
1.9. Revisione e aggiornamento del documento	9
Treatmento 1: Trattamento dati personali a seguito della segnalazione da parte dei soggetti che, in ragione del proprio rapporto di lavoro presso l'Ente, vengano a conoscenza di condotte illecite ai sensi del D lgs 24/2023	10
Descrizione del trattamento	10
Rappresentazione del trattamento	10
Dati personali oggetto del trattamento	10
Soggetti interessati	11
Modalità del trattamento e strumenti coinvolti nel trattamento	11
Valutazione del rispetto della normativa in materia di protezione dei dati personali	11
Base giuridica e finalità del trattamento	11
Valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità	12
Soggetti che hanno accesso ai dati	12
Trasferimento dei dati a soggetti terzi	12
Conservazione dei dati trattati e modalità di cancellazione/distruzione dei dati	13
Modalità di resa delle informazioni agli interessati	13
Trasferimento dei dati al di fuori dell'Unione Europea	13
Diritti degli interessati	13
Valutazione dei rischi	15
Identificazione dei rischi	15
Misure di sicurezza adottate	15

 CITTÀ DI BRA	MODELLO ORGANIZZATIVO WHISTLEBLOWING	Edizione 01 Revisione 00	Pag. 4
	VALUTAZIONE DI IMPATTO PRIVACY		
01-PRI	N° di pagine 30	19/02/2025	

Valutazione _____ 16

1. INTRODUZIONE

1.1. Nozione di valutazione d'impatto

Una *Data Protection Impact Assesment* (in seguito DPIA) è un processo volto a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché determinare l'origine, la natura, la particolarità e la gravità degli eventuali rischi per i diritti e le libertà delle persone fisiche. L'esito di tale valutazione dovrebbe essere considerato nella definizione delle ulteriori misure da adottare per dimostrare che il trattamento dei dati personali rispetta il Regolamento (UE) 2016/679 (in seguito GDPR).

1.2. Quadro normativo di riferimento

Si elencano qui di seguito i riferimenti normativi rilevanti al fine del presente documento:

- REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);
- DECRETO LEGISLATIVO 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali ((, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE));
- DECRETO LEGISLATIVO 18 maggio 2018, n. 51 Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;
- Regolamento Cloud, Decreto Direttoriale ACN n. 21007/24 del 27 giugno 2024.
- DECRETO LEGISLATIVO 4 settembre 2024, n. 138 Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148. L. 90/2024.
- LEGGE 28 giugno 2024, n. 90 Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.
- DECRETO LEGISLATIVO 10 marzo 2023, n. 24, 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 e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali;
- Linee guida ANAC in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne. Approvate con Delibera n°311 del 12 luglio 2023;
- Legge 190/2012, Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione;
- D.lgs. 33/2013, Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni;
- D.lgs. 39/2013, Disposizioni in materia di inconferibilità e incompatibilità di incarichi presso le pubbliche amministrazioni e presso gli enti privati in controllo pubblico, a norma dell'articolo 1, commi 49 e 50, della legge 6 novembre 2012, n. 190;

 CITTÀ DI BRA	MODELLO ORGANIZZATIVO WHISTLEBLOWING	Edizione 01 Revisione 00	Pag. 5
	VALUTAZIONE DI IMPATTO PRIVACY		
01-PRI	N° di pagine 30	19/02/2025	

- Art. 6, commi da 1 a 4, del decreto-legge 9 giugno 2021, n. 80, convertito, con modificazioni, in legge 6 agosto 2021, n. 113;
- ALLEGATO 1 AL PROVVEDIMENTO N. 467 DELL'11 OTTOBRE 2018 [doc. web n. 9058979] (Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018) Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto;
- WP248, 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
- ENISA, Handbook on Security of Personal Data Processing, 2017;
- EDPS, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, 2019;
- UNI CEI EN ISO/IEC 29134, Tecnologie informatiche- tecniche di sicurezza- Linee guida per la valutazione di impatto privacy, giugno 2020.

1.3. Valutazione di necessità della DPIA

Condurre una valutazione d'impatto consente al Titolare di comprendere meglio la natura dei trattamenti e i loro potenziali rischi, attuare le contromisure e dimostrare la conformità degli stessi.

Tale valutazione deve essere condotta alla luce delle indicazioni metodologiche del GDPR, delle Linee guida WP29 e delle diverse metodologie che si possono adottare. L'art. 35, paragrafo 3, GDPR richiede la Valutazione d'Impatto sulla protezione dei dati nei seguenti casi:

- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- il trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'art. 10;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Inoltre, il WP29, al fine di fornire un insieme più concreto di operazioni di elaborazione che richiedono una DPIA a causa del loro intrinseco alto rischio, suggerisce di considerare alcuni criteri. La valutazione sulla necessità di condurre una DPIA viene qui effettuata utilizzando una check-list. È sufficiente che siano soddisfatti due criteri per rendere necessaria la DPIA.

Criteri per valutare se effettuare una DPIA	
Sono previsti trattamenti valutativi o di scoring compresa la profilazione e attività predittive, con particolare riferimento a: 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?	
Sono effettuate decisioni automatizzate che producono significativi effetti giuridici o di analoga natura?	
Il trattamento comporterà un controllo sistematico degli interessati?	
Sono trattati dati sensibili o dati di natura estremamente personale?	X
I dati saranno elaborati su larga scala?	X
È prevista la combinazione o raffronto di insiemi di dati?	
Il trattamento di dati personali è relativo a interessati vulnerabili?	X
Sono previsti nel trattamento utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative?	X

 CITTÀ DI BRA	MODELLO ORGANIZZATIVO WHISTLEBLOWING	Edizione 01 Revisione 00	Pag. 6
	VALUTAZIONE DI IMPATTO PRIVACY		
01-PRI	N° di pagine 30	19/02/2025	

Il trattamento determinerà decisioni o azioni relative ai soggetti che avranno un significativo impatto su di loro?	X
---	---

Inoltre, ai sensi dell'art. 35 del GDPR deve essere effettuata una valutazione di impatto sulla protezione dei dati per quei trattamenti che prevedono un rischio elevato per i diritti e le libertà delle persone fisiche. In particolare, nel rispetto della lett. b), c. 3 del suddetto art. 35, tale valutazione è necessaria nel caso in cui venga effettuato un *trattamento, su larga scala, di categorie particolari di dati personali, o di dati relativi a condanne penali e a reati*, quale ad esempio un trattamento effettuato tramite una piattaforma per la ricezione e la gestione delle segnalazioni.

Come indicato nelle Linee guida in materia di valutazione d'impatto sulla protezione dei dati del WP 248 Art. 29, per "trattamento 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.

In assenza di misure di sicurezza tecniche e organizzative adeguate, è verosimile che un trattamento che preveda l'impiego di una piattaforma per la gestione delle segnalazioni presenti rischi elevati per i diritti e le libertà dei soggetti coinvolti, comportando tutte le casistiche elencate dal WP.

Le attività di trattamento oggetto della presente DPIA, considerati la presenza di numerosi elementi all'interno della check-list di cui sopra, la valutazione dei dati oggetto di trattamento, la natura, l'oggetto, il contesto e le finalità del trattamento, i criteri di cui all'art. 35, c. 3, lett. b) del GDPR, potrebbero dunque presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Condurre una valutazione d'impatto, consente al Titolare di comprendere meglio la natura dei trattamenti e i loro potenziali rischi, attuare le contromisure e dimostrare, in conclusione, la conformità degli stessi.

1.4. Soggetti coinvolti nell'elaborazione della DPIA

Premesso che: nell'ambito del PNRR, M1C1 Investimento 1.2, abilitazione al cloud per le PA locali, finanziato dall'Unione Europea nell'ambito del bando Next Generation EU, con determina n. 2254 del 12/12/2024, è stata formalizzata l'aggiudicazione del servizio di Whistleblowing al Consorzio per il Sistema Informativo CSI Piemonte (CUP: G71C23000630006 - CIG: B4B3A19A95); ritenuto di voler procedere all'elaborazione della valutazione di impatto sulla protezione dei dati (Dpia), ai sensi dell'art. 35 del GDPR 2016/679, relativamente alla piattaforma di gestione segnalazioni whistleblowing in uso all'Ente; la CITTA' DI BRA, con Determinazione Registro Generale N. 323 del 19/02/2025 del Dirigente dell'Area degli Staff, ha provveduto all'affidamento del servizio all' "Ambiente Sicuro Servizi società cooperativa" con sede a Cuneo, in via Cascina Colombaro 56, richiedendo un'analisi complessiva dei canali di segnalazione adottati in materia, inclusa la predetta piattaforma fornita da CSI Piemonte (CSI).

Le responsabilità dei trattamenti oggetto della presente DPIA sono in capo alla CITTÀ DI BRA, nella persona del rappresentate legale pro-tempore (Sindaco), in qualità di titolare del trattamento ai sensi dell'art. 4 del GDPR.

Il CSI PIEMONTE, responsabile del trattamento ai sensi dell'art. 28 del GDPR, è stata coinvolto durante il processo di valutazione, nella veste di fornitore e proprietario del cloud NIVOLA, il quale ha messo a

 CITTÀ DI BRA	MODELLO ORGANIZZATIVO WHISTLEBLOWING		
	VALUTAZIONE DI IMPATTO PRIVACY	Edizione 01 Revisione 00	Pag. 7
01-PRI	N° di pagine 30	19/02/2025	

disposizione l'Allegato Tecnico Servizi Nivola al Catalogo e Listino dei Servizi del CSI (approvato dal CdA del CSI Piemonte il 21 ottobre 2022 in vigore dal 1° gennaio 2023) ed il Report Privacy By Design e By Default del 08 novembre 2023, ai sensi dell'art. 25 del GDPR.

I trattamenti oggetto di valutazione attengono all'area riferita al Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) *pro tempore*, individuato quale referente per la conduzione della DPIA e per valutare la necessità di aggiornamento del presente documento.

Il presente documento è soggetto ad approvazione della Giunta Comunale, mediante deliberazione.

1.5. Consultazione degli interessati

Ai sensi dell'art. 35, c. 9, del GDPR, il titolare del trattamento deve raccogliere le opinioni degli interessati o dei loro rappresentanti, anche per il tramite di mezzi diversi, quali studi, indagini, questionari, confronti, ecc., motivando eventuali decisioni prese in opposizione ad esse. Qualora il titolare decida di non procedere con la raccolta delle opinioni degli interessati, deve documentare le motivazioni a riguardo.

Per quanto riguarda i trattamenti oggetto di valutazione, la CITTÀ DI BRA intende tenere a disposizione degli interessati il presente documento in modo tale che se dovessero pervenire, anche a distanza di tempo, delle segnalazioni/osservazioni da parte degli interessati, ove ritenute rilevanti, il RPCT provvederà ad un aggiornamento della valutazione.

Per quanto riguarda i trattamenti oggetto di valutazione, il Comune ha deciso di avviare una consultazione pubblica per raccogliere le opinioni degli interessati, con pubblicazione parziale della presente Valutazione, sul sito istituzionale.

Ai sensi dell'art. 4 co. 1 del D. Lgs. 24/2023, il Comune ha trasmesso in data ... alla Rappresentanza Sindacale Unitaria una comunicazione con avviso di ricevimento (PEC), tenendosi a disposizione per incontro di approfondimento.

1.6. Valutazione del rispetto della normativa in materia di protezione dei dati personali

In fase di descrizione di ciascun trattamento, deve essere considerato il rispetto dei seguenti aspetti:

- Finalità: determinate, esplicite e legittime (art. 5.1 (b) del GDPR);
- Base giuridica: liceità del trattamento (art. 6 del GDPR);
- Minimizzazione dei dati: adeguata, pertinente e limitata (art. 5, lettera c), del GDPR);
- Comunicazione e diffusione dei dati;
- Periodo di conservazione: limitato (art. 5, lettera e), del GDPR);
- Rispetto dei diritti degli interessati (art. 12 del GDPR);
- Rapporto con i responsabili del trattamento (art. 28 del GDPR) e con i contitolari (art. 26 del GDPR);
- Garanzie riguardanti i trasferimenti fuori dal territorio dell'Unione europea (capo V del GDPR).

Per ciascun elemento, verrà, pertanto, indicato se le misure di adeguamento intraprese dal titolare sono Accettabili (misure che garantiscono il rispetto dei principi sopra elencati), Migliorabili (misure insufficienti, che necessitano di elementi correttivi o integrativi per poter garantire il rispetto dei principi sopra elencati), Non migliorabili (misure insufficienti, che non possono garantire il rispetto dei principi sopra elencati nemmeno se integrate).