Ordine degli Ingegneri della Provincia di Cagliari (OIC)

Valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessments - DPIA)

Whistleblowing PA

ai sensi del GDPR 2016/679 "Regolamento generale sulla protezione dei dati", D.Lgs.196/2003 e ss.mm.ii "Codice in materia di protezione dei dati" come modificato dal D.Lgs. 101/2018 "Adeguamento al Regolamento UE 2016/679",

linee guida del WP Art. 29 del 4.10.2017

■	Copia controllata n. **1**	**Stato del documento**		
□	Copia non controllata	Ed/Rev	Data	Motivo
		1/0	**29/11/2024**	Prima Emissione
		-	**29/01/2025**	Parere positivo DPO

Titolare del Trattamento	**Ordine degli Ingegneri della Provincia di Cagliari (OIC)**
Responsabile della Protezione Dati (Data Protection Officer "DPO")	Dott.Marcello Trudu

1 SEZIONE 1: INTRODUZIONE

1.1 SCOPO DELLA VALUTAZIONE DI IMPATTO (DPIA) E CAMPO D'APPLICAZIONE

Lo scopo della presente Valutazione di Impatto sulla protezione dei dati, nel seguito anche abbreviata come "DPIA" (Data Protection Impact Assessment) è effettuare una valutazione di impatto del trattamento del dato sulla protezione dei dati personali relativamente alle comunicazione, da parte dei dipendenti e dei collaboratori dell'**Ordine degli Ingegneri della Provincia di Cagliari (OIC)**, di reati o di irregolarità di cui siano venuti a conoscenza in ragione del rapporto di lavoro, ai sensi dell'art.54 del D.Lgs.24/2023 di recepimento della Direttiva UE 2019/1937 in materia di whistleblowing.

1.2 NORMATIVA

Con il D.Lgs. n. 24/2023, il legislatore italiano ha recepito i principi comunitari espressi nella direttiva (UE) 2019/1937 che ha introdotto una serie di norme comuni finalizzate a garantire un adeguato livello di protezione ai whistleblowers pubblici e privati, nell'intento di uniformare le normative degli Stati membri.

Il D.Lgs. n. 24/2023 rafforza le regole esistenti, ampliandone la portata. In ambito nazionale, difatti, la materia era disciplinata dal D.Lgs. n. 165/2001 (settore pubblico), e dal D.Lgs. n. 231/2001 (settore privato) in materia di prevenzione dei crimini d'impresa e dalla L. 179/2017.

Il D.Lgs. n. 24/2023, superando la precedente stratificazione normativa, interviene sull'intera disciplina dei canali di segnalazione e intensifica le tutele riconosciute ai segnalanti; amplia la platea dei destinatari degli obblighi, declina ulteriori condotte potenzialmente illecite meritevoli di segnalazione e delinea i profili sanzionatori delle violazioni e dei comportamenti, anche ritorsivi.

1.2.1 RIFERIMENTI NORMATIVI E LINEE GUIDA

- GDPR 2016/679 Regolamento Europeo "General Data Protection Regulation";
- D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali" - Codice Privacy;
- D.Lgs. 101/2018 " Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679";
- Legge 30 Novembre 2017, n. 179 "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato."
- Direttiva (UE) 2019/1937 del 23/10/2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione
- D.Lgs. n.24 del 10/03/2023 "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. (23G00032)"
- Linee guida Working Part 29 *"Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato"*, documento n. 248 del 4 aprile 2017, modificate in data 4 ottobre 2017;
- Deliberazione ANAC n. 469 del 09.6.2021;
- Disposizioni Autorità Garante Privacy.

1.3 WHISTLEBLOWING E PROTEZIONE DEI DATI PERSONALI

1.3.1 WHISTLEBLOWING

L'istituto del whistleblowing è uno strumento giuridico finalizzato alla tutela dei lavoratori che segnalano illeciti o attività fraudolente svolte all'interno della struttura di appartenenza, ai soggetti incaricati (es. ANAC o Autorità giudiziarie). Tale Istituto si applica a soggetti pubblici o privati.

Al fine di garantire la riservatezza dell'identità del segnalante, è obbligatoria da parte dell'**OIC** l'attivazione di canali di segnalazione che assicurino le dovute tutele ad esso riconosciute e l'assenza di ritorsioni.

Il trattamento dei dati personali e la documentazione relativa alle segnalazioni devono, pertanto, essere gestiti rispettando le regole e i principi contenuti nel GDPR.

1.3.2 RISERVATEZZA E PROTEZIONE DEI DATI

I canali che l'**OIC** è tenuto a mettere a disposizione dei potenziali segnalatori (whistleblowers) devono garantire, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità whistleblower, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione stessa e della relativa documentazione.

1.3.3 WHISTLEBLOWERS

La platea delle persone legittimate alla segnalazione, ai sensi dell'art. 3, comma 3, del D.Lgs. 24/2023, oltre quelle operanti nel settore pubblico (dipendenti, comprese le forze di polizia e il personale militare), comprende:

- i lavoratori dipendenti in aziende del settore privato;
- i lavoratori autonomi, nonché i titolari di un rapporto di collaborazione;
- i lavoratori o i collaboratori, che svolgono la propria attività lavorativa presso soggetti del settore privato che forniscono beni o servizi o che realizzano opere in favore di terzi;
- i liberi professionisti e i consulenti che prestano la propria attività presso soggetti del settore pubblico o del settore privato;
- i volontari e i tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso soggetti del settore pubblico o del settore privato;
- gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza.

La segnalazione può avvenire anche quando il rapporto di lavoro non è ancora iniziato, se le informazioni sulle violazioni sono state acquisite, ad esempio, durante le fasi di selezione, ovvero nel corso del periodo di prova o anche successivamente alla risoluzione del rapporto, purché le informazioni riferite alle violazioni siano state acquisite nel corso del rapporto.
Tra i whistleblowers si possono annoverare anche i "facilitatori" ossia persone che assistono il segnalante nel processo di segnalazione, tra cui colleghi e parenti.

1.3.4 CONTENUTO DELLE SEGNALAZIONI

Le violazioni oggetto di segnalazione possono consistere in comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'organizzazione privata ("wrongdoing"), tra cui:

- illeciti amministrativi, contabili, civili o penali;
- condotte illecite ai sensi del D.Lgs. n. 231/2001 o violazione dei modelli organizzativi e gestionali previsti dallo stesso decreto;
- illeciti che rientrano nell'ambito di applicazione degli atti dell'UE o nazionali indicati nello specifico allegato al decreto o nell'allegato alla direttiva (UE) 2019/1937, nei settori degli appalti pubblici, servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo, sicurezza e conformità dei prodotti, sicurezza dei trasporti, tutela dell'ambiente, radioprotezione e sicurezza nucleare, sicurezza degli alimenti, mangimi e salute e benessere degli animali, salute pubblica, protezione dei consumatori, tutela della privacy e delle reti e sistemi informativi;
- atti od omissioni che ledono interessi finanziari dell'UE;

- atti od omissioni riguardanti il mercato interno;
- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni UE nei settori richiamati dal decreto.

Le informazioni sulle segnalazioni possono riguardare anche le violazioni non ancora commesse che il segnalante, ragionevolmente, ritiene potrebbero esserlo sulla base di elementi concreti (art. 2, comma 1, lett. b)). Al contrario, esse non devono essere riconducibili a rimostranze personali o richieste di interventi in merito ai rapporti che intercorrono con colleghi e superiori (screzi, lamentele, etc.). Sono infatti esclusi dall'applicazione della normativa in esame, i casi in cui il denunciante abbia un interesse personale e la denuncia abbia esclusiva attinenza con il proprio rapporto di lavoro.

Non possono essere oggetto di segnalazione, divulgazione pubblica o denuncia (D.Lgs. n. 24/2023, art. 1, comma 2):

- le contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante o della persona che ha sporto una denuncia all'Autorità giudiziaria che attengono esclusivamente ai propri rapporti individuali di lavoro o di impiego pubblico, ovvero inerenti ai propri rapporti di lavoro o di impiego pubblico con le figure gerarchicamente sovraordinate;
- le segnalazioni di violazioni laddove già disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali indicati nella parte II dell'allegato al decreto ovvero da quelli nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nella parte II dell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nella parte II dell'allegato al decreto;
- le segnalazioni di violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato pertinente dell'Unione europea.

1.3.5 MODALITA' DI SEGNALAZIONE: CANALI INTERNI ED ESTERNI

1.3.5.1 CANALI INTERNI

Le segnalazioni possono essere effettuate con canali interni, predisposti dai soggetti pubblici o privati, o esterni all'organizzazione.

Le segnalazioni interne sono effettuate per iscritto, anche con modalità informatiche, busta chiusa o in forma orale attraverso linee telefoniche o sistemi di messaggistica vocale o, su richiesta del segnalante, mediante un incontro diretto.

Il soggetto/ufficio deputato a ricevere le segnalazioni deve:

- rilasciare al whistleblower un avviso di ricevimento della segnalazione entro 7 giorni dalla data di ricezione;
- intrattenere interlocuzioni con lo stesso, richiedendo, se necessario, integrazioni;
- fornire riscontro alla segnalazione entro 3 mesi dalla data di avviso di ricevimento o, in mancanza, entro 3 mesi dalla scadenza del termine di 7 giorni dalla sua presentazione.

Al whistleblower devono essere fornite informazioni chiare sul canale di segnalazione interna, sulla procedura e sui presupposti per effettuare la segnalazione, anche attraverso la creazione di una sezione dedicata sul sito.
L'obbligo si sostanzia nell'adozione di una piattaforma di segnalazione sicura, che tuteli la riservatezza dell'identità e i dati personali dei denuncianti.

La gestione delle segnalazioni può avvenire tramite software che utilizzano sistemi crittografici, adeguati a garantire la riservatezza dell'identità del segnalante, della persona coinvolta e del contenuto della segnalazione, nel rispetto di regole e i principi contenuti nel GDPR.

Il legislatore incoraggia l'adozione di canali interni, ritenuti più prossimi ai fatti oggetto di segnalazione.

1.3.5.2 AUTORITA' NAZIONALE ANTI-CORRUZIONE (ANAC) E ALTRI CANALI ESTERNI

La gestione dei canali esterni di segnalazione è di competenza ANAC, a cui ci si può rivolgere quando:

- nel contesto lavorativo non è previsto un canale di segnalazione interna o questo non è attivo o, se attivo, non è conforme alle prescrizioni dettate al riguardo;

- è stata presentata una segnalazione attraverso il canale di segnalazione interna che non ha avuto seguito;

- vi è giustificato motivo di ritenere che la segnalazione attraverso il canale di interno non sarà efficace o sarà oggetto di ritorsione oppure la violazione possa costituire pericolo imminente o palese per l'interesse pubblico.

In via residuale, il whistleblower può effettuare divulgazioni di pubblico dominio tramite stampa o altri mezzi elettronici o mezzi di diffusione in grado di raggiungere un numero elevato di persone, oltre che una denuncia all'Autorità giudiziaria o contabile. Ovviamente il whistleblower dovrà preoccuparsi di avere un ragionevole e fondato motivo di ritenere che le informazioni sulle violazioni segnalate siano vere e rispettino le condizioni previste (art. 16, comma 1).

L'ANAC equipara le segnalazioni anonime a segnalazioni ordinarie, se circostanziate; il segnalante o il denunciante anonimo, successivamente identificato, che comunica ad ANAC di aver subito ritorsioni può beneficiare della tutela appositamente prevista dal decreto (art. 16, comma 4).

1.4 WHISTLEBLOWING E OBBLIGO DI REDAZIONE DELLA DPIA

1.4.1 VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

Il Regolamento Europeo 2016/679 "General data Protectione Regulation" (GDPR), prevede che qualora un trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, considerata la natura, il contesto e le finalità del trattamento, sia obbligatorio effettuare una Valutazione di impatto del trattamento del dato sulla protezione dei dati personali, Data Protection Impact Assessments (DPIA).

Il GDPR introduce 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.

Una DPIA si basa su due presupposti:

1. i principi e i diritti fondamentali dell'interessato, punto cardine dell'intero impianto del GDPR, 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, attraverso le misure tecniche ed organizzative di volta in volta adeguate rispetto al rischio, che determina i controlli tecnici e organizzativi opportuni a tutela dei dati personali.

1.4.2 VALUTAZIONE PRELIMINARE DELLA NECESSITA' DI SVOLGIMENTO DELLA DPIA

Il trattamento dei dati effettuato nell'ambito dell'istituto del whistleblowing, da parte dell' **OIC**, ricade in tale fattispecie e rende necessaria la redazione della presente valutazione di impatto del trattamento per le caratteristiche proprie del trattamento in esame di pervasità e le implicazioni che le rivelazioni illecita, in relazione al segnalante, possono determinare.

1.5 METODOLOGIA OPERATIVA APPLICATA PER LA CONDUZIONE DELLA DPIA

1.5.1 RIFERIMENTI METODOLOGICI

L'analisi sulla Valutazione di Impatto viene condotta secondo quanto indicato dal Working Part 29 (di seguito anche abbreviato come **"WP29"**), *"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.

In particolare, le suddette linee guida definiscono i criteri in base ai quali il Titolare del trattamento deve decidere se fare ricorso o meno a una DPIA, quali sono le metodologie utilizzabili per la sua conduzione e quali sono gli elementi sufficienti per una DPIA accettabile.

1.5.2 SOGGETTO RESPONSABILE DELLA REDAZIONE DELLA DPIA

Il GDPR impone al solo **Titolare del trattamento** di effettuare la DPIA, qualora ne ricorrano i presupposti (art. 35). Nell'elaborazione di una DPIA il Titolare potrà essere coadiuvato dal DPO (che ne sorveglia il regolare svolgimento e la cui valutazione viene riportata formalmente all'interno del documento), con la collaborazione dei Responsabili del Trattamento.

1.5.3 CASI PREVISTI DAL GDPR

L'art. 35, paragrafo 3, GDPR cita espressamente tre casi in cui sussiste un rischio elevato ed è quindi necessaria l'effettuazione di una DPIA, ossia:

a) *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;*

b) *il trattamento su **larga scala** di **categorie particolari di dati personali** di cui all'articolo 9, paragrafo 1 o di **dati relativi a condanne penali e a reati** di cui all'articolo 10;*

e) sorveglianza sistematica su **larga scala** di una **zona accessibile al pubblico.**

Tale elenco non è esaustivo. Secondo il WP29 art. 29 la DPIA deve essere anche condotta per valutare **l'impatto di un nuovo dispositivo tecnologico** in termini di protezione dei dati.

Il GDPR assegna alle autorità di controllo (per l'Italia, al Garante) il compito di redigere e rendere pubblico **un elenco delle tipologie di trattamento** da assoggettare e da non assoggettare a DPIA (vedere art. 35, paragrafi 4 e 5).

1.5.4 CRITERI ENUNCIATI DAL WP 29 ART.29 - CASI PARTICOLARI ED ESCLUSIONI

Secondo il WP art. 29 il Titolare dovrà condurre una DPIA quando ricorrono almeno **due dei seguenti criteri:**

1. trattamenti valutativi o di *scoring,* compresa la **profilazione** e attività predittive, in particolare a partire da "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (considerando 71 e 91).
2. decisioni automatizzate che producono significativi effetti giuridici o di analoga natura.
3. monitoraggio sistematico: trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o "la sorveglianza sistematica di un'area accessibile al pubblico";

4. dati sensibili o dati di natura estremamente personale: si tratta dei dati particolari di cui all'art. 9 e dei dati giudiziari di cui all'art. 10;

5. trattamenti di dati su larga scala: il **GDPR** si occupa di definire il termine "larga scala" nel considerando 91. Il Gruppo art. 29 raccomanda di tenere conto dei seguenti fattori al fine di stabile se un trattamento sia svolto su larga scala:

a) numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento;

b) volume dei dati e/ o ambito delle diverse tipologie di dati oggetto di trattamento;

e) durata, o persistenza, dell'attività di trattamento;

d) ambito geografico dell'attività di trattamento;

6. combinazione o raffronto di insiemi di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/ o da titolari distinti;

7. dati relativi a interessati vulnerabili, compresi i minori, i dipendenti, i soggetti con patologie psichiatriche, i richiedenti asilo, gli anziani, i pazienti e ogni interessato rispetto al quale possa identificarsi una situazione di disequilibrio con il rispettivo titolare del trattamento;

8. utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

9. trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (art. 22 e cons. 91).

Tuttavia, in alcuni casi si dovrà procedere a una DPIA anche di fronte ad un trattamento che soddisfi **solo uno dei criteri** di cui sopra. È, inoltre, possibile che vi sia perfetta coincidenza tra le ipotesi legislative e i criteri enucleati dal WP29 art. 29.

Si potrebbe verificare anche il caso, ma il WP29 art. 29 non chiarisce quando tale ipotesi potrebbe verificarsi in concreto, in cui il Titolare esclude che debba svolgersi una DPIA perché, pur in presenza dei criteri summenzionati, il trattamento **non** presenta un rischio elevato.

In questo caso, il Titolare dovrà motivare e documentare la scelta della mancata conduzione della DPIA, allegando o annotando il parere del **DPO.** Possiamo immaginare che si tratti della situazione in cui vengano adottate dal Titolare misure di sicurezza tali da scongiurare la possibilità di rischio (elevato) per i diritti e le libertà degli interessati (ad esempio, mediante la pseudonimizzazione e la cifratura dei dati che vengono profilati).

1.5.5 METODOLOGIA OPERATIVA: DETTAGLI

Il GDPR definisce le caratteristiche minime di una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 7, e considerando 84 e 90):

- *"una descrizione dei trattamenti previsti e delle finalità del trattamento";*
- *"una valutazione della necessità e proporzionalità dei trattamenti";*
- *"una valutazione dei rischi per i diritti e le libertà degli interessati";*
- *"le misure previste per:*
  - "*affrontare i rischi*";
  - "*dimostrare la conformità al presente regolamento";*

tenendo conto di eventuali codici di condotta applicabili (art.40 del GDPR).

La figura che segue, tratta dal WP 29, illustra il processo iterativo generico per lo svolgimento di una valutazione d'impatto sulla protezione dei dati:

- **FASI OPERATIVE**

Le fasi operative della valutazione sono le seguenti:

- **Fase 1. Definizione del contesto** *"tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio";*
- **Fase 2. Valutazione dei rischi:** *"valutare la particolare probabilità e gravità del rischio"; (Allegato 2 del WP29);*
- **Fase 3. Esito della valutazione e trattamento dei rischi**: *"atten[uando] tale rischio" e "assicurando la protezione dei dati personali", e "dimostrando la conformità al presente regolamento",* anche mediante la consultazione preventiva del Garante Privacy, in caso di un rischio residuo elevato;
- **Fase 4. Rivalutazione periodica**: "il Titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento".

Durante la predisposizione della presente valutazione di impatto si è proceduto, dunque:

Fase 1. Definizione del contesto: nel § 2.1 si fa riferimento a tutta la documentazione del sistema di gestione privacy dell' **OIC** al fine di descrivere le attività svolte ed i trattamenti applicabili, le modalità di trattamento, le persone autorizzate, gli strumenti adottati, le misure di prevenzione e protezione in atto.

Fase 2. Relativamente ai trattamenti "a rischio", si procede alla valutazione della conformità /non conformità/ non applicabilità dei criteri enunciati nel GDPR, definendo una check list che prende in considerazione le finalità del trattamento; la base giuridica del trattamento (principi di liceità che rendono il trattamento legittimo); le modalità di resa dell'informativa agli interessati; la necessità di richiesta del consenso al trattamento; l'individuazione dei soggetti autorizzati; dei trattamenti svolti; delle tipologie di trattamento; le modalità di archiviazione; i sistemi di protezione in atto; i termini di conservazione; i trattamenti svolti da esterni (Titolari Autonomi; Responsabili del Trattamento); applicazione del principio di adeguatezza per i trasferimenti del dato al di fuori dell'Unione Europea.

Per ogni aspetto della valutazione sono riportate le evidenze rese in forma discorsiva per giustificare il giudizio di conformità.

L'analisi dei rischi è stata condotta tenendo conto delle ripercussioni che ogni trattamento può avere sulla libertà e sui diritti fondamentali dell'interessato.

Fase 3. L'**OIC** esplicita in apposita documentazione le misure adottate per il contenimento del rischio esprimendo nella Valutazione dei rischi l'accettabilità o meno del rischio residuo ed eventuali misure di miglioramento da attuare, soggetti responsabili e data termine.

Dall'analisi svolta deriva il giudizio finale sul livello di rischio del trattamento e sulla necessità o meno di chiedere la consultazione preventiva al Garante Privacy.

Fase 4. Periodicamente (almeno una volta all'anno), e in caso di modifiche relative a qualsiasi aspetto inerenti ai trattamenti svolti viene rivalutata l'adeguatezza della DPIA e l'eventuale necessità di integrazione del documento.

- **ESITI DELLA DPIA E AZIONI DA INTRAPRENDERE**

A seguito dello svolgimento della Valutazione di Impatto, il giudizio finale sarà espresso mediante la formula di "**Rischio accettabile" / "Rischio Non accettabile".**

In caso di **accettabilità del rischio** si procede periodicamente alla sua rivalutazione per la tenuta sotto controllo del rischio;
In caso di **non accettabilità del rischio** (rischio residuo elevato) la DPIA deve essere inviata in versione integrale al Garante Privacy (articolo 36, paragrafo 3, lettera e) che fornirà il proprio parere.

- **PARERE DEGLI INTERESSATI**

La valutazione d'impatto sulla protezione dei dati svolta ai sensi del GDPR è uno strumento per gestire i rischi per i diritti degli interessati, pertanto, il WP 29 precisa che:

"Il titolare del trattamento deve "raccoglie[re] le opinioni degli interessati o dei loro rappresentanti" (articolo 35, paragrafo 9), "se del caso"*.*
Il WP29 ritiene che:

- *tali opinioni possono essere raccolte attraverso una varietà di mezzi, a seconda del contesto, assicurando che il Titolare del trattamento disponga di una base giuridica valida per il trattamento di qualsiasi dato personale; sebbene sia opportuno osservare che il consenso al trattamento non è ovviamente un modo per raccogliere le opinioni degli interessati;*
- *qualora la decisione finale del Titolare del trattamento si discosti dalle opinioni degli interessati, le sue motivazioni a sostegno del procedere o meno vanno documentate;*
- *il Titolare del trattamento deve altresì documentare la sua giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che ciò non sia appropriato, ad esempio qualora ciò comprometterebbe la riservatezza dei piani economici dell'impresa o sarebbe sproporzionato o impraticabile."*

- **PUBBLICAZIONE DELLA DPIA**

La Pubblicazione della DPIA non è un requisito giuridico sancito dal GDPR, ma è auspicabile che il Titolare del trattamento realizzi una sintesi delle risultanze della valutazione DPIA (o una dichiarazione sulla sua conduzione) e la renda pubblica, in particolare quando gli interessati possano essere influenzati dal trattamento.

2 SEZIONE 2: VALUTAZIONE DI IMPATTO - DPIA

2.1 FASE 1: DEFINIZIONE DEL CONTESTO

2.1.1 GENERALITA'

Il presente documento si riferisce ai trattamenti di dati personali relativi al processo di whistleblowing effettuati dal **Titolare del Trattamento**:

Ordine degli Ingegneri della Provincia di Cagliari (OIC)
via Tasso n. 25 - 09128 Cagliari (CA)
Tel. 070 499 703
Pec: protocollo.oic@ingpec.eu
PI 00458800927

2.1.2 DOCUMENTAZIONE DI RIFERIMENTO

La presente DPIA, elaborata ai sensi dell'art.35 del GDPR, si colloca all'interno del Sistema di gestione privacy dell'**OIC** avente l'obiettivo di garantire i diritti e le libertà fondamentali dell'interessato nell'ambito dei trattamenti svolti, sostenendo il Titolare del Trattamento al rispetto della normativa privacy ed evidenziando l'adozione di misure appropriate al rispetto di tale normativa ("accountability").

La DPIA ha lo scopo di contribuire alla gestione dei rischi che gravano sui dati personali nell'ambito dei trattamenti di whistleblowing effettuali dall'**OIC,** coadiuvando la **valutazione dei rischi per i diritti e le libertà delle persone fisiche** posta in essere dal Titolare del trattamento al fine di pervenire alla valutazione dell'accettabilità del rischio residuo o all'individuazione della necessaria implementazione di misure di protezione da mettere in atto, finalizzate ad incrementare il livello di sicurezza nel trattamento dei dati.

Nell'ambito della presente relazione si fa riferimento a tutti i contenuti della documentazione Privacy, delle procedure e istruzioni operative, nonché di tutte le registrazioni che dettagliano i trattamenti effettuati dall'**OIC,** in riferimento alle misure di sicurezza fisiche relative alle aree e locali sede dell'**OIC** in cui si trattano dati e possono essere custoditi documenti contenenti dati personali volte a garantire l'integrità e la disponibilità dei dati; alle misure di sicurezza fisiche relative alla gestione dei documenti e misure di sicurezza logiche relative alle infrastrutture informatiche dell'**OIC**; alle azioni correttive da attuare in caso di anomalie; ai criteri e le modalità di ripristino dei dati a seguito di distruzione o danneggiamento (data breach); al programma delle misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, stabilite a seguito della valutazione dei rischi.

2.1.3 REDAZIONE E VALIDAZIONE DELLA DPIA - PARERE CONCLUSIVO DEL DPO

La presente DPIA è stata elaborata dal Titolare del Trattamento Ordine degli Ingegneri della Provincia di Cagliari (OIC)**, con la consulenza tecnica del Dott.Ing. Emanuela Porcu**. L'iter di elaborazione del documento è stato verificato da parte del DPO interno che si è espresso con parere positivo al termine dello stesso, come da comunicazione formale.

2.1.4 RICHIESTA DEL PARERE DA PARTE DEGLI INTERESSATI - MOTIVAZIONE

Non è stato richiesto il parere dei soggetti interessati o dei loro rappresentanti.

Motivazione: vista la liceità del trattamento avente come base giuridica **l'adempimento di obblighi di legge**, non si richiede il parere da parte degli interessati, ma si effettua l'informazione necessaria tramite pubblicazione di stralcio della DPIA su sito dell'**OIC**, sezione "Amministrazione Trasparente".

2.2 DEFINIZIONE DELL'AMBITO DI ANALISI DELLA DPIA

Sono di seguito descritte i dettagli relativi al trattamento effettuato dall'**OIC** nell'ambito del trattamento oggetto della DPIA.

2.2.1 DESCRIZIONE DEL TRATTAMENTO PRESO IN CONSIDERAZIONE

DESCRIZIONE DEL TRATTAMENTO
I dati trattati sono i dati forniti dal segnalante (whistleblower) al fine di rappresentare le presunte condotte illecite di soggetti che a vario titolo interagiscono con l'**Ordine degli Ingegneri della Provincia di Cagliari (OIC),** delle quali sia venuto a conoscenza in ragione del proprio rapporto di servizio con l'Ente medesimo. Tali dati vengono trattati allo scopo di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti.

2.2.2 RESPONSABILITA' CONNESSE CON IL TRATTAMENTO

RUOLI E RESPONSABILITA' IN AMBITO PRIVACY	
vedere Organigramma nominativo (Sez.03 All.1) - ultimo aggiornamento disponibile	
Titolare del trattamento	**Ordine degli Ingegneri della Provincia di Cagliari (OIC)**
Data Protection Officer (DPO) o Responsabile della Protezione dei Dati	**Dott.Marcello Trudu**
Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT), anche definito come "Responsabile Anticorruzione"	**Dott.Marcello Trudu**
Responsabile del Trattamento	**non presente**
Sub Responsabile del trattamento	**non presente**

2.2.3 INTERESSATI AL TRATTAMENTO

Sono individuabili quali "interessato al trattamento" le persone fisiche cui appartengono i dati trattati nell'ambito della procedura relativa al whistleblowing.

Si tratta di soggetti appartenenti alle seguenti categorie:

a) referenti del Titolare del Trattamento che attivano il servizio di digital whistleblowing:
   - es: Responsabile Anticorruzione, altri soggetti autorizzati per la gestione delle segnalazioni i cui nominativi sono caricati sulla piattaforma, identificati mediante credenziali di autenticazione personali;

b) soggetti che effettuano la segnalazione (whistleblowers) ed eventuali soggetti facilitatori;

c) soggetti nei confronti dei quali possono essere effettuate le segnalazioni, ossia:
   - Personale del Consiglio Direttivo;
   - Personale di segreteria e amministrativo dell'OIC;
   - Personale del Consiglio di Disciplina Territoriale;
   - Personale delle Commissioni Tecniche;
   - i consulenti e i collaboratori;
   - i lavoratori e i collaboratori delle imprese fornitrici di beni o servizi presso l'**OIC**, nonché altri soggetti che a vario titolo interagiscono con l'**OIC** stesso.

La DPIA è relativa ai soggetti individuati ai punti b) e c).

2.2.4 ANALISI DEI DATI OGGETTO DEL TRATTAMENTO

I dati oggetto del trattamento sono relativi a:

- **dati personali di persone fisiche** che effettuano la segnalazione (compresi i soggetti facilitatori);
- **dati personali di persone fisiche e/o di persone giuridiche** oggetto di segnalazione come possibili responsabili delle condotte illecite o coinvolti a vario titolo nelle vicende segnalate,

tali dati sono relativi a dati personali comuni e di contatto (ad esempio: nome e cognome, CF, mansione, recapiti per contatto, etc.), ma possono eventualmente riguardare anche categorie particolari e dati personali relativi a condanne penali e reati ("dati giudiziari"), contenuti nella segnalazione e/o in atti e documenti in essa allegati.

2.2.5 DESCRIZIONE DEL CICLO DI VITA DEL TRATTAMENTO DEI DATI

I dati forniti dal segnalante al fine di rappresentare le presunte condotte illecite, delle quali sia venuto a conoscenza, commesse dai soggetti che a vario titolo interagiscono con il segnalante medesimo, vengono trattati dal Titolare del Trattamento, anche per il tramite di soggetti formalmente autorizzati, in possesso di specifica formazione, allo scopo di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti.

La gestione e la preliminare verifica sulla fondatezza delle circostanze rappresentate nella segnalazione sono affidate al RPCT che vi provvede nel rispetto dei principi di imparzialità e riservatezza effettuando ogni attività ritenuta opportuna, inclusa l'audizione personale del segnalante e di eventuali altri soggetti che possono riferire sui fatti segnalati.

Qualora, all'esito di tale verifica, si ravvisino elementi di non manifesta infondatezza del fatto segnalato, il Responsabile provvederà a trasmettere l'esito dell'accertamento per approfondimenti istruttori o per l'adozione dei provvedimenti di competenza:

a) al Responsabile del personale, nonché al Responsabile dell'Area di appartenenza dell'autore della violazione, affinché sia espletato, ove ne ricorrano i presupposti, l'esercizio dell'azione disciplinare;

b) agli organi e alle strutture competenti dell'**OIC** affinché adottino gli ulteriori provvedimenti e/o azioni ritenuti necessari, anche a tutela dell'Ente stesso;

c) se del caso, all'Autorità Giudiziaria, alla Corte dei conti, al Dipartimento della Funzione Pubblica e all'ANAC.

In tali casi, nell'ambito dell'eventuale procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del Codice di Procedura Penale.

Nell'ambito del procedimento dinanzi alla Corte dei conti, l'identità del segnalante non può essere rivelata fino alla chiusura della fase istruttoria.

Nell'ambito del procedimento disciplinare l'identità del segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa; in caso contrario, il segnalante può opporsi alla rivelazione della propria identità, di conseguenza il procedimento deve essere archiviato.

2.2.6 STRUMENTI UTILIZZATI PER IL TRATTAMENTO

La gestione delle segnalazioni viene effettuata da parte dell'**Ordine degli Ingegneri della Provincia di Cagliari (OIC)** attraverso un canale esterno:

STRUMENTI UTILIZZATI PER IL TRATTAMENTO
Per la raccolta e gestione delle segnalazioni di illeciti per contrastare fenomeni corruttivi relativa alla **Ordine degli Ingegneri della Provincia di Cagliari (OIC) è definita apposita procedura.** **Non sono utilizzate piattaforme software.**

2.2.7 TRATTAMENTO E CICLO DI VITA DEI DATI

Le segnalazioni ricevute e la documentazione relativa alla loro gestione sono conservate per cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

2.2.8 MISURE DI PREVENZIONE E PROTEZIONE DEI DATI PERSONALI RELATIVI AL WHISTLEBLOWING

Si elencano di seguito alcune misure di prevenzione e protezione e le misure organizzative implementate da parte dell' **OIC** applicate ai dati e relative ai sistemi informatici.

2.2.8.1 MISURE APPLICATE AI DATI

Si individuano le seguenti misure di prevenzione e protezione dei dati:

- **CONTROLLO DELL'ACCESSO AI DATI** per l'accesso alla documentazione è riservata al solo RPCT ed eventuale personale autorizzato.
- **ARCHIVIAZIONE:** tutti gli archivi sono conservati in modo da prevenire l'accesso ai non autorizzati.
- **SICUREZZA DEI DOCUMENTI CARTACEI:** i documenti cartacei sono gestiti secondo le logiche di "clean desk" e ne è preservato l'accesso da parte di personale non autorizzato.
- **MINIMIZZAZIONE DEI DATI**: la richiesta dei dati è relativa alle informazioni strettamente necessarie per la gestione della segnalazione.

2.2.8.2 MISURE ORGANIZZATIVE:

- **POLITICA DI TUTELA DELLA PRIVACY:** l'**OIC** ha provveduto:
  - alla designazione del Responsabile Protezione Dati (DPO), ai sensi dell'art. 37 Reg. Ue 2016/679;
  - alla designazione e delega dei soggetti di cui all'art. 2quaterdecies D.Lgs. 196/2003 ai fini della nomina da parte degli stessi dei Responsabili del trattamento dei dati personali;

  provvede, inoltre:
  - alla tenuta del Registro delle attività di trattamento, delle informative, delle nomine dei Responsabili del trattamento, delle valutazioni di impatto (ove necessarie);
  - alla formazione dei soggetti autorizzati/delegati al trattamento dei dati.
- **GESTIONE DEGLI INCIDENTI DI SICUREZZA E DELLE VIOLAZIONI DEI DATI PERSONALI:** l'**OIC** in accordo con quanto previsto dal GDPR in caso di Data Breach, si è dotato di specifiche procedure 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.)
- **GESTIONE DEL PERSONALE**: l'**OIC**, in qualità di Titolare del trattamento ha provveduto e provvede alla formazione dei soggetti designati/autorizzati al trattamento dei dati personali.
  I soggetti designati/autorizzati al trattamento dei dati sono nominati con specifici atti e sono istruiti e formati sul corretto trattamento.
- **GESTIONE DEI TERZI CHE ACCEDONO AI DATI**: l'accesso ai dati da parte di terzi è legittimato da contratti o convenzioni.
- **VIGILANZA SULLA PROTEZIONE DEI DATI**: il Titolare del trattamento svolge una costante attività di verifica dei trattamenti effettuati e se necessario provvede all'aggiornamento del Registro delle attività di trattamento, delle Valutazioni di impatto, delle informative.

2.3 SCHEDA DPIA - WHISTLEBLOWING

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI	
Tipologia di dato oggetto del trattamento:	Dati personali relativi a persone fisiche; dati relativi a condanne penali o reati
Interessato:	soggetti segnalanti e soggetti nei confronti dei quali possono essere effettuate le segnalazioni di presunte condotte illecite
Categorie di dati (vedere § 2.2.4)	▪ **dati personali di persone fisiche** che effettuano la segnalazione ▪ **dati personali di persone fisiche e/o di persone giuridiche** oggetto di segnalazione come possibili responsabili delle condotte illecite o coinvolti a vario titolo nelle vicende segnalate

Aspetto oggetto della valutazione / dettaglio		Esito valutaz			Evidenze / Riferimenti GDPR
		C	NC	NA	
Finalità principale associata al trattamento	raccolta e gestione delle segnalazioni di illeciti per contrastare fenomeni corruttivi relativa all'**OIC** (forma scritta- modello di segnalazione disponibile online- o piattaforma ANAC)	C	-	-	Gli scopi del trattamento denominato "Wistleblowing" sono specifici, espliciti e legittimi ai sensi dell'art. 5.1.a) Reg. UE 679/2016. I dati forniti dal segnalante al fine di rappresentare le presunte condotte illecite delle quali sia venuto a conoscenza in ragione del proprio rapporto di servizio con il Ordine degli Ingegneri della Provincia di Cagliari **(**OIC)vengono trattati allo scopo di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti
Base giuridica del trattamento (principi di liceità che rendono il trattamento legittimo)	Il fondamento giuridico del trattamento dei dati risiede nell'assolvimento di funzioni ed obblighi di legge e nell'esecuzione di un compito di interesse pubblico da parte dell'**OIC**	C	-	-	"Informativa Privacy - Segnalazioni Whistleblowing", pubblicata sul sito internet dell'**OIC** *rif. GDPR art.6 "Liceità del trattamento"* *1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: [...] (* *c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;* *e) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento*
Informazione agli interessati	L' **OIC** informa gli interessati dei propri diritti e di tutti gli aspetti relativi al trattamento mediante rilascio di apposita informativa avente contenuti conformi agli artt.13-	C			Riferimento all'allegato "Informativa Privacy - Segnalazioni Whistleblowing", pubblicata sul sito dell'**OIC**, sezione "Amministrazione trasparente"

Aspetto oggetto della valutazione / dettaglio		Esito valutaz			Evidenze / Riferimenti GDPR
		C	NC	NA	
	14 del GDPR				
Minimizzazione dei dati	I dati raccolti sono quelli strettamente necessari alla finalità del whistleblowing	C			La raccolta dei dati viene effettuata nel rispetto del principio di minimizzazione dei dati, di cui all'art. 5.1 lett. c) Reg. UE 679/2016, ovvero si svolge in maniera tale da ridurre la gravità dei rischi limitando la raccolta di dati personali al minimo necessario per la specifica finalità. I dati raccolti sono adeguati, pertinenti e limitati. Per la registrazione e attivazione del servizio sono richiesti dati anagrafici e di contatto.
Richiesta di consenso	☐ necessario ☑ non necessario	C			Nel solo caso di contestazione basata, in tutto o in parte, sulla segnalazione con indispensabile individuazione e conoscenza dell'identità del segnalante per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare quando sia stato rilasciato specifico consenso alla rivelazione della sua identità da parte del segnalante; in caso contrario il procedimento dovrà essere archiviato.
Esattezza e aggiornamento	i dati indicati nel modulo di segnalazione o caricati nella piattaforma ANAC sono quelli forniti dal segnalante	C			Ai sensi dell'art. 5 par. 1 lett. d) Reg. UE 2016/679, i dati trattati sono esatti e, se necessario, aggiornati. L'aggiornamento è a cura degli utenti stessi o dell'**OIC** in caso di richiesta non anonima
Esercizio dei diritti di accesso da parte degli interessati	L'**OIC** garantisce i diritti degli interessati previsti dal GDPR	C			L'**OIC** garantisce mediante specifica procedura che gli interessati possano esercitare i diritto previsti dal Reg. UE 679/2016 mediante il deposito di specifica istanza al Responsabile della prevenzione della corruzione e della trasparenza (R.P.C.T.)
Esercizio dei diritti di	accesso ai dati	C			L'**OIC** garantisce l'esercizio del diritto di accesso ai dati da parte degli interessati ai sensi dell'art. 15 Reg. UE 679/2016 mediante specifica istanza.
	rettifica	C			L'**OIC** adotta tutte le misure ragionevoli per rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati. Gli interessati possono esercitare il diritto di rettifica ai sensi dell'art. 16 Reg. UE 679/2016

Aspetto oggetto della valutazione / dettaglio		Esito valutaz C	NC	NA	Evidenze / Riferimenti GDPR
					mediante specifica istanza.
	cancellazione (o "diritto all'oblio")			NA	L'esercizio del diritto di cancellazione ("diritto all'oblio") ai sensi dell'art. 17.3 lett. b), non è esercitabile in riferimento al trattamento in esame
	limitazione	C			Gli interessati possono esercitare i loro diritti di limitazione (art.18 GDPR) presentando apposita istanza
	portabilità dei dati			NA	Ai sensi dell'art. 20.3 Reg. UE 679/2016, il diritto alla portabilità dei dati "non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento".
	opposizione	C			Gli interessati possono esercitare i loro diritto di opposizione (art.21 GDPR) presentando apposita istanza
Trattamenti svolti:	raccolta	C			i dati sono raccolti mediante la piattaforma o modulo di segnalazione scaricabile dal sito dell'**OIC**
	registrazione	C			i dati raccolti sono essere registrati, organizzati, conservati, strutturati all'interno della piattaforma o di archivio cartaceo
	organizzazione	C			
	strutturazione	C			
	conservazione	C			
	adattamento o modifica	C			i dati possono essere modificati in caso di necessità per rettifica, in caso di formale richiesta da parte del segnalante.
	estrazione	C			i dati possono essere estratti per la successiva fase della verifica
	consultazione	C			i dati sono consultati esclusivamente da parte di personale autorizzato
	uso	C			i dati sono utilizzati per le attività relative alle segnalazioni (es:analisi, verifica, etc.)
	comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione	C			i dati possono essere comunicati alle figure preposte all'interno dell'**OIC** e agli Enti di controllo. I dati non sono soggetti a diffusione.
	raffronto o interconnessione	C			i dati possono essere raffrontati con altre informazioni necessarie allo svolgimento delle indagini

Aspetto oggetto della valutazione / dettaglio		Esito valutaz C	NC	NA	Evidenze / Riferimenti GDPR
	limitazione	C			i dati possono essere soggetti a limitazione su richiesta dell'interessato
	cancellazione o distruzione	C			i dati possono essere cancellati o distrutti secondo i termini definiti in apposito contratto e/o secondo termini di legge
Tipologia di trattamento	**☑cartaceo**	C			i dati personali possono essere trattati su supporto cartaceo in conformità con le istruzioni operative e in conformità con i principi del GDPR
	☑elettronico	C			I dati sono trattati mediante i PC, collegati internamente mediante una rete LAN da cui è possibile accedere alla piattaforma
Modalità di archiviazione	**a) documenti cartacei**	C			L'**OIC** dispone l'archiviazione della documentazione in forma prevalentemente cartacea. L'archiviazione elettronica (su piattaforma ANAC è a cura dell'ANAC stesso)
	b) banche dati	C			
Sistemi di protezione in atto	**a) trattamenti cartacei**	C			Le informazioni cartacee sono soggette a specifiche misure di protezione fisiche (conservazione all'interno di armadi chiusi a chiave)
	b) trattamenti informatici	C			Sono previste specifiche misure di protezione fisiche e logiche da parte dell'ANAC (crittografia, anonimizzazione, controllo degli accessi logici mediante definizione di credenziali personali esclusivamente da parte di personale autorizzato e formato sulla base di definite procedure operative)
Termini di conservazione	Durata della conservazione dei dati secondo termini di legge	C			I dati personali trattati vengono conservati nel rispetto del principio di "limitazione della conservazione" di cui all'art. 5.1 lett. e) Reg. UE 679/2016. L'ANAC (soggetto che gestisce la piattaforma), Titolare Autonomo del Trattamento, su richiesta dell'interessato provvede alla distruzione di tutti gli eventuali dati personali di cui dovesse disporre o, in alternativa, salvo eventuali esigenze di conservazione in adempimento di obblighi normativi gravanti sullo stesso Ente. Quest'ultimo conserva i dati personali oggetto del trattamento in questione per il periodo previsto dalla normativa vigente.
Trattamenti svolti da esterni	**Titolari Autonomi**	C			I dati possono essere trattati da autorità competenti per adempimento di obblighi di legge e/o di disposizioni dettate da organi pubblici individuabili come Titolari Autonomi (es: ANAC)
	Responsabili del Trattamento	C			non individuati

Aspetto oggetto della valutazione / dettaglio		Esito valutaz			Evidenze / Riferimenti GDPR
		C	NC	NA	
Principio di Adeguatezza -art.45 del GDPR	trasferimenti del dato al di fuori dell'Unione Europea	C			I dati non sono trasferiti all'esterno dell'Unione Europea

2.4 FASE 2: VALUTAZIONE DEL RISCHIO

L'analisi dei possibili rischi consente di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del sistema informatico e di avere una mappa delle possibili contromisure di sicurezza da adottare in relazione all'entità delle minacce rilevate.

2.4.1 METODOLOGIA DI ANALISI

L'analisi dei rischi che gravano sui dati è stata effettuata sulla base del modello ENISA (https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing) combinando due tipi di rilevazioni:

- quelle insite nella tipologia dei dati trattati, che dipendono dalla loro appetibilità per i soggetti estranei all'organizzazione, nonché dalla loro pericolosità per la privacy dei soggetti cui essi si riferiscono;
- quelli legati alle caratteristiche degli strumenti utilizzati per il trattamento dei dati e del luogo fisico in cui tale trattamento è svolto.

L'analisi dei rischi si articola in una prima fase in cui si valutano qualitativamente i rischi presenti sulla base della letteratura e dei dati statistici disponibili relativi all'Ente ed allo specifico settore di attività, e in una seconda fase in cui si quantifica l'entità di ciascun rischio in considerazione della probabilità di verificarsi dell'evento dannoso e della gravità delle sue conseguenze.

La valutazione quantitativa è svolta in termini di "rischio lordo", ossia considerando un'organizzazione priva di misure di sicurezza, in cui vi sia assenza di formazione-informazione al personale autorizzato al trattamento dei dati; mancata manutenzione delle apparecchiature, etc.

Si ricalcola poi il "rischio netto" sulla base delle già descritte misure di sicurezza in essere alla data di redazione del presente documento (Sez. 06 All.1 "Relazione Tecnica Misure di sicurezza"), riportate in sintesi nella colonna "Azioni messe in atto per prevenire, minimizzare, eliminare il rischio", ossia di procedure, istruzioni operative (IO), regole e prescrizioni contrattuali, contenuti dell'avvenuta formazione del personale, manutenzioni effettuate sugli impianti, macchine, infrastrutture.

Il rischio netto è poi valutato in termini di accettabilità (sottolineando la necessità di approfondimento mediante lo svolgimento della DPIA) e, quando sia possibile, sono individuate le Opportunità di miglioramento / Misure da adottare e i termini di realizzazione delle azioni stabilite.

Fase1) VALUTAZIONE QUALITATIVA DEL RISCHIO

Le componenti di rischio che incombono sul dato sono suddivise nelle seguenti categorie di rischio, che fanno riferimento alle "Fonti di minacce" relative a:

A) Fattore Umano: Comportamento degli operatori. Rischio relativo a carenza di consapevolezza, disattenzione, incuria nel trattamento dei dati su supporti cartacei e/o informatici, errore umano, ma anche al sabotaggio da parte di persone che con essa hanno stretti contatti (es: consulenti, manutentori, etc.);

B) Fattore infrastrutture: indisponibilità e danni fisici degli strumenti (HW - SW). Rischio relativo alle apparecchiature; interessa in particolare gli strumenti elettronici (risorse hardware, software e supporti) a seguito di malfunzionamento o degrado degli strumenti; ma anche relativi a intrusione da parte di esterni;

accesso / blocco/ furto delle informazioni in possesso da parte dell'**OIC** a seguito di azione di virus, intercettazione di informazioni in rete, accesso fisico ai dati;

C) Fattori di rischio legati al contesto. Rischio dipendente dal luogo dove gli strumenti sono ubicati. Tale rischio è legato sostanzialmente al verificarsi di eventi distruttivi (incendi, allagamenti, corti circuiti..); alla possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti, atti vandalici, etc.).

Alla prima fase di analisi, segue una seconda fase di valutazione quantitativa del rischio effettuata sulla base della probabilità e della magnitudo, il cui prodotto dà l'effettiva "entità del rischio".

Si esprime, dunque, il giudizio di accettabilità del rischio e di necessità della DPIA.

In caso di non accettabilità si individuano le opportunità di miglioramento e le misure da adottare, nonché i termini temporali di realizzazione ed i soggetti responsabili dell'attività.

Fase 2) VALUTAZIONE QUANTITATIVA DEL RISCHIO

La valutazione quantitativa del rischio netto e lordo è effettuata sulla base della probabilità e della magnitudo, il cui prodotto dà l'effettiva entità del rischio.

- **Sottofase 2A)** Calcolo della **Probabilità** che si verifichi l'evento (concetto statistico).

  La **Probabilità** di ogni rischio analizzato è la possibilità che il rischio si manifesti, secondo la seguente gradualità, in considerazione delle misure tecniche (manutenzione, protezioni delle macchine) e/o procedurali (procedure di lavoro, istruzioni e norme operative, formazione e informazione del personale) già in atto:

Valore di Probabilità	Livello Probabilità	**Criterio probabilistico** (probabilità di accadimento stimata nell'anno)
4	Quasi certo	Prob.>70%
3	Probabile	40% ≤ Prob.<70%
2	Possibile	20% ≤Prob.<40%
1	Improbabile	1% <Prob.<20%

- **Sottofase 2B)** Calcolo della **Magnitudo o gravità del danno** (Impatto sui dati).

  Criteri per la valutazione dell'impatto.

  Il metodo Enisa considera per la valutazione dell'impatto che la minaccia ha sul dato i seguenti criteri:

  - tipo di dato;
  - criticità del processo di trattamento;
  - caratteristiche dell'ambito operativo di riferimento.

  Tipo di dato: si valuta quanto la perdita o corruzione del dato (personale, particolare, relativo a condanne penali o reati) impatta sulla persona a cui si riferisce.

  Criticità del processo di trattamento: si valuta la criticità del trattamento sia in termini di tipologia del trattamento effettuato (es: semplice consultazione, profilazione, interconnessione, archiviazione in database) e quantità dei dati trattati (es: big data).

  Caratteristiche dell'ambito operativo di riferimento: si valuta il settore di attività in cui opera l'Organizzazione che effettua i trattamenti oggetto della valutazione dei rischi.

Valuta anche l'impatto sull'interessato in termini di mancanza di

- Riservatezza del dato (R);
- Integrità del dato (I);
- Disponibilità del dato (D).

Disponibilità dei dati: ossia salvaguardia del patrimonio informativo nella garanzia di accesso, usabilità e confidenzialità dei dati. Da un punto di vista di gestione della sicurezza significa ridurre a livelli accettabili i rischi connessi all'accesso alle informazioni (intrusioni, furto di dati, etc.).

Integrità dei dati: intesa come garanzia che l'informazione non subisca modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici.

Riservatezza informatica: cioè gestione della sicurezza in modo tale da mitigare i rischi connessi all'accesso o all'uso delle informazioni in forma non autorizzata e ovviamente data privacy.

Valore di impatto	Livello Magnitudo (Gravità del danno)	IMPATTO SU INTERESSATI	IMPATTO SULL' ORGANIZZAZIONE (descrizione degli impatti sull' **OIC** che effettua il trattamento)
4	**Alto**	La mancanza di **riservatezza** nel trattamento dei dati, **integrità** e **disponibilità** del dato relativi all'interessato **ha impatti irreversibili** sulla vita degli interessati	La **diffusione** dei dati ha elevati impatti in relazione al mancato rispetto della normativa vigente
			La **mancanza di integrità** dei dati ha elevati impatti sul rispetto della normativa vigente
			L'**indisponibilità dei dati** non consente all'Ente di svolgere gli adempimenti previsti per legge, successivi alla segnalazione
3	**Medio**	La mancanza di **riservatezza** nel trattamento dei dati, **integrità** e **disponibilità** del dato relativi all'interessato **ha impatti non critici e che creano disagi superabili nonostante alcune difficoltà**	La **diffusione** dei dati ha moderati impatti sul rispetto della normativa vigente
			La **mancanza di integrità** dei dati ha moderati impatti sulle attività operative o sul rispetto della normativa vigente.
			L'**indisponibilità dei dati** ha moderati impatti in quanto ad essa consegue l'applicazione di multe o penali non particolarmente rilevanti.
2	**Basso**	La mancanza di **riservatezza** nel trattamento dei dati, **integrità** e **disponibilità** del dato relativi all'interessato **ha impatti lievi** sulla vita sociale o personale degli interessati (es: perdita di tempo necessario per correggere / reinserire le informazioni; fastidio; etc.).	I dati non presentano particolari requisiti di riservatezza. I dati sono pubblici
			I dati non presentano particolari requisiti di integrità. I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie.
			L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente non comporta multe o penali rilevanti.
1	**Irrilevante**	Gli interessati non incontrano inconvenienti significativi	----------

- Sottofase 2C) Calcolo dell'**Entità del Rischio**

Dalla combinazione dei due fattori **Probabilità x Magnitudo**

$$R = f(P, M) = P \times M$$

si è ricavata la seguente MATRICE DI RISCHIO con Gradualità:

		Magnitudo		
Probabilità	**1 (Irrilevante)**	**2 (Basso)**	**3 (Medio)**	**4 (Alto)**
1 (Improbabile)	1	2	3	4
2 Possibile	2	4	6	8
2 (Probabile)	3	6	9	12
3 (Quasi certo)	4	8	12	16

Misure di Prevenzione e protezione esistenti e % mitigazione

Descrizione	Rating		Rischio residuo	
Misure esistenti parzialmente adeguate	1-25%		6,1 - 16	Rischio Alto
Misure esistenti sufficienti	26-50%		3,1 - 6	Rischio Medio
Misure esistenti adeguate	51-75%		1-3	Rischio basso

e azioni conseguenti alla Valutazione del livello del **Rischio**:

Livello del rischio residuo	Azioni da intraprendere
Alto	Azioni di miglioramento necessarie a brevissimo termine
Medio	Azioni di miglioramento necessarie a medio termine
Accettabile (basso)	Monitoraggio mantenimento delle condizioni di sicurezza in essere. Possibili interventi finalizzati al miglioramento continuo

2.4.2 ANALISI DEI RISCHI

2.4.2.1 ACCESSO ILLEGITTIMO - PERDITA DELLA RISERVATEZZA		
Probabilità	I 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	2
Magnitudo **(Gravità del danno)**	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, ritorsioni.	3
Fonti di rischio	A) Fattore Umano: - Risorse umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale) - umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker)	
	B) Fattori di rischio legati alle infrastrutture e C) fattori di rischio legati al contesto (es. allagamenti, materiali pericolosi o virus informatici generici)	
Misure di mitigazione del rischio	Tutte le misure di prevenzione e protezione descritte al § 2.2.8	50%
Valutazione quantitativa	P x M =2 x3 = 6 x 50% =	3
Esito della valutazione	Rischio basso	

2.4.2.2 MODIFICHE INDESIDERATE - PERDITA DELL'INTEGRITA' DEL DATO		
Probabilità	I 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	2
Magnitudo **(Gravità del danno)**	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, ritorsioni.	3
Fonti di rischio	A) Fattore Umano: - Risorse umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale) - umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker)	
	B) Fattori di rischio legati alle infrastrutture e C) fattori di rischio legati al contesto (es. allagamenti, materiali pericolosi o virus informatici generici)	
Misure di mitigazione del rischio	Tutte le misure di prevenzione e protezione descritte al § 2.2.8	50%
Valutazione quantitativa	P x M =2 x3 = 6 x 50% =	3
Esito della valutazione	Rischio basso	

2.4.2.3 PERDITA DEL DATO - PERDITA DELLA DISPONIBILITA' DEL DATO		
Probabilità	I 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	2
Magnitudo **(Gravità del danno)**	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, ritorsioni.	3
Fonti di rischio	A) Fattore Umano: - Risorse umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale) - umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker)	
	B) Fattori di rischio legati alle infrastrutture e C) fattori di rischio legati al contesto (es. allagamenti, materiali pericolosi o virus informatici generici)	
Misure di mitigazione del rischio	Tutte le misure di prevenzione e protezione descritte al § 2.2.8	50%
Valutazione quantitativa	P x M =2 x3 = 6 x 50% =	3
Esito della valutazione	Rischio basso	

2.5 FASE 3. ESITO DELLA VALUTAZIONE E TRATTAMENTO DEI RISCHI

Esito della valutazione

L'Ordine degli Ingegneri della Provincia di Cagliari (OIC) ha elaborato la presente Valutazione di impatto sulla protezione dei dati "DPIA" (Data Protection Impact Assessment), secondo l'art.35 GDPR 2016/679, analizzando la documentazione del Sistema di Gestione Privacy, e valutando che:

- sono stati rispettati i principi fondamentali applicabili al trattamento dei dati personali di cui al Capo II del GDPR, ossia il principio di liceità, correttezza e trasparenza; il principio di limitazione della finalità; il principio di minimizzazione dei dati; il principio di esattezza dei dati; il principio di limitazione della conservazione dei dati; il principio di integrità e riservatezza.
- il sistema di gestione consente di dar seguito alle richieste di esercizio dei diritti degli interessati di cui al Capo III (diritto di informazione; diritto di accesso ai dati; diritto di portabilità dei dati; diritto di rettifica dei dati; diritto di cancellazione dei dati -"diritto all'oblio"-; diritto di limitazione del trattamento; diritto di opposizione al trattamento), in conformità con quanto definito dalla normativa in materia di whistleblowing;
- non è necessaria un'ulteriore consultazione dell'Autorità di controllo (Garante Privacy), rispetto alla prima consultazione tra il Garante e ANAC, in quanto le misure di prevenzione e protezione in essere permettono l'attenuazione dei rischi per i diritti e le libertà degli interessati ad un livello accettabile;

conclude si possa procedere con i trattamenti e che non siano necessarie ulteriori misure di salvaguardia oltre alle misure fisiche e logiche di prevenzione e protezione dai rischi già in atto.

2.5.1 ESITO DELLA VALUTAZIONE

La Valutazione di impatto sulla protezione dei dati si conclude con la definizione dell'**accettabilità del rischio** per il trattamento di dati personali nell'ambito dell'istituto del whistleblowing.

2.6 FASE 4. RIVALUTAZIONE PERIODICA

2.6.1 AGGIORNAMENTO DELLA VALUTAZIONE

La presente valutazione di impatto relativa ai trattamenti di dati personali svolti dall'**Ordine degli Ingegneri della Provincia di Cagliari (OIC)** verrà periodicamente riesaminata per adeguatezza e dovrà essere rivalutata in occasione di eventuali modifiche nei processi, anche in considerazione della natura di “processo continuo” della DPIA medesima.

INDICE

1 SEZIONE 1: INTRODUZIONE 3
1.1 SCOPO DELLA VALUTAZIONE DI IMPATTO (DPIA) E CAMPO D'APPLICAZIONE 3
1.2 NORMATIVA 3
1.2.1 RIFERIMENTI NORMATIVI E LINEE GUIDA 3
1.3 WHISTLEBLOWING E PROTEZIONE DEI DATI PERSONALI 4
1.3.1 WHISTLEBLOWING 4
1.3.2 RISERVATEZZA E PROTEZIONE DEI DATI 4
1.3.3 WHISTLEBLOWERS 4
1.3.4 CONTENUTO DELLE SEGNALAZIONI 4
1.3.5 MODALITA' DI SEGNALAZIONE: CANALI INTERNI ED ESTERNI 5
1.3.5.1 CANALI INTERNI 5
1.3.5.2 AUTORITA' NAZIONALE ANTI-CORRUZIONE (ANAC) E ALTRI CANALI ESTERNI 6
1.4 WHISTLEBLOWING E OBBLIGO DI REDAZIONE DELLA DPIA 6
1.4.1 Valutazione d'impatto sulla protezione dei dati (DPIA) 6
1.4.2 VALUTAZIONE PRELIMINARE DELLA NECESSITA' DI SVOLGIMENTO DELLA DPIA 6
1.5 METODOLOGIA OPERATIVA APPLICATA PER LA CONDUZIONE DELLA DPIA 7
1.5.1 riferimenti metodologici 7
1.5.2 SOGGETTO RESPONSABILE DELLA REDAZIONE DELLA DPIA 7
1.5.3 Casi previsti dal GDPR 7
1.5.4 CRITERI ENUNCIATI DAL WP 29 art.29 - CASI PARTICOLARI ED ESCLUSIONI 7
1.5.5 METODOLOGIA OPERATIVA: DETTAGLI 8
2 SEZIONE 2: VALUTAZIONE DI IMPATTO - DPIA 11
2.1 FASE 1: DEFINIZIONE DEL CONTESTO 11
2.1.1 GENERALITA' 11
2.1.2 DOCUMENTAZIONE DI RIFERIMENTO 11
2.1.3 REDAZIONE E VALIDAZIONE DELLA DPIA - PARERE CONCLUSIVO DEL DPO 11
2.1.4 RICHIESTA DEL PARERE DA PARTE DEGLI INTERESSATI - MOTIVAZIONE 11
2.2 DEFINIZIONE DELL'AMBITO DI ANALISI DELLA DPIA 12
2.2.1 DESCRIZIONE DEL TRATTAMENTO PRESO IN CONSIDERAZIONE 12
2.2.2 RESPONSABILITA' CONNESSE CON IL TRATTAMENTO 12
2.2.3 INTERESSATI AL TRATTAMENTO 12
2.2.4 ANALISI DEI DATI OGGETTO DEL TRATTAMENTO 13
2.2.5 DESCRIZIONE DEL CICLO DI VITA DEL TRATTAMENTO DEI DATI 13
2.2.6 STRUMENTI UTILIZZATI PER IL TRATTAMENTO 13
2.2.7 TRATTAMENTO E CICLO DI VITA DEI DATI 13
2.2.8 MISURE DI PREVENZIONE E PROTEZIONE DEI DATI PERSONALI RELATIVI AL WHISTLEBLOWING 14
2.2.8.1 MISURE APPLICATE AI DATI 14
2.2.8.2 MISURE ORGANIZZATIVE: 14
2.3 SCHEDA DPIA - WHISTLEBLOWING 15
2.4 FASE 2: VALUTAZIONE DEL RISCHIO 19
2.4.1 METODOLOGIA DI ANALISI 19

2.4.2 ANALISI DEI RISCHI 23
2.4.2.1 ACCESSO ILLEGITTIMO - PERDITA DELLA RISERVATEZZA 23
2.4.2.2 MODIFICHE INDESIDERATE - PERDITA DELL'INTEGRITA' DEL DATO 24
2.4.2.3 PERDITA DEL DATO - PERDITA DELLA DISPONIBILITA' DEL DATO 24
2.5 FASE 3. ESITO DELLA VALUTAZIONE E TRATTAMENTO DEI RISCHI 25
2.5.1 ESITO DELLA VALUTAZIONE 25
2.6 FASE 4. RIVALUTAZIONE PERIODICA 25
2.6.1 AGGIORNAMENTO DELLA VALUTAZIONE 25