UNIVERSITÀ DEL PIEMONTE ORIENTALE

DIREZIONE GENERALE
UFFICIO AFFARI GENERALI
E SERVIZI LEGALI
Trasparenza e anticorruzione

Via Duomo, 6 – 13100 Vercelli VC
Tel. 0161 261557-
E-mail: giuseppina.galizia@uniupo.it

GG

Decreto Rettorale
Rep. n. 2069/2022
Prot. n. 163643 del 15/12/2022

OGGETTO: Emanazione del Regolamento in materia di segnalazioni di illecito – whistleblowing ai sensi dell'art. 54 –bis, D.Lgs. n. 165/2001 e della Delibera ANAC N. 469/2021".

IL RETTORE

VISTO l'art. 13 comma 2, lettera b) dello Statuto di Ateneo, emanato con D.R. rep. n. 300 del 27.05.2014, secondo il quale "il *Consiglio di Amministrazione in particolare approva i regolamenti che rientrano nel proprio ambito di competenza";*

VISTA la delibera n. 12/2022/6.6 del 25.11.2022 del Consiglio di Amministrazione con la quale, ai sensi dell'art. 13 comma 2, lettera b) dello Statuto di Ateneo, è stato approvato, con voto espresso nella forma di legge, il testo del Regolamento in materia di segnalazioni di illecito – whistleblowing ai sensi dell'art. 54–bis, D.Lgs. n. 165/2001 e della Delibera ANAC N. 469/2021" (ALLEGATO A), comprensivo di allegati quali sue parti integranti e sostanziali:
a) ALLEGATO 1 - Approfondimenti misure di sicurezza adottate dal responsabile esterno del trattamento dati;
b) ALLEGATO 2 - Informativa sul trattamento dei dati personali;
c) ALLEGATO 3 - modello segnalazione whistleblowing aggiornato;

VALUTATO ogni opportuno elemento

DECRETA

1. È emanato, nel testo in allegato, il Regolamento "Regolamento in materia di segnalazioni di illecito – whistleblowing ai sensi dell'art. 54 –bis, D.Lgs. n. 165/2001 e della Delibera ANAC N. 469/2021", comprensivo di allegati quali sue parti integranti e sostanziali:
   a) ALLEGATO 1 – Approfondimenti misure di sicurezza adottate dal responsabile esterno del trattamento dati;
   b) ALLEGATO 2 - Informativa sul trattamento dei dati personali;
   c) ALLEGATO 3 - modello segnalazione whistleblowing aggiornato.

2. Il presente Regolamento sostituisce ogni procedura o disposizione precedentemente applicata qualora incompatibile con quanto in esso contenuto ed entra in vigore il giorno successivo dalla data del decreto rettorale di emanazione.

VISTO: LA DIRETTRICE GENERALE - RPCT DI ATENEO
(Dott.ssa Loredana SEGRETO)

F.to *Loredana SEGRETO*

IL RETTORE
(Prof. Gian Carlo AVANZI)

F.to *Gian Carlo AVANZI*

Documento informatico sottoscritto con firma digitale ai sensi del D.Lgs. n. 82/2005 e ss.mm.ii.

UNIVERSITÀ DEL PIEMONTE ORIENTALE

DIVISIONE RISORSE
UFFICIO AFFARI GENERALI
E SERVIZI LEGALI
Trasparenza e anticorruzione

Via Duomo, 6 – 13100 Vercelli VC
Tel. 0161 261557-
E-mail: giuseppina.galizia@uniupo.it

GG

ALLEGATO A

Regolamento in materia di segnalazioni di illecito – whistleblowing ai sensi dell'art. 54 –bis, D.Lgs. n. 165/2001 e della Delibera ANAC N. 469/2021

PREMESSA

L'Università degli Studi del Piemonte Orientale di seguito "UPO", crede e favorisce l'utilizzo del *whistleblowing* quale fondamentale misura di prevenzione della corruzione e della "*maladministration*", incoraggiando e tutelando tutti coloro che, nell'interesse all'integrità della Amministrazione, intendano segnalare fatti illeciti, secondo i migliori modelli nazionali ed internazionali.

Il presente Regolamento ha ad oggetto la disciplina relativa alla ricezione e alla gestione delle segnalazioni di illeciti che possano, in vario modo, interessare l'UPO nonché la tutela degli autori della segnalazione in attuazione di quanto previsto dall'art. 54-*bis*, del D.Lgs. 30 marzo 2001, n. 165, come modificato ad opera della L. n. 179/2017, e della Delibera A.N.AC. n. 469 del 9 giugno 2021, recante "*Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001 (c.d. whistleblowing)*".

La finalità del presente Regolamento è quella di fornire indicazioni operative ai soggetti coinvolti nel procedimento di ricezione e gestione delle segnalazioni di illecito, con particolare riguardo a:

a) i soggetti ai quali è consentito effettuare la segnalazione;

b) l'oggetto, i contenuti e le modalità di effettuazione della segnalazione;

c) le forme di tutela che devono essere garantite in favore del segnalante;

d) i soggetti deputati a ricevere la segnalazione;

e) le modalità di gestione della segnalazione;

f) i termini procedimentali;

g) la trasmissione della segnalazione ai soggetti competenti;

h) le responsabilità del segnalante e dei soggetti, in vario modo, coinvolti nel procedimento di gestione della segnalazione.

DEFINIZIONI

A.N.A.C.	l'Autorità Nazionale Anti Corruzione, di cui all'art. 1, comma 1, della L. 6 novembre 2012, n. 190, recante "*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione*"
ILLECITO	la condotta, attiva e/o omissiva, oggetto di segnalazione
DPF	Dipartimento della Funzione Pubblica
CUSTODE DELL'IDENTITA' DEL SEGNALANTE	Il RPCT, come a seguire definito
PTPCT	il Piano Triennale di Prevenzione della Corruzione e della Trasparenza dell'UPO
RPCT	il Responsabile della Prevenzione della Corruzione e della Trasparenza dell'UPO, nella rispettiva funzione di soggetto incaricato del compito di ricevere le segnalazioni di illecito e gestirne il procedimento fino alla trasmissione della segnalazione al soggetto competente
RESPONSABILE DEL PROCEDIMENTO DISCIPLINARE	il soggetto deputato alla gestione del procedimento disciplinare secondo quanto previsto dalla normativa e dalla prassi vigente nonché dalla contrattazione collettiva applicabile verso il personale dell'UPO, in ogni caso, soggetto diverso dal RPCT laddove il procedimento disciplinare scaturisca dalla segnalazione *whistleblowing*
SEGNALAZIONE	la segnalazione redatta dal segnalante, resosi identificabile, sulla base del modello allegato al presente Regolamento o comunque, se redatta in forma libera, contenente tutti i dati e le informazioni richieste nel medesimo modello allegato
SEGNALAZIONE ANONIMA	la denuncia di illeciti redatta senza l'indicazione dell'identità del segnalante
SEGNALANTE O *WHISTLEBLOWER*	il soggetto, interno o esterno all'UPO, che segnala agli organi legittimati episodi di Illecito o altre ipotesi di irregolarità commesse ai danni degli interessi perseguiti dall'UPO

Art. 1 - *Ambito di applicazione*

1. Il presente Regolamento si applica alle segnalazioni effettuate da:

- **b)** i dipendenti, in qualunque forma contrattuale, dell'UPO che, in ragione del proprio rapporto di lavoro, siano venuti a conoscenza di condotte illecite;
- **c)** i dipendenti e i collaboratori, a qualsiasi titolo (anche al di fuori del Codice dei contratti pubblici, di cui al D.Lgs. n. 50/2016), degli appaltatori di lavori, servizi e forniture in rapporto con l'UPO;
- **d)** i consulenti dell'UPO.

2. Il presente Regolamento si applica nei soli casi in cui i soggetti di cui al precedente comma, con l'effettuare la segnalazione, rendano nota la propria identità nei confronti degli organi deputati alla ricezione della segnalazione.

3. Nel caso in cui il segnalante non renda nota la propria identità al soggetto ricevente si applica quanto previsto dal presente Regolamento in materia di segnalazioni anonime.

4. Le disposizioni contenute nel presente Regolamento non esimono - in alcun modo - i soggetti che, rivestendo la qualifica di pubblico ufficiale o di incaricato di pubblico servizio, sono gravati dell'obbligo di denuncia ai sensi di quanto previsto dall'art. 331 del Codice di procedura penale e dagli artt. 361 e 362 del Codice penale.

5. Le segnalazioni effettuate da soggetti diversi da quelli di cui al comma 1, ivi inclusi i rappresentanti di organizzazioni sindacali, non rilevano quali segnalazioni *whistleblowing*.

6. Ai sensi della Delibera A.N.A.C. n. 469/2021, non rientrano tra i soggetti di cui al comma 1, coloro che, pur svolgendo un'attività lavorativa in favore dell'UPO, non sono dipendenti propriamente intesi (ad es., stagisti, tirocinanti).

7. Le segnalazioni effettuate da soggetti diversi da quelli di cui ai commi 1 e 6 al pari di quelle anonime, possono essere considerate dall'amministrazione nei procedimenti di vigilanza "ordinari" se ben dettagliate e circostanziate.

8. Il presente Regolamento si applica alle segnalazioni effettuate dai soggetti di cui al comma 1, lett. b), nei limiti in cui quanto segnalato riguardi illeciti o irregolarità relative all'UPO e non già all'impresa per la quale opera il segnalante. L'UPO, con adempimenti a cura del RPCT, adegua i propri standard contrattuali nell'ottica di consentire ai medesimi di effettuare le segnalazioni, assicurando l'accesso ai canali all'*uopo* dedicati, inclusi quelli informatici.

Art. 2 - *Oggetto della segnalazione*

1. Rientrano tra le condotte illecite per le quali è possibile effettuare la segnalazione:

a) l'intera gamma dei delitti contro la Pubblica Amministrazione di cui al Titolo II, Capo I, del Codice penale (es., i reati di corruzione per l'esercizio della funzione, corruzione per atto contrario ai doveri d'ufficio e corruzione in atti giudiziari, disciplinate rispettivamente agli artt. 318, 319 e 319-*ter* del predetto Codice);

b) le situazioni in cui, nel corso dell'attività lavorativa, si riscontri l'abuso da parte di un soggetto del potere a lui affidato al fine di ottenere vantaggi privati;

c) i fatti in cui – a prescindere dalla rilevanza penale – emerga un malfunzionamento dell'UPO (cd. *"maladministration"*) a causa dell'uso a fini privati delle funzioni attribuite (es.: casi di sprechi, nepotismo, demansionamenti, ripetuto mancato rispetto di eventuali tempi procedimentali, assunzioni non trasparenti ovvero avvenute in aperta violazione della normativa vigente; irregolarità contabili; false dichiarazioni; violazione delle norme ambientali e di sicurezza sul lavoro, etc.).

Il contenuto del fatto segnalato, in ogni caso, deve presentare elementi dai quali sia chiaramente desumibile una lesione, un pregiudizio, un ostacolo, un'alterazione del corretto ed imparziale svolgimento di un'attività o di un servizio pubblico o per il pubblico, anche sotto il profilo della credibilità e dell'immagine dell'UPO.

2. Il segnalante può segnalare le sole condotte illecite di cui al precedente comma del presente articolo delle quali sia venuto a conoscenza in ragione del rapporto di lavoro o di collaborazione/consulenza con UPO, ed in particolare:

a) le condotte illecite che abbia appreso in virtù dell'ufficio rivestito;

b) le notizie che siano state acquisite in occasione e/o a causa dello svolgimento delle mansioni lavorative ovvero di collaborazione, seppure in modo casuale.

3. In caso di trasferimento, comando, distacco (o situazioni analoghe) di un dipendente dell'UPO presso altro Ente tenuto agli obblighi in materia di anticorruzione e trasparenza, il dipendente medesimo potrà segnalare fatti illeciti accaduti in occasione del rapporto di lavoro con l'UPO al soggetto deputato a ricevere le segnalazioni presso l'Ente di destinazione oppure al RPCT dell'UPO.

4. Nel caso in cui la segnalazione sia effettuata da un dipendente dell'UPO proveniente da altro Ente soggetto agli obblighi in materia di anticorruzione e trasparenza e la segnalazione medesima abbia ad oggetto fatti illeciti accaduti durante il rapporto di lavoro instaurato con l'Ente di provenienza, l'UPO trasmetterà la segnalazione all'Ente di provenienza assicurando la riservatezza sulla identità del segnalante.

5. Ai fini della segnalazione non è necessario che il segnalante sia certo dell'effettivo accadimento dei fatti denunciati e dell'autore degli stessi, essendo sufficiente che il segnalante, in base alle proprie conoscenze, ne sia ragionevolmente convinto.

6. Possono formare oggetto di segnalazione attività illecite non ancora compiute ma che il segnalante ritenga ragionevolmente possano verificarsi in presenza di elementi precisi e concordanti.

7. La segnalazione dovrà, in ogni caso, essere quanto più possibile circostanziata e contenere il maggior numero di elementi al fine di consentire agli organi competenti di effettuare le dovute verifiche.

8. Non sono meritevoli di tutela e, conseguentemente, non sono oggetto di esame da parte dell'UPO, le segnalazioni basate su mere supposizioni e/o sospetti e/o opinioni personali del segnalante e/o di eventuali terzi dal medesimo indicati.

9. Le tutele di cui al presente Regolamento non operano nei confronti del segnalante che viola la legge al fine di raccogliere informazioni, indizi o prove di illeciti in ambito lavorativo.

10. Le tutele di cui al presente Regolamento non operano in relazione alle segnalazioni di informazioni che siano già totalmente di dominio pubblico, alle notizie prive di fondamento e alle c.d. "voci di corridoio".

Art. 3 - *Disciplina della segnalazione anonima*

1. La segnalazione anonima è oggetto di valutazione in termini di ammissibilità e fondatezza secondo quanto previsto dal presente articolo.

2. L'UPO prende in considerazione la segnalazione anonima quando la stessa sia adeguatamente circostanziata e resa con dovizia di particolari e comunque tale da far emergere fatti e situazioni

relazionandoli a contesti determinati (es.: indicazione di nominativi o qualifiche particolari, menzione di uffici specifici, procedimenti o eventi particolari, etc.).

Art. 4 - *Modalità per la effettuazione della segnalazione e soggetti deputati alla ricezione*

1. La segnalazione, anche se già trasmessa all'Autorità giudiziaria, alla Corte dei conti o all'A.N.AC., deve essere indirizzata al RPCT - unico destinario dell'UPO competente a ricevere e gestire le segnalazioni aventi rilevanza agli effetti del presente Regolamento - utilizzando preferibilmente il modello di segnalazione allegato al presente Regolamento - reperibile sul sito web istituzionale dell'UPO, sezione "Regolamenti, trasparenza, sindacati" – "Trasparenza e anticorruzione" e sezione "Amministrazione Trasparente" - "Altri contenuti", ricorrendo alternativamente alle seguenti modalità:

a) in via telematica, tramite la piattaforma dedicata, denominata "Whistleblowing Intelligente" reperibile al link:

https://www.uniupo.it/it/segnalazione-illeciti-whistleblowing sull'apposito:

- link per il dipendente, qualificandosi obbligatoriamente attraverso il sistema SPID: https://wb.anticorruzioneintelligente.it/anticorruzione/index.php?codice=UELEXG&dipendente=1:
- link per il cittadino, in cui non è richiesta l'identificazione tramite SPID e non è obbligatorio inserire i dati relativi all'identità del segnalante**:** https://wb.anticorruzioneintelligente.it/anticorruzione/index.php?codice=UELEXG&dipendente=0 . In questo caso non potranno essere concesse al segnalante le tutele previste dalla legge.

Il segnalante è tenuto a compilare in modo esaustivo chiaro, preciso e circostanziato le sezioni del modulo di segnalazione, fornendo le informazioni richieste come obbligatorie e il maggior numero possibile di quelle facoltative. Al segnalante si richiede un comportamento collaborativo tenendo costantemente aggiornato l'Ateneo in ordine all'evoluzione della propria segnalazione/comunicazione secondo le modalità più avanti illustrate.

All'invio della segnalazione, la piattaforma presenta al segnalante una videata con il codice univoco di segnalazione, necessario per:

- integrare/aggiornare in un secondo momento quanto riportato nel modulo di segnalazione;
- rispondere ad eventuali richieste di chiarimenti/approfondimenti;
- verificare l'avanzamento dell'iter di gestione della segnalazione.

Il codice univoco di segnalazione non può essere rigenerato dalla piattaforma. Pertanto, il segnalante dovrà conservarlo con cura per poter rientrare nella segnalazione al fine di verificarne l'iter di esame, per rispondere ad eventuali richieste del RPCT o, ancora, per integrare spontaneamente le informazioni già sottoposte all'attenzione del RPCT.

b) in forma cartacea, tramite lettera in doppia busta chiusa, recante la dicitura *"Riservata per il RPCT dell'UPO - Segnalazione Whistleblowing"*, da spedire, al seguente indirizzo*:* Palazzo del

Rettorato, Via Duomo n. 6 – 13100 Vercelli, a mezzo posta ordinaria o raccomandata con ricevuta di ritorno o consegna "*brevi manu*" in sede;

c) in posta elettronica, indirizzo istituzionale: anticorruzione@uniupo.it.

2. Al fine di facilitare il segnalante, nel caso in cui il canale prioritario della piattaforma presenti momentanee disfunzioni o l'interessato non abbia familiarità con le procedure informatiche o non sia in possesso di strumenti informatici, l'Università ha predisposto un modello per la segnalazione allegato al presente regolamento (ALLEGATO 3).

3. Qualora la segnalazione riguardi il RPCT o, qualora fosse costituito un ufficio di supporto nel caso dedicato alla gestione delle segnalazioni *whistleblowing*, un componente dell'ufficio di supporto, il segnalante può inviare la segnalazione direttamente all'A.N.A.C. ovvero alle altre Autorità competenti, secondo quanto previsto dalla legge. Le indicazioni operative per la registrazione al sistema dedicato nonché i termini e le regole tecniche per la trasmissione della segnalazione all'A.N.A.C. sono reperibili sul sito: *www.anticorruzione.it*., al seguente url: https://servizi.anticorruzione.it/segnalazioni/#!/#%2F

4. Le segnalazioni di misure ritorsive nei confronti di chi ha fatto una segnalazione di Whistleblowing, devono essere inviate esclusivamente tramite la piattaforma messa a disposizione dall'A.N.A.C.

5. Le segnalazioni whistleblowing di cui sopra ricevute da soggetti diversi dal RPCT devono essere tempestivamente e, comunque, entro 24 (ventiquattro) ore dalla ricezione, trasmesse a quest'ultimo, a pena di sanzione disciplinare.

6. In aderenza alle linee di indirizzo offerte in termini di principio dalla Direttiva (UE) 2019/1937 l'UPO raccomanda di trasmettere la segnalazione, in prima istanza, al RPCT.

7. In relazione alla gestione delle segnalazioni *whistleblowing* tramite piattaforma informatica, "canale primario" di acquisizione delle segnalazioni, l'UPO assicura adeguati standard di sicurezza, tenendo conto delle indicazioni di cui alla Delibera n. 469/2021.

Art. 5 - Riservatezza dell'identità del segnalante

1. L'identità del segnalante non può essere rivelata.

2. 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.

3. Qualora la contestazione dell'illecito disciplinare sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identità.

4. Il Responsabile del procedimento disciplinare valuta, su istanza dell'incolpato, se ricorrono i presupposti in ordine alla necessità di conoscere l'identità del segnalante ai fini del diritto di difesa, dando adeguata motivazione della sua decisione sia in caso di accoglimento dell'istanza sia in caso

di diniego. Il Responsabile del procedimento disciplinare si pronuncia sull'istanza dell'incolpato entro 5 (cinque) giorni lavorativi dalla ricezione dell'istanza dell'incolpato, comunicando l'esito a quest'ultimo e al RPCT.

5. È fatto divieto assoluto al RPCT e, qualora fosse costituito un un ufficio di supporto nel caso dedicato alla gestione delle segnalazioni *whistleblowing*, al suddetto ufficio di supporto, di cui al presente Regolamento di rendere nota, in assenza di presupposti, l'identità del segnalante al Responsabile del procedimento disciplinare.

6. Nell'ambito del procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'art. 329 del Codice di procedura penale.

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

8. Restano ferme le disposizioni di legge speciale che impongono che l'identità del segnalante debba essere rivelata esclusivamente alle Autorità procedenti (es.: indagini penali, tributarie o amministrative, ispezioni, etc.).

9. La segnalazione e la documentazione alla stessa allegata sono, in ogni caso, sottratte all'accesso agli atti amministrativi ex artt. 22 e seguenti della L. n. 241/1990, all'accesso civico generalizzato di cui all'art. 5, comma 2, del D.Lgs. 33/2013 nonché all'accesso di cui all'art. 2-undecies, comma 1, lett. f), del D.Lgs. 196/2003.

10. Nell'informativa in merito al trattamento dei dati personali, resa al segnalante all'atto della segnalazione, anche mediante piattaforma telematica, quest'ultimo è informato dell'eventualità per la quale la segnalazione potrebbe essere trasmessa ai soggetti competenti secondo quanto previsto dalla legge.

Art. 6 - *Ulteriori tutele in favore del segnalante*

1. Il dipendente dell'UPO che segnali al RPCT, all'Autorità giudiziaria, alla Corte dei Conti o all'A.N.A.C. condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro, non può essere sanzionato, demansionato, licenziato, trasferito, o sottoposto ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro determinata dalla segnalazione.

2. L'adozione di misure ritenute ritorsive di cui al precedente comma nei confronti del segnalante é comunicata in ogni caso all'A.N.A.C. dall'interessato, dal RPCT o dalle organizzazioni sindacali maggiormente rappresentative dell'UPO, ove esistenti. L'A.N.A.C. informa il DFP della Presidenza del Consiglio dei ministri o gli altri organismi di garanzia o di disciplina per le attività e gli eventuali provvedimenti di competenza.

3. È a carico dell'UPO dimostrare che le misure discriminatorie o ritorsive - se ed in quanto accertate tali - adottate nei confronti del segnalante, siano motivate da ragioni estranee alla segnalazione stessa.

4. Gli atti accertati discriminatori o ritorsivi adottati sono nulli.

5. Il segnalante che sia licenziato a motivo della segnalazione è reintegrato nel posto di lavoro ai sensi dell'art. 2, del D.Lgs. 4 marzo 2015, n. 23.

6. Le tutele del segnalante di cui al presente Regolamento non sono garantite nei casi in cui sia accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante medesimo per i reati di calunnia o diffamazione o comunque per reati commessi con la denuncia ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave.

Art. 7 - *Integrazione della disciplina dell'obbligo di segreto d'ufficio, aziendale, professionale, scientifico e industriale*

1. Nelle segnalazioni effettuate nel rispetto di quanto previsto dal presente Regolamento nonché dell'art. 54-*bis*, del D.Lgs. 165/2001, il perseguimento dell'interesse all'integrità delle Pubbliche Amministrazioni, inclusa l'UPO, nonché alla prevenzione e alla repressione delle malversazioni, costituisce giusta causa di rivelazione di notizie coperte dall'obbligo di segreto di cui agli artt. 326, 622 e 623 del Codice penale e all'art. 2105 del Codice civile.

2. La disposizione di cui al precedente comma non si applica nel caso in cui l'obbligo di segreto professionale gravi su chi sia venuto a conoscenza della notizia in ragione di un rapporto di consulenza professionale o di assistenza con l'UPO o la persona fisica interessata.

3. Quando notizie e documenti che sono comunicati al RPCT siano oggetto di segreto aziendale, professionale o d'ufficio, costituisce violazione del relativo obbligo di segreto la rivelazione con modalità eccedenti rispetto alle finalità dell'eliminazione dell'illecito e, in particolare, la rivelazione al di fuori dei canali previsti per l'effettuazione della segnalazione previsti dalla presente Procedura.

Art. 8 – *Fasi del procedimento di gestione delle segnalazioni whistleblowing*

1. Il procedimento di gestione delle segnalazioni *whistleblowing* è composto dalle seguenti fasi:

a) ricezione e protocollazione della segnalazione;

b) valutazione preliminare della segnalazione;

c) fase istruttoria;

d) trasmissione della segnalazione al soggetto competente.

Art. 9 - *Fase di ricezione e protocollazione della segnalazione*

1. Il procedimento di gestione delle segnalazioni *whistleblowing* è avviato a seguito della ricezione della segnalazione.

2. Entro 2 (due) giorni lavorativi dalla ricezione della segnalazione, il RPCT procede:

a) ove non già effettuato - in automatico - dalla piattaforma informatica, alla protocollazione su registro riservato alle segnalazioni *whistleblowing,* attribuendo un codice univoco progressivo, registrando la data e l'ora di ricezione.
La piattaforma informatica, dopo aver attribuito alla segnalazione un numero progressivo e la data di ricezione, invia alla casella di posta elettronica indicata dal RPCT in fase di impostazione, un messaggio di avviso. Nessuna informazione circa il contenuto della segnalazione sarà inviata via mail;

b) se strettamente necessario ai fini della gestione della segnalazione, e ove non già precisato nell'istanza, alla corretta identificazione del segnalante acquisendone, oltre all'identità, anche la qualifica e il ruolo e tutti gli ulteriori dati ritenuti utili ai fini della valutazione preliminare della segnalazione;

c) ove non già effettuato - in automatico - dalla piattaforma informatica, alla separazione dei dati identificativi del segnalante dal contenuto della segnalazione, attraverso l'adozione di codici sostitutivi dei dati identificativi, in modo che la segnalazione possa essere gestita in forma anonima e rendere possibile la successiva associazione della segnalazione con l'identità del segnalante nei soli casi previsti dal presente Regolamento;

d) all'adozione di ogni opportuna misura di sicurezza per impedire a terzi di risalire all'identità del segnalante nonché alla conservazione della segnalazione e della documentazione a corredo in luogo segreto;

e) ove non già confermato - in automatico - dalla piattaforma informatica, alla tempestiva trasmissione di apposita *informazione* di *"conferma di avvenuta ricezione"* al segnalante - se è stato indicato nel modulo di segnalazione un indirizzo di posta elettronica - con l'indicazione del numero di protocollo assegnato alla segnalazione e dei codici sostitutivi dell'identità del segnalante, sottolineando l'assoluta segretezza dei dati e il divieto della loro diffusione.

3. Il RPCT, nell'ambito delle attività di ricezione e gestione della segnalazione, può avvalersi - ove assolutamente necessario ed in via del tutto straordinaria, previa adozione delle dovute misure tecniche ed organizzative ai sensi della disciplina in materia di protezione dei dati personali - di un gruppo di lavoro dedicato, formato da dipendenti dell'UPO, da individuare con specifico atto di nomina del Consiglio di Amministrazione, su proposta del RPCT. L'atto di nomina è reso pubblico sulla intranet aziendale.

4. Non possono fare parte del gruppo di lavoro dedicato di cui al precedente comma i dipendenti dell'UPO che:

a) operano nelle aree a maggior rischio (es., Amministrazione, Appalti, Personale, etc.);

b) svolgono funzioni di supporto nell'ambito della gestione dei procedimenti disciplinari.

5. In capo al RPCT e a ciascun componente del gruppo di lavoro dedicato di cui al presente articolo grava l'obbligo di assoluta riservatezza sull'identità del segnalante. La rivelazione dell'identità del segnalante fuori dai casi previsti dal presente Regolamento costituisce grave illecito disciplinare.

6. Il RPCT e, qualora fosse costituito un ufficio di supporto nel caso dedicato alla gestione delle segnalazioni *whistleblowing*, i componenti del suddetto ufficio di supporto dedicato di cui al presente articolo devono astenersi in caso di conflitto di interessi, anche solo apparente o

potenziale, e sono contestualmente tenuti a segnalare tale conflitto al Consiglio di Amministrazione.

7. Fermo restando quanto previsto con riferimento all'identità del segnalante, il RPCT e, qualora fosse costituito un ufficio di supporto nel caso dedicato alla gestione delle segnalazioni *whistleblowing*, i componenti dell'ufficio di supporto dedicato di cui al presente articolo mantengono riservata l'indentità del segnalato e i contenuti della segnalazione durante l'intera fase di gestione della medesima e, comunque, fintantoché risulti necessario.

8. I dati personali del segnalante e di tutti gli ulteriori soggetti coinvolti in conseguenza della segnalazione, ivi compreso il segnalato, sono trattati nel rispetto di quanto previsto dal D.Lgs. 30 giugno 2003, n. 196 (Codice Privacy) e del Regolamento UE 2016/679.

Art. 10 - *Fase di valutazione preliminare della segnalazione e attività di verifica del RPCT*

1. Il RPCT, anche avvalendosi dell'ufficio di supporto dedicato alla gestione delle segnalazioni, qualora il suddetto ufficio di supporto fosse costituito, effettua una valutazione preliminare sui contenuti della segnalazione ricevuta al fine di:

a) appurare la gravità e la rilevanza della condotta illecita imputata al segnalato;

b) verificare se la segnalazione sia effettivamente sorretta dall'interesse del segnalante a tutelare l'integrità dell'UPO e/o alla prevenzione/repressione delle malversazioni in danno della medesima;

c) verificare la presenza di concorrenti interessi personali del segnalante ovvero di altri soggetti in rapporto con quest'ultimo.

Circa la procedura informatizzata, per compiere l'analisi preliminare, il RPCT si autentica sulla piattaforma al seguente URL: https://wb.anticorruzioneintelligente.it/login.php digitando nome e password o, in alternativa, attraverso il sistema SPID. Nell'apposita sezione della piattaforma, il RPCT individua ed entra nella nuova segnalazione prendendone visione. I dati riferiti all'identità del segnalante non sono visibili. La piattaforma mette la segnalazione in stato "Analisi preliminare" ed invia al segnalante (se questi ha lasciato i suoi riferimenti di posta elettronica) una notifica di passaggio di stato della segnalazione). Il RPCT può procedere all'esame preliminare della segnalazione.

d) ove necessario, svolgere attività di verifica e, comunque, chiedere al segnalante e/o ad eventuali altri soggetti coinvolti nella segnalazione gli occorrendi chiarimenti e/o integrazioni, anche documentali, adottando le opportune cautele per garantire la riservatezza del segnalante. Il messaggio inviato al segnalante interrompe automaticamente il conteggio del tempo necessario per concludere la fase di analisi preliminare, che riprenderà automaticamente al momento in cui il segnalante risponde all'RPCT. Nel caso di utilizzo della procedura automatizzata, il suddetto conteggio del tempo riprende con la ricezione del messaggio del segnalante all'interno della piattaforma informatica alle richieste ricevute dall'RPCT e, quest'ultimo, viene immediatamente avvertito con un messaggio in posta elettronica senza riportare nessun dato o informazione utile a rivelare il contenuto della segnalazione o sue parti.

Decorsi 7 giorni senza ricevere alcuna risposta, il RPCT riprende l'iter di valutazione con le informazioni disponibili.

e) identificare i soggetti terzi competenti all'adozione dei conseguenti provvedimenti.

2. Il RPCT dichiara inammissibile la segnalazione, procedendo alla relativa archiviazione per:

a) manifesta mancanza di interesse all'integrità dell'UPO;

b) manifesta incompetenza dell'UPO sulle questioni segnalate;

c) manifesta infondatezza per l'assenza di elementi di fatto idonei a giustificare accertamenti;

d) accertato contenuto generico della segnalazione di illecito tale da non consentire la comprensione dei fatti, ovvero segnalazione di illeciti corredata da documentazione non appropriata o inconferente;

e) produzione di sola documentazione in assenza della segnalazione di condotte illecite o irregolarità;

f) mancanza dei dati che costituiscono elementi essenziali della segnalazione, quali la denominazione e i recapiti del *whistleblower,* i fatti oggetto di segnalazione, le ragioni connesse all'attività lavorativa svolta che hanno consentito la conoscenza dei fatti segnalati.

3. Nei casi di cui alle lettere c) ed f) del comma precedente, il RPCT formula richieste di integrazioni e chiarimenti. In caso di utilizzo della procedura informatizzata, la segnalazione verrà posta in stato "istruttoria" e il segnalante sarà avvertito con messaggio in posta elettronica del cambiamento di stato della segnalazione e, se chiusa, delle motivazioni.

4. La fase di valutazione preliminare deve concludersi entro 15 (quindici) giorni decorrenti dalla ricezione della segnalazione.

Art. 11 - *Fase istruttoria*

1. Ove necessario, il RPCT avvia la propria attività istruttoria nel rispetto dei principi di tempestività, indipendenza, equità e riservatezza. Nel corso delle verifiche, il RPCT può chiedere il supporto degli uffici dell'Amministrazione di volta in volta competenti e, ove ritenuto opportuno, di Autorità pubbliche, o, ancora, di consulenti esterni specializzati nell'ambito della segnalazione ricevuta ed il cui coinvolgimento sia funzionale all'accertamento della segnalazione, assicurando la riservatezza e l'anonimizzazione dei dati personali eventualmente contenuti nella segnalazione.

2. Le strutture dell'UPO interessate dall'attività di verifica del RPCT garantiscono la massima e tempestiva collaborazione.

3. La metodologia da impiegare nello svolgimento delle attività di verifica è valutata, di volta in volta, individuando la tecnica ritenuta più efficace, considerata la natura dell'evento sottostante alla violazione e le circostanze esistenti.

4. Le verifiche possono essere eseguite, a titolo esemplificativo, mediante: analisi documentali, interviste, somministrazione di questionari, ricerca di informazioni su database pubblici, nel

rispetto della normativa sulla protezione dei dati personali nonché, ove ritenuta pertinente, della normativa in materia di indagini difensive.

5. In nessun caso sono consentite verifiche lesive della dignità e della riservatezza del dipendente e/o verifiche arbitrarie, non imparziali o inique, tali da screditare il dipendente ovvero da comprometterne il decoro davanti ai colleghi.

6. In caso di utilizzo della piattaforma informatizzata, il RPCT avrà la possibilità di tenere all'interno della piattaforma un diario in riferimento alle attività istruttorie effettuate ed, inoltre, sarà possibile scrivere la relazione delle risultanze delle attività istruttorie senza ricorrere al download/upload di file.

7. Anche in questa fase è possibile, come descritto nella fase precedente, attivare un dialogo a distanza tra RPCT e segnalante. L'invio di un messaggio da parte del RPCT interrompe il conteggio dei giorni utili per la conclusione della fase istruttoria. Decorsi 15 giorni senza aver ricevuto risposta, il RPCT può decidere di proseguire l'istruttoria avvalendosi dei soli elementi disponibili. Al termine dell'istruttoria, in caso di utilizzo della piattaforma informatizzata, la segnalazione sarà messa in stato "Chiusa" indicando la motivazione e l'azione seguente compiuta, ovvero archiviata (come discipllinato nel successivo co. 8) oppure inviata ad uno o più soggetto competenti come stabilito nell'art. 12).

8. Nel caso in cui, all'esito della fase istruttoria, la segnalazione sia ritenuta manifestamente infondata, il RPCT procede all'archiviazione della segnalazione medesima, dandone comunicazione al segnalante, al Consiglio di Amministrazione.

9. La fase istruttoria deve concludersi, di norma, entro 60 (sessanta) giorni decorrenti dalla data di avvio della fase medesima.

10. Ove necessario, il Consiglio di Amministrazione può autorizzare il RPCT a estendere il predetto termine fornendo adeguata motivazione.

Art. 12 - *Fase di trasmissione della segnalazione al soggetto competente*

1. Nel caso in cui, all'esito della valutazione preliminare di cui al comma 1 del precedente articolo, la segnalazione non sia ritenuta manifestamente infondata, il RPCT valuta, in relazione ai profili di illiceità riscontrati e ai contenuti della segnalazione, a chi inoltrare la segnalazione medesima, individuando i destinatari tra i seguenti soggetti:

a) se competente, e per i soli casi in cui non si ravvisino ipotesi di reato, il Dirigente della struttura dell'UPO alla quale è ascrivibile il fatto;

b) il Responsabile del procedimento disciplinare a carico dell'incolpato ai soli effetti dell'avvio del procedimento in questione;

c) l'Autorità giudiziaria, la Corte dei Conti, l'A.N.A.C, per i profili di rispettiva competenza;

d) il Dipartimento della Funzione Pubblica, per quanto di competenza rispetto alle misure ritorsive e/o discriminatorie eventualmente assunte in danno del segnalante.

2. In ogni caso, il RPCT provvede a comunicare l'esito del propria valutazione preliminare al Consiglio di Amministrazione, per le ulteriori eventuali azioni che si rendano necessarie a tutela della medesima Amministrazione.

3. In caso di trasmissione della segnalazione il RPCT trasmette solo i contenuti della segnalazione medesima, espungendo tutti i riferimenti dai quali sia possibile risalire all'identità del segnalante.

4. Poiché nella documentazione trasmessa potrebbero essere presenti dati di altri interessati, i soggetti che trattano i dati sono comunque "autorizzati" al riguardo (artt. 4, par. 1, n. 10,29,32 e par.4 del Regolamento UE n. 679/2016).

5. Il Responsabile del procedimento disciplinare informa tempestivamente il RPCT dell'adozione di eventuali provvedimenti di propria competenza a carico dell'incolpato.

6. In caso di trasmissione verso i soggetti di cui al comma 1, lett. d) il RPCT inoltra la segnalazione secondo le indicazioni diramate dall'A.N.A.C., a mezzo posta elettronica certificata o lettera A.R., tramite plico chiuso, con indicazione della dicitura *"Riservata – Segnalazione whistleblowing ex art. 54-bis del D.Lgs. 165/2001"*.

7. Il RPCT, all'atto della trasmissione della segnalazione, invia al segnalante apposita comunicazione contenente l'indicazione dei soggetti verso i quali la segnalazione è stata trasmessa.

8. La trasmissione della segnalazione deve avvenire, di norma, entro 2 (due) giorni decorrenti dall'esaurimento della fase di valutazione preliminare della segnalazione.

Art. 13 - *Notizie sullo stato della segnalazione*

1. Il segnalante può, in qualunque momento, chiedere informazioni al RPCT sullo stato di avanzamento del procedimento mediante l'invio di apposita richiesta, secondo le modalità indicate dal RPCT medesimo. Il segnalante, altresì, in caso di utilizzo della procedura informatizzata, può integrare/aggiornare le informazioni già riportate nel modulo di segnalazione, oppure può prendere visione dell'iter di esame della segnalazione ed eventuali messaggi ricevuti da parte del RPCT entrando nella piattaforma secondo le modalità già indicate e inserendo il codice univoco di segnalazione dopo aver fatto clic sul pulsante "Verifica stato segnalazione". Se il segnalante ha inserito un indirizzo di posta elettronica all'interno del modulo di segnalazione, la piattaforma provvederà ad inviare via email tutte le notifiche di cambio stato della segnalazione ed eventuali richieste di informazioni/integrazioni da parte del RPCT. All'interno della mail sarò presente anche un link che consentirà di accedere automaticamente alla segnalazione senza dover digitare il codice univoco.

2. Il RPCT, ove non ricorrano gravi ragioni impeditive (es. indagini penali in corso e corrispondenti obblighi di segreto), risponde alla richiesta di informazioni di cui al precedente comma entro il termine di 5 (cinque) giorni lavorativi decorrenti dalla data di ricezione della richiesta medesima.

Art. 14 - *Il Custode dell'identità del segnalante e l'accesso ai dati*

1. Il RPCT svolge anche il ruolo di Custode dell'identità del segnalante e ha sempre la possibilità di accedere ai dati identificativi del segnalante per gli usi consentiti o richiesti dalla legge.

2. L' accesso ai dati identificativi del segnalante da parte del RPCT è motivato e la motivazione, in caso di utilizzo della procedura informatizzata, viene registrata all'interno della piattaforma. Il Segnalante riceve avviso delle motivazioni per le quali i suoi dati identificativi sono stati messi in chiaro. Il RPCT ha comunque la possibilità di ri-oscurare i dati relativi al segnalante in modo tale da poter esportare in PDF la segnalazione, qualora ne ravvisi la necessità, senza rendere visibili i dati identificativi del segnalante.

3. Laddove l'Autorità giudiziaria per esigenze istruttorie volesse conoscere il nominativo del segnalante, il responsabile della prevenzione della corruzione e della trasparenza provvede a comunicare l'identità del segnalante, così come previsto dalle disposizioni di legge. È opportuno precisare che il whistleblower, in caso di utilizzo della procedura informatizzata, è preventivamente avvisato, attraverso l'informativa presente nel modulo di segnalazione, della eventualità che la sua segnalazione potrà essere inviata all'Autorità giudiziaria ordinaria e contabile.

Art. 15 - *Il consenso a rivelare l'identità del segnalante nell'ambito del procedimento disciplinare*

1. Qualora si rendesse necessario, il segnalante ha la possibilità di esprimere chiaramente e inequivocabilmente il consenso a rivelare le sue generalità nell'ambito di un procedimento disciplinare originatosi a seguito della segnalazione. In caso di utilizzo della procedura informatizzata, il Segnalante, quando rientra nella segnalazione, ha a disposizione un pulsante con il quale può acconsentire o meno a rivelare la sua identità nell'ambito del procedimento disciplinare. In caso in cui egli esprima il suo consenso, tale scelta non sarà più revocabile.

2. La piattaforma registra e rende visibile data e ora in cui è stato accordato il consenso.

3. Appena espresso il consenso, la piattaforma invia un messaggio al RPCT per informarlo della scelta avvenuta da parte del segnalante.

Art. 16 - *La perdita delle tutele*

1. Il co. 9 dell'art. 54-bis del D.Lgs. n. 165/2001 stabilisce che la tutela non è più garantita nel caso in cui il whistleblower non svolga la segnalazione in buona fede, precisando che la protezione per quest'ultimo viene meno ove sia accertata, anche con sentenza di primo grado, la sua responsabilità penale per i reati di calunnia o diffamazione o per quelli comunque commessi con la segnalazione, ovvero la sua responsabilità civile, nei casi di dolo o colpa grave.

2. Laddove la sentenza di condanna in primo grado dovesse essere riformata in senso favorevole al segnalante nei successivi gradi di giudizio, quest'ultimo potrà ottenere nuovamente la tutela prevista dall'art. 54-bis del D.Lgs. n. 165/2001 solo a seguito del passaggio in giudicato della

pronuncia che accerta l'assenza della sua responsabilità penale per i reati di calunnia e/o diffamazione e/o commessi con la segnalazione.

3. Solo dove intervenga, in sede giudiziaria, l'accertamento della responsabilità per dolo o colpa grave in merito alla condotta calunniosa o diffamatoria messa in atto attraverso la segnalazione, l'UPO potrà sanzionare disciplinarmente il segnalante.

Art. 17 - *Conservazione di dati, disposizioni sul trattamento dei dati personali e ulteriori misure di sicurezza*

1. Le segnalazioni pervenute e la documentazione a corredo delle medesime sono conservate, a cura del RPCT, presso i locali dell'UPO individuati dal RPCT, previa adozione di ogni opportuna cautela al fine di garantirne la massima riservatezza. Circa la procedura informatizzata, la segnalazione sarà resa disponibile tanto al segnalante tanto al RPCT per 5 anni. Indipendentemente dallo stato della segnalazione, segnalante e RPCT potranno utilizzare la chat asincrona contenuta nel modulo di segnalazione anche quando a segnalazione già esaminata.

2. Salvo quanto previsto da specifiche disposizioni di legge, l'accesso ai dati inerenti alle segnalazioni é consentito esclusivamente al RPCT e agli eventuali componenti dell'ufficio di supporto dedicato, previa autorizzazione del RPCT.

3. Nell'ambito delle attività di trattamento previste dal presente regolamento, l'Università adotta ogni cautela al fine di evitare la indebita circolazione di informazioni personali, non solo verso l'esterno, ma anche all'interno degli uffici dell'Università in capo a soggetti non autorizzati al trattamento dei dati, anche mediante:

- una corretta configurazione dei sistemi di protocollo informatico;
- l'individuazione di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti in esame;
- la definizione di un idoneo modello di gestone delle segnalazioni in conformità ai principi di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita, tenuto conto anche delle eventuali osservazioni presentate al riguardo dal Responsabile della protezione dei dati personali.

Circa l'applicativo utilizzato per acquisire e gestire le segnalazioni si rimanda all'ALLEGATO 1 del presente Regolamento.

4. Le Informazioni di cui all'art. 13 del Regolamento (EU) 2016/679 sopra riportate sono inserite anche nell'informativa allegata al presente regolamento (ALLEGATO 2) che verrà pubblicata sul sito istituzionale dell'Ateneo e nella sezione "Amministrazione Trasparente/Altri contenuti/Whistleblowing".

Art. 18 - *Gli obblighi di sicurezza*

1. Il RPCT è obbligato alla riservatezza e a non rivelare a nessun altro, se non nei casi previsti dalla legge, l'identità del segnalante. Restano ferme le responsabilità disciplinari previste per violazione degli appositi doveri di comportamento e per violazione delle norme sulla tutela dei dati personali.

2. La Società Tecnolink S.r.l. è ideatrice e proprietaria della piattaforma Whistleblowing Intelligente e si occupa di fornire il software in modalità Software as a Service (SaaS). La Tecnolink S.r.l nella persona del suo legale rappresentante pro tempore, è stata nominata Responsabile esterno del trattamento dei dati personali. L'Università degli Studi del Piemonte Orientale, nell'ambito di quanto previsto nell'atto di nomina, verifica e controlla le modalità operative con cui il Responsabile esterno assicura il trattamento dei dati personali in piena conformità a quanto previsto dal Regolamento (UE) 2016/679 in particolar modo per le parti richiamate dalle Linee Guida ANAC in materia di Whistleblowing adottate con delibera n. 469 del 9 giugno 2021 (per un dettaglio delle misure di sicurezza adottate dal Responsabile esterno del trattamento dati vedasi l'Allegato 1).

Art. 19 - *Analisi periodica delle informazioni in materia di whistleblowing*

4. Il RPCT, anche con il supporto dell'ufficio di lavoro dedicato alla gestione della segnalazioni, raccoglie e organizza, periodicamente ed in forma anonima, i dati relativi alle segnalazioni e allo stato dei procedimenti di gestione delle segnalazioni medesime (es. numero di segnalazioni ricevute, tipologie di illeciti segnalati, ruoli e funzioni degli incolpati, tempi di definizione del procedimento disciplinare, etc.) pervenute in corso d'anno, al fine di:

a) identificare le aree di criticità dell'UPO sulle quali risulti necessario intervenire in termini di miglioramento e/o implementazione del sistema di controllo interno;

b) introdurre nuove misure specifiche di prevenzione della corruzione e/o di fenomeni di *maladministration* secondo quanto previsto dalla normativa vigente e dalle correlate prassi attuative.

Art. 20 - *Formazione e sensibilizzazione in materia di whistleblowing*

1. L'UPO garantisce a tutto il proprio personale dipendente la partecipazione a sessioni formative in materia di *whistleblowing* al fine di evidenziare l'importanza dello strumento, favorirne l'utilizzo e prevenire pratiche distorte. Tali momenti informativi/formativi possono essere estesi anche a particolari categorie di soggetti esterni e a tutta la comunità amministrata.

2. L'UPO intraprende ogni ulteriore iniziativa di sensibilizzazione ricorrendo a tutti gli strumenti che saranno ritenuti idonei a divulgare la conoscenza dell'istituto (a titolo esemplificativo: eventi, articoli, studi, *newsletter* e portale internet, etc.).

3. Il RPCT invia a tutto il personale una comunicazione specifica in cui sono illustrate le finalità del *whistleblowing*, gli eventuali aggiornamenti di disciplina e gli estremi del presente Regolamento esplicativa delle modalità operative di effettuazione delle segnalazioni.

Art. 21 - *Adozione, entrata in vigore e revisione del Regolamento*

1. Il presente Regolamento è adottato con delibera del Consiglio di Amministrazione dell'UPO ed entra in vigore a decorrere dalla data di esecutività della delibera medesima.

2. Eventuali revisioni o modifiche del presente Regolamento sono approvate dal RPCT e adottate con Delibera del Consiglio di Amministrazione medesimo.

3. Il presente Regolamento è comunicato a tutti i dipendenti dell'UPO nonché pubblicato sul sito internet istituzionale, sezione "Amministrazione Trasparente" nonché reso disponibile nella intranet aziendale.

Art. 22 – *Abrogazioni*

1. Dall'entrata in vigore del presente regolamento si considerano superate ed abrogate le precedenti indicazioni, informazioni e modelli in uso.

Art. 23 – *Norma di rinvio*

2. Per tutto quanto non previsto nel presente regolamento si rimanda all'applicazione della normativa vigente (D.Lgs. 165/2001) e alle linee guida ANAC n. 469/2021.

ALLEGATO 1 – APPROFONDIMENTI MISURE DI SICUREZZA ADOTTATE DAL RESPONSABILE ESTERNO DEL TRATTAMENTO DATI

ALLEGATO 2 - INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

ALLEGATO 3 – MODELLO SEGNALAZIONE AGGIORNATO

ALLEGATO 1 - APPROFONDIMENTI MISURE DI SICUREZZA ADOTTATE DAL RESPONSABILE ESTERNO DEL TRATTAMENTO DATI

RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI PERSONALI

DATI DI CONTATTO DEL RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

- Sede Legale: Via P. Bagetti, 10 – 10143 Torino
- Numero di telefono: 011 19878715
- Posta certificata:tecnolink@mypec.eu
- Persona di riferimento: Antonio Cappiello
- Indirizzo email: cappiello@anticorruzioneintelligente.it

MISURE DI SICUREZZA ADOTTATE DAL RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

A seguito dell'utilizzo del servizio in cloud Whistleblowing Intelligente https://wb.anticorruzioneintelligente.it/ possono essere acquisiti dati relativi a persone identificate o identificabili.

COOKIES

Nessun dato personale degli utenti viene in proposito acquisito dalla piattaforma.
Non viene fatto uso di cookies per la trasmissione di informazioni di carattere personale, né vengono utilizzati c.d. cookies persistenti di alcun tipo, ovvero sistemi per il tracciamento degli utenti.
L'uso di c.d. cookies di sessione, c.d. "tecnici" (che non vengono memorizzati in modo persistente sul computer dell'utente e svaniscono con la chiusura del browser) è strettamente limitato alla trasmissione di identificativi di sessione (costituiti da numeri casuali generati dal server) necessari per consentire l'esplorazione sicura ed efficiente del servizio.
I c.d. cookies di sessione utilizzati evitano il ricorso ad altre tecniche informatiche potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti e non consentono l'acquisizione di dati personali identificativi dell'utente.
Il sito utilizza altresì cookies analytics per raccogliere informazioni, in forma aggregata, sul numero degli Utenti e su come gli stessi visitano la piattaforma. I dati sono raccolti all'unico fine di elaborare informazioni statistiche anonime sull'uso del della piattaforma e per verificare il corretto funzionamento della stessa; i dati di navigazione potrebbero essere utilizzati in vista dell'identificazione dell'Utente solo nel caso in cui ciò fosse necessario per l'accertamento di reati di natura informatica o su richiesta di un'Autorità pubblica.

I cookies non sono utilizzati per attività di profilazione dell'utente.

ULTERIORE RESPONSABILE DEL TRATTAMENTO

I dati personali raccolti dalla piattaforma https://wb.anticorruzioneintelligente.it/ sono trattati dalla Società:

Interzen Consulting s.r.l., con sede in Pescara, Strada Comunale Piana 3, cap. 65129 (P. IVA e C.F. 1446720680), in persona dell'amministratore delegato pro tempore regolarmente nominata da Tecnolink S.r.l con atto formale come sub responsabile del trattamento dei dati personali.

SICUREZZA DEL TRATTAMENTO – PIANO DI GESTIONE DEL RISCHIO PRIVACY

Il Responsabile indirettamente e il sub responsabile direttamente, attua le seguenti misure:

- si accerta che chiunque agisca sotto la propria autorità ed abbia accesso a dati personali, non tratti tali dati se non è stato istruito in tal senso dal responsabile stesso e vincolato contrattualmente (o ex lege) alla riservatezza/segreto
- applica le misure minime di sicurezza ict per le pubbliche amministrazioni individuate dall AGID
- applica misure tecniche di crittografia dei dati personali, dei documenti e del DB
- garantisce la riservatezza e l'integrità adottando strumenti e tecnologie di accesso mediante sistemi di autenticazione forte
- adotta mezzi che permettono di garantire la continuità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- adotta mezzi che permettono di garantire la capacità di ripristinare la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico]
- adotta delle misure tecniche per la gestione dei log a norma di legge
- luogo fisico di archiviazione dei dati: Italia
- modalità' di conservazione dei dati, conservazione digitale

Vedasi il dettaglio delle misure riportato più avanti

PERIODO DI CONSERVAZIONE

I dati personali saranno conservati sino al termine dell'incarico di erogazione del servizio di "Whistleblowing Intelligente" e comunque per un periodo di tempo non superiore ad anni 5.

DETTAGLIO MISURE DI SICUREZZA

1° LIVELLO – SISTEMI ESTERNI DI PREVENZIONE	
Scansione online delle vulnerabilità	Nessus® Essentials: soluzione per la rilevazione delle vulnerabilità di **Tenable®, Inc.** Nel 2021 Tenable è stato un Software Vendor di Gartner rappresentativo della Vulnerability Assessment.

2° LIVELLO – INFRASTRUTTURA I.T. DEL CLOUD SERVICE PROVIDER	
Service Provider	**Microsoft Azure.**
Tipologia di servizio cloud	Public CloudID
Certificazioni del cloud service provider	Tutta la documentazione aggiornata sulle conformità di Microsoft Azure **è disponibile qui.**
Localizzazione dei data center utilizzati	**West Europe (Netherlands).**

Livelli di sicurezza adottati dal service provider	**L'insieme di operazioni eseguite da Microsoft per proteggere l'infrastruttura di Azure è disponibile qui.**
Ridondanza dei dati del service provider	**Archiviazione con ridondanza di zona (Zone Redundancy Storage, ZRS): replica i dati archiviati in Azure in modalità sincrona su tre aree disponibili interne all'area primaria (primary region); approfondimento disponibile qui.**

3° LIVELLO – INFRASTRUTTURA I.T.	
Sicurezza informatica di Tecnolink	**Tecnolink ha validato i propri livelli di gestione della riservatezza e della sicurezza dei dati di Whistleblowing Intelligente cloud presso lo STAR Registry (Security, Trust, Assurance, and Risk) della Cloud Security Alliance come condizione preliminare per la qualificazione SaaS AGID Visualizza la scheda di qualificazione del Cloud Marketplace AGID**
Firewall	**Interzen ha adottato pfSense®, firewall riconosciuto come uno dei più potenti, sicuri ed affidabili.**
Back-up e disaster recovery	● **Procedura di back-up database e documenti ogni 4 ore;** ● ✔ **Back-up con ridondanza geografica: North Europe (Ireland);** ● ✔ **Data retention di 7 giorni;** ● ✔ **Servizio opzionale di DRAAS (Disaster Recovery As A Service).**

4° LIVELLO – COMPONENTI SOFTWARE	
Sistema operativo	**Antivirus Microsoft Forefront**
Server virtuale	**L'accesso ai server virtuali avviene mediante una VPN ed utilizzando un profilo utente dimensionato strettamente in base alle necessità di monitoraggio e manutenzione.**

5° LIVELLO – CODICE APPLICATIVO	
Sistema di autenticazione	**Sistema proprietario. È il sistema che vincola la password di accesso del singolo utente alle seguenti regole:** ● ✔ **Scadenza alla prima autenticazione sulla piattaforma ZenShare;** ● ✔ **Lunghezza minima di 8 caratteri;** ● ✔ **Scadenza periodica ogni 3 mesi;** ● ✔ **Divieto di riutilizzo delle ultime 5 password;** ● ✔ **Vincoli sulla complessità della password (utilizzo di una lettera maiuscola/minuscola, numero, simbolo, divieto dello username);** ● ✔ **Blocco dell'utente dopo 5 tentativi falliti.** **Interfacciamento con sistemi esterni di autenticazione:** ✔ **SPID (Sistema Pubblico di Identità Digitale).**

IP filtering	● ✔ **Utenti collegati. Possibilità di visualizzare tutti gli utenti autenticati (non i Segnalanti) sulla piattaforma Whistleblowing Intelligente con i seguenti dati: cognome, nome, ruolo, indirizzo IP, ultimo accesso effettuato.**

6° LIVELLO – DATI E DOCUMENTI DELLA PIATTAFORMA WHISTLEBLOWING INTELLIGENTE	
Criptaggio database e documenti	● ✔ **Database. Chiave di criptazione dati a sua volta criptata mediante un algoritmo per un ulteriore livello di sicurezza. Il dato resta criptato nel database e la sua decriptazione avviene solo quando viene visualizzato.** ● ✔ **Documenti. Criptazione e decriptazione mediante chiave privata.**
Protocollo HTTPS	**L'HyperText Transfer Protocol Secure (over Secure Socket Layer) è un protocollo per la comunicazione su Internet che protegge integrità e riservatezza dei dati scambiati tra la Whistleblowing Intelligente e l'hardware (PC, tablet, smartphone) dell'utente che vi accede. Certificato SSL erogato da Network Solutions LLC.**

ALLEGATO 2 - INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI AI SENSI DEGLI ARTICOLI 13 E 14 DEL REGOLAMENTO UE 2016/679 E ART. 54-BIS D.LGS. N. 165/2001

***

Titolare del trattamento e Responsabile della protezione dei dati (o "DPO")

Titolare del trattamento, e cioè il soggetto che determina le finalità e i mezzi del trattamento dei dati personali al quale ci si può rivolgere per esercitare i diritti riconosciuti dal GDPR, è l'Università degli Studi del Piemonte Orientale "Amedeo Avogadro", P. Iva n. 01943490027, Codice Fiscale 94021400026, sede del Rettorato in Via Duomo, n. 6 - 13100 Vercelli.

Il Titolare del trattamento può essere contattato inoltrando una email all'indirizzo affarigiuridici@uniupo.it

L'Università ha designato un Responsabile della protezione dei dati (DPO), contattabile all'indirizzo email dpo@uniupo.it

Fonti e categorie di dati trattate, natura del conferimento dei dati e modalità di trattamento

I dati personali oggetto di trattamento sono i dati forniti volontariamente dall'interessato sulla piattaforma https://wb.anticorruzioneintelligente.it e comportano la successiva acquisizione e trattamento degli stessi. L'interessato è libero di fornire i dati personali richiesti, il loro mancato conferimento potrebbe comportare l'impossibilità di attivare l'iter di esame della segnalazione.

Sono raccolti i seguenti dati personali dei Segnalanti (dipendenti dell'ente o equiparati):

- Nome e Cognome
- Luogo e data di nascita
- Datore di lavoro
- Posizione/Ruolo lavorativo
- indirizzo di posta elettronica
- Codice Fiscale

Nel modulo di segnalazione, il segnalante potrebbe riportare dati personali di altre persone.

Per il Responsabile della Prevenzione della corruzione ed eventuali collaboratori autorizzati, oltre ai dati già indicati, sono raccolti i seguenti dati:

- indirizzo ip
- dati di log

Finalità del trattamento e base giuridica

I dati forniti verranno trattati esclusivamente per l'istruttoria della segnalazione ai sensi dell'art. 54-bis "Tutela del dipendente pubblico che segnala illeciti" del D.Lgs. n. 165/2001.

Al fine di garantire la riservatezza del segnalante per tutta la durata della gestione della segnalazione, l'identità dello stesso sarà conosciuta solo dal Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) di Ateneo. Ad eccezione dei casi in cui sia configurabile una responsabilità a titolo di calunnia e di diffamazione ai sensi delle disposizioni del codice penale o dell'art. 2043 del codice civile e delle ipotesi in cui l'anonimato non sia opponibile per legge (ad esempio, indagini

penali, tributarie o amministrative, ispezioni di organi di controllo), l'identità del segnalante viene protetta in ogni contesto successivo alla segnalazione. Pertanto, fatte salve le citate eccezioni, l'identità del segnalante non può essere rivelata senza il suo espresso consenso, e tutti coloro che ricevono o sono coinvolti nella gestione della segnalazione sono tenuti a tutelare la riservatezza di tale informazione.
La base giuridica di tale trattamento è rappresentata dall'art. 6, c. 1, lett. c), del Regolamento (adempimento di un obbligo legale al quale è soggetto il titolare del trattamento).
Il trattamento dei dati personali è improntato ai principi di correttezza, liceità e trasparenza e di tutela della riservatezza e dei diritti dell'interessato, nonché agli ulteriori principi previsti dall'art. 5 del Regolamento.

Eventuali destinatari o le eventuali categorie di destinatari dei dati personali e trasferimento di dati personali in un Paese terzo o fuori dallo Spazio Economico Europeo (SEE).

Ai dati potranno accedere esclusivamente soggetti autorizzati debitamente istruiti (anche con riguardo al rispetto delle misure di sicurezza e agli obblighi di riservatezza) ai sensi degli artt. 29 GDPR e 2-quaterdecies del Codice per la protezione dei dati personali
I dati personali saranno comunicati ex lege al Responsabile della prevenzione della Corruzione e della Trasparenza (RPCT) dell'Amministrazione. Potranno altresì essere comunicati:

- a persone fisiche autorizzate dal RPCT, vincolate alla riservatezza;
- all''Autorità Giudiziaria e/o Contabile su loro richiesta
- all'ufficio procedimenti disciplinari e, quindi, al soggetto segnalato ma solo con il consenso espresso del segnalante.

I dati personali sono inoltre trattati informaticamente dal Responsabile del trattamento, società esterna fornitrice della piattaforma tecnologica in uso. La società è vincolata alla riservatezza.
Per ottenere un elenco aggiornato dei soggetti che possono venire a conoscenza dei dati personali, è possibile inoltrare una comunicazione a mezzo email all'indirizzo di contatto del DPO dpo@uniupo.it, avendo cura di specificare il motivo della richiesta.
I dati non saranno diffusi e non verranno trasferiti ad un paese terzo (o sito al di fuori dal Spazio Economico Europeo) o a un'organizzazione internazionale.
Qualora si renda necessario trasferire i dati verso un paese terzo sito al di fuori dallo Spazio Economico Europeo (come ad esempio per la gestione dei programmi internazionali Erasmus) l'Università garantisce che tale trasferimento avverrà esclusivamente in presenza di una decisione di adeguatezza della Commissione Europea o di altre garanzie adeguate previste dalle Leggi in materia di protezione dei dati personali (come ad esempio la stipula di clausole contrattuali standard con il soggetto che riceverà i dati).

Periodo di conservazione dei dati

I dati raccolti sono conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati e/o per il tempo necessario per adempiere agli obblighi di legge. Oltre tale criterio di conservazione, i dati potranno essere conservati per finalità di difesa e tutela dell'Università in sede giudiziaria e per finalità di archiviazione, con accesso limitato, in ogni caso per un tempo non superiore a 5 anni.

Diritti dell'interessato

L'esercizio dei diritti indicati nella presente sezione non è soggetto ad alcun vincolo di forma ed è gratuito, salvo per richieste manifestamente infondate o eccessive, ai sensi dell'art. 12 (5) del GDPR.

In relazione ai trattamenti descritti nella presente informativa ed ai sensi del GDPR, l'interessato può esercitare i seguenti diritti:

- diritto di accesso ai propri dati personali ed a tutte le informazioni di cui all'art. 15 del GDPR,
- diritto di rettifica dei propri dati personali inesatti e l'integrazione di quelli incompleti,
- diritto di cancellazione dei propri dati, fatta eccezione per quelli contenuti in atti che devono essere obbligatoriamente conservati dall'Università e salvo che sussista un motivo legittimo prevalente per procedere al trattamento;
- diritto alla limitazione del trattamento ove ricorra una delle ipotesi di cui all'art. 18 del GDPR;
- diritto di opporsi al trattamento dei propri dati personali, fermo quanto previsto con riguardo alla necessità ed obbligatorietà del trattamento ai fini dell'instaurazione del rapporto;
- diritto di revocare il consenso eventualmente prestato per i trattamenti non obbligatori dei dati, senza con ciò pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca.

L'Interessato ha inoltre diritto di avanzare un reclamo al Garante per la Protezione dei Dati Personali (www.garanteprivacy.it) o all'Autorità Garante dello Stato dell'UE in cui l'Interessato risiede abitualmente o lavora, oppure del luogo ove si è verificata la presunta violazione, in relazione a un trattamento che consideri non conforme.
Per tutte queste richieste l'interessato si può rivolgere all'Università degli Studi del Piemonte Orientale "Amedeo Avogadro" inoltrando una comunicazione a mezzo posta tradizionale all'indirizzo Via Duomo, n. 6 - 13100 Vercelli o tramite email all'indirizzo affarigiuridici@uniupo.it), oppure contattando il DPO all'indirizzo dpo@uniupo.it

Il soggetto segnalato, presunto autore dell'illecito, con riferimento ai propri dati personali trattati dall'Università, non può esercitare i diritti previsti dagli articoli da 15 a 22 del Regolamento(UE) n. 2016/679. In tal caso, dunque, al soggetto interessato (segnalato) è preclusa la possibilità di rivolgersi al titolare del trattamento e, in assenza di risposta da parte di quest'ultimo, di proporre reclamo al Garante della Privacy (ai sensi dell'art. 77 del Regolamento (UE) n. 2016/679). Resta ferma la possibilità per il soggetto segnalato, presunto autore dell'illecito, di richiedere al Garante accertamenti sulla conformità del trattamento dei propri dati da parte dell'Amministrazione.

ALLEGATO 3 – MODELLO SEGNALAZIONE WHISTLEBLOWING AGGIORNATO

SEGNALAZIONE

WHISTLEBLOWING

(art. 54-*bis*, D.Lgs. n. 165/2001 e s.m.i.)

Al Responsabile

della Prevenzione della Corruzione

e della Trasparenza dell'UPO

Il/la sottoscritto/a: _____

consapevole delle responsabilità e delle conseguenze civili e penali previste in caso di dichiarazioni mendaci e/o formazione o uso di atti falsi, anche ai sensi del D.P.R. n. 445 del 28 dicembre 2000

DICHIARA

ai fini sensi dell'art. 54-*bis* del D.Lgs. n. 165/01 quanto segue:

DATI DEL SEGNALANTE	
Nome	
Cognome	
Codice Fiscale	
Qualifica servizio attuale nell'UPO	
Incarico (Ruolo) di servizio attuale nell'UPO	
Servizio / Struttura di servizio attuale nell'UPO	
Incarico (Ruolo) di servizio all'epoca del fatto segnalato nell'UPO	
Servizio / Struttura di servizio all'epoca del fatto segnalato nell'UPO	

Specificare se il Segnalante è dipendente o collaboratore di impresa che esegue lavori, servizi o forniture per l'UPO, precisando il nominativo del rappresentante legale dell'impresa d'afferenza insieme ai relativi recapiti	
Telefono	
Email per le comunicazioni al di fuori della Piattaforma ***NB. Per ragioni di sicurezza, l'indirizzo mail non può coincidere con l'indirizzo di posta aziendale***	

Se la segnalazione è già stata effettuata ad altri soggetti compilare la seguente tabella:

Soggetto cui è stata effettuata la segnalazione **(es. Procura della Repubblica, Corte dei Conti, A.N.AC., etc.)**	**Data della segnalazione**	**Stato / Esito della segnalazione**

DATI E INFORMAZIONI SULLA CONDOTTA ILLECITA	
Ente in cui si è verificato il fatto	
Periodo in cui si è verificato il fatto	
Data in cui si è verificato il fatto	

Luogo fisico in cui si è verificato il fatto	
Soggetto che ha commesso il fatto **Nome, cognome, qualifica** *(possono essere inseriti più nomi)*	
Eventuali soggetti privati coinvolti	
Eventuali imprese coinvolte	
Modalità con cui è venuto a conoscenza del fatto	
Eventuali altri soggetti che possono riferire sul fatto *(Nome, cognome, qualifica, recapiti)*	
Area / Servizio a cui può essere riferito il fatto	
Descrizione del fatto	

La condotta è illecita perché ***(facoltativo)***	☐ penalmente rilevante; ☐ posta in essere in violazione del Codice Etico e/o di altre disposizioni sanzionabili in via disciplinare; ☐ idonea ad arrecare un pregiudizio patrimoniale a ZZZ; ☐ idonea ad arrecare un pregiudizio all'immagine di ZZZ; ☐ suscettibile di arrecare un danno alla salute o sicurezza dei dipendenti, utenti e cittadini, o di arrecare un danno all'ambiente; ☐ suscettibile di arrecare pregiudizio agli utenti o ai dipendenti o ad altri soggetti che svolgono la loro attività presso ZZZ; ☐ altro […]
INTERESSI PERSONALI DEL SEGNALANTE ***In questo campo il segnalante deve dichiarare eventuali interessi personali che lo coinvolgono in relazione al segnalato o a quanto oggetto di segnalazione***	
CONSENSO ALLA RIVELAZIONE DELLA IDENTITA' AI SENSI DELL' ART. 54-BIS, COMMA 3, DEL D.LGS. N. 165/2001 ***COMPILAZIONE FACOLTATIVA***	Il segnalante, ai sensi dell'art. 54-bis, comma 3, del D.Lgs. n. 165/2001, laddove ne ricorra la necessità, e al fine di rendere utilizzabile la segnalazione nei confronti del segnalante nell'ambito del procedimento disciplinare, ☐ presta, fin da subito, il proprio consenso affinché sia rivelata la sua identità al segnalato; ☐ NON presta, fin da subito, il proprio consenso affinché sia rivelata la sua identità al segnalato, riservandosi, se del caso, di prestarlo in seguito.

[Luogo e Data] _____, _____.

[Firma del dichiarante per esteso, leggibile]

_____

Alla presente dichiarazione si allega:

1) Copia fotostatica del Documento di identità in corso di validità del dichiarante.

2) Eventuale documentazione a corredo della segnalazione.