UNIVERSITÀ DEGLI STUDI DI BARI ALDO MORO

IL RETTORE

D.R. n. 2605

VISTO il D.lgs. n 165/2001 *"Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche"*;

VISTO il D.lgs. n.196/2003 *"Codice in materia di protezione dei dati personali"*;

VISTA la Legge n. 190/2012 *"Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione"*;

VISTO il D.P.R. n. 62/2013 *"Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165*", modificato dal D.lgs. n. 81/2023;

VISTO il Regolamento UE 2016/679 relativo alla protezione dei dati personali;

VISTA la Direttiva UE 2019/1937 del Parlamento europeo e del Consiglio del 23.09.2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione;

VISTA la delibera ANAC n. 469 del 09.06.2021, recante *"Schema di 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)*", modificate con il Comunicato del Presidente dell'Autorità del 21.07.2021 (*errata corrige*);

RILEVATO CHE l'Università di Bari si è dotata dell'applicativo informatico GlobaLeaks quale strumento prioritario per la gestione delle segnalazioni di *whistleblowing*, un *software* libero ed *open source* impiegato anche dall'ANAC, conforme allo *standard* ISO 37002, alla Direttiva UE 2019/1937 ed al Regolamento Generale sulla Protezione dei Dati (GDPR

679/2016), in grado di proteggere la *privacy* dei segnalanti, delle loro segnalazioni e dei soggetti per qualunque titolo coinvolti nella segnalazione;

ATTESO CHE l'Università di Bari, con le "*Linee guida di Ateneo in materia di segnalazioni di illeciti (c.d. whistleblowing) sulla scorta della normativa di cui all'art. 54 bis del D.lgs. n. 165/2001 e della delibera ANAC n. 469 del 09.06.2021*" adottate con D.R. n. 4565 del 20.12.2022, ha disciplinato le procedure da adottare per gestire le segnalazioni di *whistleblowing* indirizzate all'Amministrazione;

VISTO il D.lgs. n. 24 del 10.03.2023, che ha dato attuazione alla direttiva UE 2019/1937 del Parlamento Europeo e del Consiglio prevedendo, all'art. 4 comma 1, che "*i soggetti del settore pubblico […] sentite le rappresentanze o le organizzazioni sindacali di cui all'articolo 51 del decreto legislativo n. 81 del 2015, attivano […] propri canali di segnalazione, che garantiscono […] la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione*";

CONSIDERATO che il predetto decreto acquisirà efficacia a decorrere dal 15.07.2023;

VISTO lo "*Schema di Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali – procedure per la presentazione e gestione delle segnalazioni esterne*" pubblicato dall'ANAC sul proprio sito istituzionale in data 01.06.2023, che dovranno essere adottate sentito il Garante per la protezione dei dati personali, così come previsto dall'art. 10 comma 1 del D.lgs. n. 24/2023;

PRESO ATTO dell'informativa resa agli Organi di governo dell'Università dal RPCT *pro-tempore*, nelle adunanze del 26 e 29.06.2023, recanti ad oggetto aggiornamento del canale interno dedicato alle segnalazioni di whistleblowing e delle "*linee guida di ateneo in materia di segnalazioni di illeciti (c.d. whistleblowing)*", emanate con D.R. n. 4565 del 20.12.2022, alla luce dell'entrata in vigore del D.lgs. n. 24 del 10.03.2023;

RILEVATO CHE con nota prot. n. 158705 del 28.06.2023, le OO.SS. maggiormente rappresentative operanti nell'ambito dell'Università di Bari sono state invitate "*a far pervenire […] eventuali osservazioni entro la data del*

07.07.2023, al fine di consentire all'Università di adeguare il proprio canale interno destinato alle segnalazioni di whistleblowing entro la data del 15.07.2023 di entrata in vigore della nuova normativa" e che le stesse, spirato il termine loro indicato, non hanno formulato rilievi;

VISTA la delibera del Consiglio di Amministrazione del 29.06.2023 con la quale la Dott.ssa Chiara Deninno è stata nominata RPCT dell'Università degli Studi di Bari Aldo Moro in sostituzione dell'Avv. Paolo Squeo, a decorrere dalla data del 01.07.2023;

TENUTOC ONTO che la Fase 1 della misura anticorruzione "*Tutela del dipendente che segnala illeciti (whistleblower)*" contenuta nella sottosezione "*Rischi corruttivi e trasparenza*" del PIAO 2023-2025, prevede l'"*aggiornamento delle linee guida di Ateneo in materia di whistleblowing sulla base della normativa italiana di recepimento della Direttiva Europea 2019/1937 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione*", da realizzarsi entro il termine ultimo del 31.12.2023;

RAVVISATA la necessità di adeguare il proprio canale interno per la gestione delle segnalazioni entro la data del 15.07.2023, nelle more del processo di aggiornamento delle "*linee guida di Ateneo in materia di whistleblowing*", anche all'esito dell'emanazione da parte di ANAC delle proprie linee guida definitive;

DECRETA

la modifica parziale delle "*Linee guida di Ateneo in materia di segnalazioni di illeciti (c.d. whistleblowing) sulla scorta della normativa di cui all'art. 54 bis del D.lgs. n. 165/2001 e della delibera ANAC n. 469 del 09.06.2021*", adottate con D.R. n. 4565 del 20.12.2022, ed in particolare l'adeguamento del canale interno per la gestione delle segnalazioni di *whistleblowing*, in quella sede già regolamentato, secondo le previsioni di seguito specificate:

1) **<u>presentazione delle segnalazioni mediante applicativo informatico</u>**: l'Università si è dotata di un applicativo informatico, in grado di garantire la riservatezza dell'identità del segnalante, dei facilitatori, della persona coinvolta nonché dei soggetti menzionati, per qualunque titolo, nella denuncia. Lo strumento, parimenti, assicura la riservatezza della segnalazione e della documentazione ad essa allegata. Sotto il profilo della sicurezza, il predetto applicativo

informatico: A) prevede cinque distinte tipologie di utenti: A.1) il *whistleblower*, che accede ai soli dati inerenti la propria segnalazione, in forma anonima, grazie ad un codice identificativo univoco di 16 cifre (c.d. *key code*) generato automaticamente dal *software* in seguito all'invio della denuncia, che non può essere replicato. Pertanto, è onere del segnalante custodirlo accuratamente atteso che in caso di suo smarrimento questi non potrà più accedere alla propria segnalazione; A.2) il ricevente 1 della segnalazione (il RPCT) che, per legge, è il soggetto deputato a dare seguito alle segnalazioni. Questi può visualizzare l'elenco delle segnalazioni e delle comunicazioni acquisite dal sistema; A.3) qualora un apposito atto organizzativo individui unità che supportino il RPCT nella gestione delle segnalazioni, l'applicativo prevede la figura del ricevente 2 che, ove designato dal RPCT per istruire la segnalazione, ha la possibilità di accedere alle sole segnalazioni assegnategli; A.4) il custode dell'identità, che riceve e visualizza unicamente le eventuali richieste di accesso ai dati personali del segnalante, provenienti dal RPCT; A.5) l'amministratore del sistema informatico, che ha il compito di assicurare l'aggiornamento del *software*; B) non consente agli utenti abilitati (ricevente 1, ricevente 2, custode dell'identità e amministratori di sistema) di accedere ai dati identificativi del segnalante; C) nei casi previsti dalla legge, consente di accedere ai dati personali del segnalante unicamente al ricevente 1 (RPCT), previa richiesta motivata da inviare al Custode dell'identità, che può approvarla o rigettarla. La piattaforma informatica conserva traccia delle ragioni per cui il RPCT richiede al Custode dell'identità di poter accedere ai dati personali del segnalante e del conseguente provvedimento di autorizzazione/diniego, con relativa motivazione. Presso l'Università di Bari la funzione di Custode dell'identità viene ricoperta dallo stesso RPCT; D) consente al RPCT, agli istruttori, al custode dell'identità ed agli amministratori di sistema di accedere alle informazioni pertinenti il proprio ruolo utilizzando apposite credenziali di autenticazione. Con ricorrenza periodica di 180 giorni il software richiede la modifica della *password*; E) assicura il disaccoppiamento dei dati personali del segnalante dalle informazioni contenute nella segnalazione; F) è progettato per non registrare alcun dato che possa indicare la provenienza della segnalazione o della singola connessione telematica al sistema. I *log* dell'applicativo, necessari esclusivamente per attività di manutenzione, non contengono alcuna informazione sulla provenienza dei *client*. Il *software*, inoltre, è accessibile tramite la rete Tor, progettata appositamente per evitare il tracciamento del traffico di rete. In ogni caso è garantita la connessione con protocollo cifrato HTTPS; G) monitora tutte le attività svolte al suo interno, registrando gli accessi degli utenti autorizzati ad adoperarlo. Sul piano operativo, invece, l'applicativo informatico consente al segnalante di: A)

effettuare una segnalazione attraverso la compilazione di un questionario, i cui campi devono essere valorizzati in modo chiaro e circostanziato, che può essere inviato anche in forma anonima, ferma restando la possibilità di integrarlo successivamente con i dati personali e/o ulteriori informazioni/documenti utili; B) allegare i documenti comprovanti i fatti denunciati (caricabili in formato word, excel, PdF, Zip, MP3, MP4, video, audio, ecc.); C) dialogare in modo anonimo e spersonalizzato con il RPCT, tramite una funzione di messaggistica integrata. Nella compilazione del questionario, il segnalante è tenuto a fornire al RPCT tutte le informazioni in esso contrassegnate come "*obbligatorie*" essendo opportuno, altresì, che specifichi anche il maggior numero possibile di quelle "*facoltative*". Il *link* di accesso all'applicativo informatico (owb.ict.uniba.it) è liberamente raggiungibile dalle pagine del sito istituzionale dell'Università;

2) **presentazione delle segnalazioni a mezzo del servizio postale**: in via residuale, le segnalazioni possono essere trasmesse all'Università a mezzo del servizio postale. L'utilizzo di questo canale, tuttavia, è consigliato soltanto nel caso in cui l'applicativo informatico presenti anomalie temporanee oppure il segnalante non abbia familiarità con le procedure informatiche o, ancora, non sia in possesso di strumenti informatici. Il modulo da utilizzare per la segnalazione è disponibile sul sito istituzionale dell'Università alla pagina *https://www.uniba.it/it/amministrazione-trasparente/altri-contenuti/altri-contenuti-corruzione/segnalazioni-di-situazioni-di-illecito* ed è composto da due sezioni distinte e separate di cui una dedicata ai dati identificativi del segnalante ed alle informazioni di carattere strettamente personale, l'altra alla segnalazione. Il plico da trasmettere dovrà essere così composto: 1) una busta più grande contenente il "*modulo per la segnalazione di reati*" e gli eventuali documenti comprovanti i fatti denunciati; 2) una busta più piccola, sigillata, da inserirsi all'interno di quella più grande, contenente la sezione del "*modulo per la segnalazione di reati*" dedicata all'identità segnalante. Detto plico dovrà essere indirizzato al Responsabile della Prevenzione della Corruzione e della Trasparenza dell'Università degli Studi di Bari Aldo Moro - Palazzo Ateneo, Piazza Umberto I, 70121 Bari - con la specificazione, sulla busta più grande ed esterna, della dicitura "*Riservato-Whistleblowing*". Le segnalazioni a mezzo posta prive dei dati personali del segnalante e/o della dicitura "*Riservato-Whistleblowing*" sulla busta saranno considerate alla stregua delle segnalazioni ordinarie e, come tali, trattate secondo i criteri stabiliti dall'ordinamento interno di Ateneo;

3) presentazione delle segnalazioni in forma orale: il segnalante ha, altresì, la possibilità di richiedere un incontro al RPCT, preferibilmente tramite l'applicativo informatico di gestione

delle segnalazioni di *whistleblowing*, atteso che, come detto, lo stesso utilizza un protocollo di crittografia in grado di garantire la sicurezza e la riservatezza delle informazioni trasmesse. Nell'ipotesi in cui l'applicativo informatico presenti delle anomalie temporanee oppure il segnalante non abbia familiarità con le procedure informatiche o, ancora, non sia in possesso di strumenti informatici, l'incontro potrà essere richiesto al RPCT a mezzo posta, avendo cura il segnalante di riportare sulla busta la dicitura "*Riservato-Whistleblowing*", affinché il plico venga consegnato direttamente ed esclusivamente al suo destinatario, nella massima riservatezza. Ricevuta la richiesta, il RPCT fissa un incontro, entro un termine ragionevole, dandone informazione al segnalante tramite il medesimo canale di comunicazione da questi prescelto. L'incontro è documentato dal RPCT attraverso la redazione di un puntuale processo verbale che il segnalante sottoscrive per conferma oppure mediante registrazione su un dispositivo idoneo alla conservazione ed all'ascolto. I documenti formatisi e/o acquisiti in ragione dell'incontro tra il RPCT ed il segnalante saranno custoditi in appositi archivi anonimizzati, allocati all'interno di armadi muniti di serrature ed accessibili unicamente al RPCT stesso;

4) **il soggetto preposto alla ricezione delle segnalazioni**: il RPCT è l'unico soggetto legittimato a ricevere e gestire le segnalazioni di *whistleblowing*. Egli rilascia al segnalante un avviso di ricevimento entro sette giorni dalla data di ricezione della denuncia. Ove quanto segnalato non sia stato adeguatamente circostanziato, il RPCT può chiedere al *whistleblower* chiarimenti ed elementi integrativi, tramite il canale a ciò dedicato o di persona, qualora il segnalante abbia richiesto un incontro diretto. Pronunciatosi sull'ammissibilità e sulla ricevibilità della segnalazione, il RPCT: A) mantiene le interlocuzioni con il *whistleblower*; B) dà un corretto seguito alle segnalazioni ricevute; C) svolge l'attività istruttoria necessaria, anche mediante audizioni e l'acquisizione di documenti; D) comunica al *whistleblower* l'esito della segnalazione;
5) **la segnalazione presentata ad un soggetto differente dal RPCT**: allorché la segnalazione interna dovesse essere presentata ad un soggetto differente da quello, per legge, preposto alla sua gestione, quegli dovrà trasmetterla al RPCT, entro sette giorni dal ricevimento, dandone contestuale notizia al *whistleblower*;
6) **fase istruttoria e termini per la definizione della segnalazione**: quando il RPCT valuta la segnalazione ammissibile e ricevibile accorda al segnalante che abbia dichiarato la propria identità, ed ai soggetti a questi equiparati dalla legge, le tutele previste dal D.lgs. n. 24/2023; avvia quindi la fase istruttoria del procedimento, nel rispetto dei principi di imparzialità e

riservatezza, ed espleta le attività che ritiene utili per accertare l'effettivo accadimento dei fatti denunciati. Il RPCT tiene traccia delle attività svolte in appositi processi verbali e, entro tre mesi dalla data dell'avviso di ricevimento della segnalazione o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla sua presentazione, fornisce riscontro alla segnalazione stessa, con provvedimento adeguatamente motivato. In tale comunicazione, il RPCT indica le misure che reputa opportuno assumere o che ha adottato o che intende adottare. Qualora il RPCT riconosca fondata la segnalazione, in considerazione della natura dell'illecito, provvede: A) a presentare denuncia all'autorità competente (Procura della Repubblica, Tribunale, Corte dei Conti, ANAC, Dipartimento della Funzione Pubblica, ecc.); B) ad informare il Rettore affinché assuma i provvedimenti necessari a tutelare l'Università; C) a trasmettere gli atti all'Ufficio Procedimenti Disciplinari. Diversamente, ove la giudichi infondata, il RPCT provvederà ad archiviarla;

7) **le segnalazioni anonime e la loro trattazione**: le segnalazioni che non consentano di ricavare l'identità del *whistleblower* sono considerate anonime. Esse, ove ben circostanziate, saranno equiparate alle segnalazioni ordinarie e, come tali, trattate secondo le procedure previste dall'ordinamento interno di Ateneo. A norma dell'art. 16 comma 4 del D.lgs. n. 24/2023, le misure di protezione previste in favore del segnalante saranno riconosciute anche al *whistleblower* anonimo, successivamente identificato, che abbia denunciato di aver subito ritorsioni a causa della propria segnalazione. L'Università registrerà la segnalazione anonima ricevuta e la conserverà, unitamente alla relativa documentazione, per un periodo di cinque anni decorrenti dalla data della sua presentazione, al fine di rintracciarla nel caso in cui il *whistleblower* comunichi all'ANAC di aver subito misure ritorsive a causa della stessa;

8) **segnalazioni inammissibili**: la segnalazione di *whistleblowing* è considerata inammissibile: A) per manifesta mancanza di interesse all'integrità della pubblica amministrazione; B) per difetto di competenza del RPCT sulle questioni segnalate; C) per manifesta infondatezza, stante l'assenza di elementi di fatto idonei a giustificare l'accertamento; D) quando il suo contenuto sia talmente generico da impedire la comprensione dei fatti denunciati; E) ove costituita da soli documenti, senza alcuna descrizione delle violazioni oggetto di denuncia; F) per carenza dei requisiti essenziali; G) per difetto di legittimazione, allorché provenga da un soggetto differente da quello individuato dalla legge quale segnalante; H) allorché la segnalazione verta su questioni che il segnalante ha sottoposto al vaglio dell'Autorità giudiziaria. In tutti i suddetti casi, il RPCT procede all'archiviazione della segnalazione dandone comunicazione al *whistleblower* entro 10 giorni, comunque entro il termine di tre mesi di cui al paragrafo 6;

9) **informativa ai sensi dell'art. 13 del regolamento U.E. n. 2016/679 sul trattamento dei dati personali**: i dati personali raccolti per gestire le segnalazioni di *whistleblowing* sono trattati dall'Università nel pieno rispetto dei princìpi europei e nazionali in materia di protezione dei dati personali nonché adottando misure appropriate a tutela dei diritti e delle libertà degli interessati in conformità di quanto previsto dal GDPR 679/2016 e dal D.lgs. n. 24/2023.

Il presente Decreto sarà portato a ratifica nelle prossime sedute del Senato Accademico e del Consiglio di Amministrazione.

Bari, 12.07.2023

Il Magnifico Rettore
Prof. Stefano Bronzini