DI SANTE SAS DI ALICE DI SANTE E ANDREA DI SANTE

Agenzia Generale di Generali Italia S.p.a. di Verbania

Modello di organizzazione, getsione e controllo

ex D. Lgs. n. 231, 8 giugno 2001

VADEMECUM ADEMPIMENTI WHISTLEBLOWING ATTO ORGANIZZATIVO DI ATTUAZIONE DELLA DISCIPLINA DEL WHISTLEBLOWING

Sommario

1. Premessa

Il presente atto organizzativo stabilisce e regola le modalità operative con cui l'Agenzia Generale dà attuazione alle previsioni di cui al D. Lgs. n. 24 del 10 marzo 2023 (intitolato "Attuazione della direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio 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") in materia di "whistleblowing", conformemente a quanto previsto dalle linee guida ANAC (Autorità Nazionale Anticorruzione) approvate con Delibera n. 311 del 12 luglio 2023.

In particolare, il presente atto organizzativo ha la finalità di descrivere e disciplinare:

1. I soggetti segnalanti e le forme di tutela nei confronti degli stessi e degli altri soggetti coinvolti;
2. Il perimetro oggettivo e il contenuto della segnalazione;
3. I canali previsti dal D. Lgs. n. 24/2023 e messi a disposizione del whistleblower per la denuncia di presunte anomalie o violazioni (comportamenti, atti od omissioni), anche solo potenziali, di disposizioni normative nazionali o dell'Unione europea che ledono gli interessi pubblici o l'integrità dell'Agenzia Generale, commesse da dipendenti, dirigenti, membri degli organi sociali o terzi e di cui il whistleblower sia venuto a conoscenza nell'ambito del contesto lavorativo;
4. Il processo interno di ricezione e di gestione della segnalazione effettuate dai whistleblower approntato dall'Agenzia Generale.

Il presente atto organizzativo si applica a DI SANTE S.A.S. DI ANTONIO DI SANTE E ALICE DI SANTE, Agenzia Generale di Generali Italia di Verbania.

Il documento è approvato con delibera della Società, al fine di garantirne la massima diffusione, viene inviato ai suoi dipendenti e collaboratori ed affisso in luogo accessibile a tutti e pubblicato sul sito internet aziendale (laddove l'Agenzia Generale abbia un proprio sito).

L'Agenzia Generale, inoltre, intende promuovere opportune attività di formazione del proprio personale dipendente e autonomo, per assicurare la consapevolezza e la corretta interpretazione del procedimento di segnalazione adottato.

1.1 AMBITO DI APPLICAZIONE SOGGETTIVO

1.2 I soggetti segnalanti ("*whistleblower*")

Ai sensi del D. Lgs. n. 24/2023, il sistema di segnalazione può essere attivato dai seguenti soggetti:

- lavoratori dipendenti (qualunque tipologia contrattuale) dell'Agenzia Generale e coloro che operano sulla base di rapporti che ne determinano l'inserimento nell'organizzazione aziendale, anche in forma diversa dal rapporto di lavoro subordinato;
- lavoratori autonomi, collaboratori, liberi professionisti e consulenti che prestano la propria attività presso l'Agenzia Generale (es. subagenti o produttori);
- volontari e tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso l'Agenzia Generale;

- persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate, in via di mero fatto, presso l'Agenzia Generale;
- soggetti terzi aventi rapporti e relazioni d'affari con l'Agenzia Generale (ad esempio clienti, fornitori, consulenti).

Le segnalazioni possono riguardare i seguenti soggetti:

- dipendenti e/o dirigenti dell'Agenzia Generale;
- membri degli organi sociali dell'Agenzia Generale e/o l'Agente Generale;
- terzi (ad esempio: fornitori, consulenti, collaboratori), la cui condotta attiva od omissiva possa determinare, in modo diretto o indiretto, un danno economico-patrimoniale e/o di immagine all'Agenzia Generale.

1.3. Le forme di tutela del segnalante e del segnalato

Obbligo di riservatezza

Ai sensi dell'art. 12 del D. Lgs n. 24/2023 l'identità del segnalante non può essere rivelata, senza il consenso espresso della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni.

Allo stesso modo è tutelata l'identità delle persone coinvolte e menzionate nelle segnalazioni fino alla conclusione dei procedimenti avviati a seguito delle segnalazioni stesse. Per identità si intende non solo il nominativo della persona, ma anche qualsiasi altra informazione da cui possa evincersi, direttamente o indirettamente, tale identità.

Pertanto, l'intera procedura di gestione della segnalazione ricevuta attraverso il canale interno di segnalazione avviene in modalità riservata, in modo da garantire la massima sicurezza e riservatezza.

In particolare, al fine di garantire la sicurezza e la riservatezza delle informazioni raccolte, l'accesso ai dati sarà consentito esclusivamente al gestore delle segnalazioni, regolarmente nominato con delibera sopra indicata, Avv. Antonella Panetta, soggetto competente e debitamente autorizzato al trattamento dei dati personali ai sensi della vigente normativa.

Nel caso la segnalazione pervenga a persone diverse dal gestore interno, le persone riceventi la segnalazione adotteranno tutte le misure necessarie per garantire la riservatezza del segnalante, delle persone coinvolte o menzionate nella segnalazione e della eventuale documentazione allegata e trasmetteranno la segnalazione erroneamente ricevuta nelle modalità e nei termini indicati nel successivo paragrafo 3.1.

La conservazione dei dati avverrà a norma di legge e per il tempo necessario all'accertamento della fondatezza della segnalazione e, se del caso, all'adozione dei provvedimenti conseguenti e/o all'esaurirsi di eventuali azioni avviate a seguito della segnalazione. Successivamente, tali dati saranno distrutti. In ogni caso, la conservazione dei dati non potrà superare il termine dei cinque anni dalla data in cui viene comunicato al segnalante l'esito finale della procedura di segnalazione.

Conformemente a quanto previsto dall'art. 12 del D. Lgs. n. 24/2023, nell'ambito del 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 disciplinare attivato dall'Agente Generale contro il presunto autore della condotta segnalata, l'identità del segnalante non può essere rivelata ove la contestazione dell'addebito disciplinare si fondi su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti ad essa. Qualora la

contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso del segnalante alla rivelazione della sua identità. Nel caso in cui l'identità del segnalante risulti indispensabile alla difesa del soggetto cui è stato contestato l'addebito disciplinare, l'Agente Generale non potrà procedere con il procedimento disciplinare se il segnalante non acconsente espressamente alla rivelazione della propria identità. In tale caso, il gestore interno provvederà quindi ad acquisire tale consenso presso il segnalante, attraverso richiesta di sottoscrizione del suddetto consenso.

Nei seguenti casi, invece, non si è tenuti a tutelare la riservatezza della identità della persona segnalante:

- la segnalazione risulti fatta allo scopo di danneggiare o recare pregiudizio al segnalato (c.d. "segnalazione in mala fede") e si configuri una responsabilità a titolo di calunnia o di diffamazione ai sensi di legge;
- nella segnalazione vengano rivelati fatti e/o circostanze tali che, seppur estranei alla sfera aziendale, rendano opportuna e/o dovuta la segnalazione all'Autorità Giudiziaria (ad es. reati di terrorismo, spionaggio).

I dati personali di segnalanti e/o denuncianti sono trattati in conformità alla normativa nazionale ed europea in materia di tutela dei dati personali (in particolare, Regolamento (UE) 2016/679 sulla protezione dei dati personali, D. Lgs. n. 196/2003 e ss.mm.ii., adeguato alle disposizioni del Regolamento D.lgs. 10 agosto 2018, n. 101, e D.Lgs. n. 51/2018 recante "Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché' alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consigli") per quanto applicabile.

A tal fine, viene consegnata ai soggetti interessati apposita informativa sul trattamento dei dati personali ai sensi dell'art. 13 GDPR 2016/679.

1.4. Le forme di tutela del segnalante e del segnalato

Protezioni da eventuali ritorsioni

L'Agente Generale garantisce la protezione da qualsiasi atto di ritorsione, discriminazione o penalizzazione, diretto o indiretto, nei confronti della persona segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione.

Per "atto di ritorsione" deve intendersi qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'Autorità Giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto. Le condotte di natura ritorsiva sono esemplificate all'art. 17, comma 4 del D. Lgs. n. 24/2023.

L'assenza di natura ritorsiva dei comportamenti, atti o omissioni previsti dall'art. 17 del D. Lgs n. 24/2023 nei confronti del segnalante deve essere provata da colui che li ha posti in essere; salvo prova contraria, si presume che gli stessi siano conseguenza della segnalazione.

I divieti di ritorsione e le misure di protezione previste per il whistleblower si applicano anche:

- al facilitatore;
- alle persone del medesimo contesto lavorativo della persona segnalante e che sono legate ad essa da uno stabile legame affettivo o di parentela entro il quarto grado;

- ai colleghi di lavoro della persona segnalante, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;
- agli enti di proprietà della persona segnalante o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone;
- in caso di segnalazione anonima, se la persona segnalante è stata successivamente identificata.

2. IL PERIMETRO OGGETTIVO

2.1. Il contenuto della segnalazione

Sono oggetto di segnalazione le informazioni sulle violazioni (compresi i fondati sospetti) di normative nazionali e dell'Unione Europea che ledono l'interesse pubblico o l'integrità dell'Agenzia Generale, commesse nell'ambito dell'organizzazione dell'Agenzia Generale con cui la persona segnalante intrattiene uno dei rapporti giuridici indicati al punto 1.1.

Le informazioni sulle violazioni possono riguardare anche le violazioni non ancora commesse che il *whistleblower*, ragionevolmente, ritiene potrebbero esserlo sulla base di elementi concreti.

A titolo esemplificativo ma non esaustivo, le segnalazioni possono riguardare:

- illeciti amministrativi, contabili, civili[1] e/o penali;
- condotte illecite rilevanti ai sensi del D. Lgs. n. 231/01 nonché violazioni del Modello 231 e degli altri Protocolli Aziendali;
- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; protezione dei consumatori; protezione dei dati personali e sicurezza delle reti e dei sistemi informativi.

Non possono essere oggetto di segnalazione:

- contestazioni e/o rivendicazioni di lavoro contro superiori gerarchici, legate ad un interesse di carattere personale del segnalante;
- violazioni già disciplinate nelle direttive e regolamenti dell'Unione Europea e/o nelle disposizioni attuative nazionali che già garantiscono apposite procedure di segnalazione;
- violazioni in materia di sicurezza nazionale e in materia di appalti relativi ad aspetti di difesa o di sicurezza nazionale;
- le notizie palesemente prive di fondamento, le informazioni che sono già totalmente di dominio pubblico o, ancora, le informazioni acquisite sulla base di indiscrezioni o vociferazioni scarsamente attendibili (c.d. voci di corridoio).

Le segnalazioni devono essere rese in coscienza e buona fede.

È ammessa la segnalazione in forma anonima.

2.2. La segnalazione anonima

La segnalazione da cui non è possibile ricavare l'identità del segnalante è considerata anonima.

[1] Ad esempio, può costituire illecito civile, la violazione delle norme in materia di tutela dei lavoratori; una condotta non coerente con i doveri etici in capo al personale dipendente; l'utilizzo improprio dei beni aziendali; l'attività illecita e/o fraudolenta in danno della clientela o del patrimonio aziendale in genere.

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

Le segnalazioni anonime sono equiparate alle segnalazioni ordinarie quando le stesse siano adeguatamente circostanziate e rese con dovizia di particolari (con l'indicazione di nominativi, menzione di uffici specifici, procedimenti o eventi particolari, etc.).

Il gestore della segnalazione valuta la segnalazione anonima e assume le iniziative ritenute opportune per l'eventuale seguito di competenza ovvero procede all'archiviazione della stessa.

Stante l'anonimato non sono applicabili al segnalante le misure di protezione di cui ai paragrafi 1.2 e 1.3.

Nei casi di segnalazione o denuncia all'autorità giudiziaria o contabile o divulgazione pubblica anonima, se la persona segnalante è stata successivamente identificata e comunica all'ANAC di aver subito ritorsioni, si applicano le misure di protezione per le ritorsioni previste dall'art. 16, comma 4, del D. Lgs. 24/2023, per la tutela dalle ritorsioni.

Le segnalazioni anonime ricevute dal gestore della segnalazione sono registrate e conservate con la relativa documentazione non oltre cinque anni decorrenti dalla data di ricezione di tali segnalazioni, rendendo così possibile rintracciarle, nel caso in cui il segnalante, o chi abbia sporto denuncia, comunichi all' ANAC di aver subito misure ritorsive a causa di quella segnalazione o denuncia anonima.

3. I CANALI DI SEGNALAZIONE PREVISTI DAL D. LGS. N. 24/2023

3.1. Il canale di segnalazione interna

La persona segnalante, qualora abbia il ragionevole sospetto che si sia verificato o che possa verificarsi una delle violazioni indicate al paragrafo 2 che precede, può effettuare una segnalazione interna utilizzando i canali di seguito riportati:

- "*Portale Segnalazioni - Whistleblowing*", accessibile dal sito internet https://whistleblowing.mrstudiolegale.it/#/ cliccando su CANALE 154;
- Posta tradizionale, inviando segnalazione scritta all'indirizzo: Avv. Antonella Panetta c/o Studio Legale M&R – Via Reno 30 – Roma 00198 (solo in caso di indisponibilità del "*Portale Segnalazioni Whistleblowing*");

In caso di utilizzo del canale analogico tradizionale, conformemente a quanto previsto nelle linee guida Anac, la persona segnalante dovrà aver cura di inserire la segnalazione in due buste chiuse: la prima, contenente i suoi dati identificativi, unitamente alla fotocopia del documento di riconoscimento; la seconda, contenente la segnalazione, in modo da separare i dati identificativi del segnalante dalla segnalazione. Entrambe dovranno poi essere inserite in una terza busta chiusa che rechi all'esterno la dicitura "riservata" al gestore della segnalazione.

Le segnalazioni possono essere effettuate sia in forma scritta che in forma orale. Per le segnalazioni in forma orale, la persona segnalante può richiedere un incontro diretto con il gestore delle segnalazioni.

La persona segnalante dovrà fornire ogni elemento utile per consentire le verifiche e gli accertamenti necessari a valutare la fondatezza e l'oggettività dei fatti segnalati, indicando i riferimenti sullo svolgimento dei fatti (es. data, luogo), ogni informazione e/o prova, anche documentale, che possa fornire un valido riscontro circa la sussistenza di quanto segnalato; generalità o altri elementi che consentano di identificare chi ha commesso quanto dichiarato; generalità di eventuali altri soggetti che possano riferire sui fatti oggetto di segnalazione.

L'Agenzia Generale, per il tramite del proprio gestore delle segnalazioni, si impegna ad analizzare le segnalazioni ricevute nella lingua italiana.

Chiunque riceva una segnalazione al di fuori dei canali istituiti provvede a trasmetterla (in originale e con gli eventuali allegati) nel più breve tempo possibile e comunque entro 7 giorni dal suo ricevimento, al gestore delle segnalazioni, nel rispetto dei criteri di massima riservatezza, anche in conformità con le normative in materia di protezione dei dati e con modalità idonee a tutelare il segnalante e l'identità delle persone coinvolte, all'indirizzo Avv. Antonella Panetta c/o Studio Legale M&R – Via Reno 30 – Roma 00198 nel caso di ricevimento di segnalazione cartacea o via mail a.panetta@mrstudiolegale.it.

3.2. Il canale di segnalazione esterna

La persona segnalante può effettuare una segnalazione esterna se, al momento della sua presentazione, ricorre una delle seguenti condizioni:

a) non è prevista, nell'ambito del suo contesto lavorativo, l'attivazione obbligatoria del canale di segnalazione interna ovvero questo, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme a quanto previsto e stabilito dall'art. 4 del D. Lgs. n. 24/2023;

b) la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito;

c) la persona segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;

d) la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

L'ANAC è il soggetto competente a gestire il canale di segnalazione esterno che deve garantire, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

La segnalazione dovrà essere fatta accedendo alla piattaforma disponibile sul sito istituzionale dell'ANAC, accedendo al servizio dedicato al "*whistleblowing*" (*https://www.anticorruzione.it/-/whistleblowing*).

3.3. La divulgazione pubblica

Il D. Lgs. n. 24/2023 introduce un'ulteriore modalità di segnalazione consistente nella divulgazione pubblica, con la quale le informazioni sulle violazioni sono rese di pubblico dominio tramite la stampa o comunque attraverso mezzi di diffusione in grado di raggiungere un numero elevato di persone.

La persona segnalante che effettua una divulgazione pubblica beneficia della protezione prevista dal D. Lgs. n. 24/2023 se, al momento della divulgazione pubblica, ricorre una delle seguenti condizioni:

a) la persona segnalante ha previamente effettuato una segnalazione interna ed esterna ovvero ha effettuato direttamente una segnalazione esterna, alle condizioni e con le modalità previste dai paragrafi 3.1 e 3.2 e non è stato fornito riscontro in merito alle misure previste o adottate per dare seguito alle segnalazioni;

b) la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;

c) la persona segnalante ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove oppure in cui vi sia fondato timore che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa.

4. IL PROCESSO DI RICEZIONE E GESTIONE DELLE SEGNALAZIONI PERVENUTE TRAMITE IL CANALE DI SEGNALAZIONE INTERNO

La gestione del canale interno di segnalazione è affidata al Avv. Antonella Panetta, soggetto dotato dei requisiti di autonomia, imparzialità e indipendenza, requisiti che l'ANAC ritiene indispensabili e necessari ai fini della gestione del canale di segnalazione.

Il gestore del canale interno di segnalazione è deputato a svolgere le attività inerenti al processo di gestione delle segnalazioni.

Il procedimento di gestione delle segnalazioni si articola nelle seguenti fasi:

a) ricezione e protocollazione delle segnalazioni e attività preistruttoria;

b) verifica dei contenuti della segnalazione e attività istruttoria;

c) trasmissione della segnalazione al soggetto competente.

Con riferimento alla fase ***sub*** **a)** il gestore della segnalazione compie le seguenti attività:

- rilascia alla persona segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione. Nel computo di tale termine non si considerano i giorni festivi e di chiusura aziendale;
- mantiene le interlocuzioni con la persona segnalante e richiede a quest'ultima, se necessario, chiarimenti e integrazioni, anche documentali;
- archivia la segnalazione qualora la stessa risulti infondata "*ictu oculi*", ovvero troppo generica e/o priva degli elementi necessari ad avviare qualsiasi approfondimento.

Con riferimento alla fase ***sub*** **b)** il gestore della segnalazione compie le seguenti attività:

- in relazione all'oggetto della segnalazione, identifica le ulteriori funzioni aziendali da coinvolgere per lo svolgimento delle ulteriori verifiche;
- valuta le ulteriori azioni da compiere, richiedendo, se del caso, l'intervento di soggetti terzi esterni preposti alle indagini e accertamenti che non possono essere svolti in ambito aziendale;
- verifica la presenza di interessi personali del segnalante ovvero di altri soggetti in rapporto con quest'ultimo.

Con riferimento alla fase ***sub*** **c)** il gestore della segnalazione compie le seguenti attività:

- predispone un *report* contenente le risultanze emerse dall'attività istruttoria;
- nel caso in cui la segnalazione non sia ritenuta manifestamente infondata, identifica, con propria valutazione, anche tenendo conto di quanto emerso in conseguenza dell'intervento di soggetti terzi esterni, i soggetti ai quali inoltrare la segnalazione medesima in relazione ai profili di illiceità riscontrati e ai contenuti della segnalazione, individuando il destinatario o i destinatari del *report* tra i seguenti soggetti e rimettendo agli stessi i provvedimenti decisionali opportuni e susseguenti alla segnalazione, ognuno secondo le proprie competenze: a) Amministratore/i e/o legale/i rappresentante/i *pro tempore* dell'Agenzia Generale e/o Agente Generale; b) enti o istituzioni esterne;
- in ogni caso, il gestore della segnalazione provvede a comunicare l'esito della propria valutazione all'Amministratore/i legale/i rappresentante/i *pro tempore* dell'Agenzia Generale e/o all'Agente Generale, per le ulteriori eventuali azioni che si rendano necessarie a tutela dell'Agenzia, ad eccezione dei casi in cui le segnalazioni riguardino l'Amministratore/i legale/i rappresentante/i dell'Agenzia o l'Agente Generale;
- qualora il gestore della segnalazione ravvisi che la segnalazione sia intenzionalmente diffamatoria ovvero si riveli infondata ed effettuata con dolo o colpa grave, lo comunica all'Amministratore/i e/o legale/i

rappresentante/i *pro tempore* dell'Agenzia Generale e/o all'Agente Generale che valuta la responsabilità, sotto il profilo disciplinare, del soggetto segnalante.

Ai sensi dell'art. 5, comma 1, lett. d) del D. Lgs. n. 24/2023, il gestore della segnalazione deve, a prescindere dalla conclusione o meno delle fasi in cui si articola il procedimento di gestione della segnalazione, fornire un riscontro, anche interlocutorio, al segnalante entro tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione.

Qualora il gestore della segnalazione intenda procedere alla archiviazione della segnalazione, dovrà parimenti fornire riscontro al segnalante entro lo stesso termine e motivare la propria scelta di procedere all'archiviazione della segnalazione.

Ai sensi dell'art. 14 del D. Lgs. n. 24/2023, il gestore della segnalazione, al fine di garantire la ricostruzione delle diverse fasi del processo, assicura la tracciabilità delle segnalazioni e delle relative attività di ricezione, istruttoria e valutazione, nonché la conservazione della documentazione inerente alle segnalazioni e le relative attività di verifica. Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

Il gestore della segnalazione raccoglie, annualmente 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 identificare le aree di criticità dell'Agenzia Generale sulle quali risulti necessario intervenire in termini di miglioramento e/o implementazione del sistema di controllo interno.

5. PRIVACY

Ai sensi della vigente normativa in materia di privacy il titolare del trattamento dei dati personali acquisiti nella gestione delle segnalazioni è individuato nell'Agente Generale.

La documentazione relativa alle segnalazioni è confidenziale e pertanto il titolare adotta le opportune misure di sicurezza atte a garantire una appropriata gestione e archiviazione della documentazione assicurando inoltre l'accesso alle informazioni ivi contenute "esclusivamente ai soggetti che abbiano necessità di conoscerle per lo svolgimento dell'attività lavorativa, in ragione delle responsabilità attribuite e in relazione al ruolo/posizione organizzativa ricoperta nell'Impresa (principio del need-to-know)".

I dati personali dei segnalanti e di altri soggetti eventualmente coinvolti, acquisiti in occasione della gestione delle segnalazioni, saranno trattati in piena conformità a quanto stabilito dall'attuale Normativa privacy, nonché nella misura necessaria e per il periodo strettamente necessario per le finalità previste dalla stessa.

6. DISPOSIZIONI FINALI

La procedura e le disposizioni individuate nel presente atto potranno essere sottoposti a eventuale revisione qualora necessario.

7. CLAUSOLA DI RINVIO

Per tutto quanto non espressamente previsto nel presente atto si rimanda al D.lgs. n. 24/2023, alle indicazioni fornite da ANAC e alla normativa vigente.

Informativa ai sensi della normativa sulla protezione dei dati personali – Whistleblowing

Ai sensi dell'art.13 del Regolamento (UE) n. 2016/679 (Regolamento Generale sulla Protezione dei Dati, di seguito GDPR) e del d.lgs. 24/2023, l'Agente Generale sig. Di Sante Antonio (o Società Di Sante Antonio), Agenzia Generale di Verbania, fornisce, qui di seguito, l'informativa sui trattamenti dei dati personali effettuati in relazione alla gestione delle Segnalazioni, disciplinate dalla Procedura *Whistleblowing* dell'Agenzia Generale.

Categorie di dati personali

a) Dati personali comuni di cui all'art. 4, punto 1, del GDPR del Segnalante (nel caso di Segnalazioni non anonime) nonché di eventuali Persone coinvolte o menzionate nella Segnalazione e Facilitatori, come definiti dalla Procedura Whistleblowing (di seguito "Interessati"), quali: dati anagrafici (ad es. nome, cognome, data e luogo di nascita), dati di contatto (es. numero telefonico fisso e/o mobile, indirizzo postale/e-mail).

b) Categorie particolari di dati di cui all'art. 9) del GDPR, qualora inserite nella segnalazione e di dati personali relativi a condanne penali e reati (di cui all'art. 10 GDPR).

Finalità del trattamento e relativa base giuridica

I suddetti dati personali sono trattati dal Titolare per le seguenti finalità:

a) gestione della Segnalazione effettuata ai sensi del d.lgs. n. 24/2023;

b) adempimento di obblighi previsti dalla legge o dalla normativa comunitaria;

c) difesa o accertamento di un di un proprio diritto in contenziosi civili, amministrativi o penali.

Tenuto conto della normativa di riferimento e in particolare, del D.lgs. 24/2023, si precisa che:

- il trattamento dei dati "comuni" si fonda sull'obbligo di legge a cui è soggetto il Titolare del trattamento (art. 6, par. 1, lett. c) del GDPR), nonché per motivi di interesse pubblico rilevante (art. 9 GDPR);
- il trattamento di dati "particolari" si fonda su motivi di interesse pubblico rilevante (art. 9 GDPR), anche in ragione dell'art. 2-sexies lett. dd) del D.lgs. 196/2003;
- il trattamento di dati relativi a condanne penali e reati, tenuto conto di quanto disposto dall'art. 10 GDPR, si fonda sull'obbligo di legge a cui è soggetto il Titolare del trattamento (art. 6, par. 1, lett. c), GDPR) e per motivi di interesse pubblico rilevante (art. 9 GDPR), anche in ragione dell'art. 2-octies lett. a) del D.lgs. 196/2003.

I dati personali sono dunque acquisiti in quanto contenuti nella segnalazione e/o in atti e documenti a questa allegati, si riferiscono al soggetto segnalante e possono altresì riferirsi a persone indicate come possibili responsabili delle condotte illecite, nonché a quelle a vario titolo coinvolte nelle vicende segnalate.

Il conferimento dei dati è necessario per il conseguimento delle finalità di cui sopra; il loro mancato, parziale o inesatto conferimento potrebbe avere come conseguenza l'impossibilità di gestire la segnalazione.

Conservazione dei dati personali

L'Agenzia Generale conserva i dati personali secondo nei termini previsti dall'art. 14 del D. Lgs. n. 24/2023, cioè per il tempo necessario al trattamento della segnalazione e comunque per non oltre 5 anni a decorrere dalla data di comunicazione dell'esito finale della Segnalazione al gestore della segnalazione.

I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati tempestivamente.

Modalità e logica del trattamento

I trattamenti dei dati sono effettuati manualmente e/o attraverso strumenti automatizzati informatici e telematici con logiche correlate alle finalità sopraindicate e, comunque, in modo da garantirne la sicurezza e la riservatezza.

Il sistema di gestione delle Segnalazioni garantisce, in ogni fase, la riservatezza dell'identità del Segnalante, delle Persone coinvolte e/o comunque menzionate nella Segnalazione, del contenuto della Segnalazione e della relativa documentazione, fatto salvo quanto previsto dall'art. 12 del d.lgs. n. 24/2023.Il Titolare del trattamento impiega idonee misure di sicurezza (crittografia dei file), organizzative, tecniche e fisiche, per tutelare le informazioni dall'alterazione, dalla distruzione, dalla perdita, dal furto o dall'utilizzo improprio o illegittimo, nel pieno rispetto del'art. 32 del GDPR.

Titolare, categorie di persone autorizzate al trattamento dei dati e categorie di destinatari dei dati personali

Il Titolare del trattamento dei dati personali è l'Agente Generale sig. Di Sante Antonio (o Società Di Sante Antonio), con sede in p.zza San Vittore 5 28923 Verbania.

Il Titolare ha nominato, ai sensi dell'art. 4, comma 2, del D. Lgs. n. 24/2023, l'Avv. Antonella Panetta quale gestore del canale di segnalazione e quale persona espressamente autorizzata al trattamento dei dati personali.

I dati personali del segnalante e quelli delle persone indicate come possibili responsabili delle condotte illecite, nonché delle persone a vario titolo coinvolte nelle vicende segnalate, non saranno oggetto di diffusione, tuttavia, se necessario possono essere trasmessi all'Autorità Giudiziaria (quale titolare autonomo del trattamento). Nell'ambito dei procedimenti penali eventualmente istaurati, l'identità del segnalante sarà coperta da segreto nei modi e nei limiti previsti dall'art. 329 c.p.p. 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 la riservatezza non è opponibile per legge, (es. indagini penali, tributarie o amministrative, ispezioni di organi di controllo) l'identità del segnalante verrà protetta sin dalla ricezione della segnalazione e in ogni fase successiva, in ossequio alle vigenti disposizioni.

Diritti degli interessati

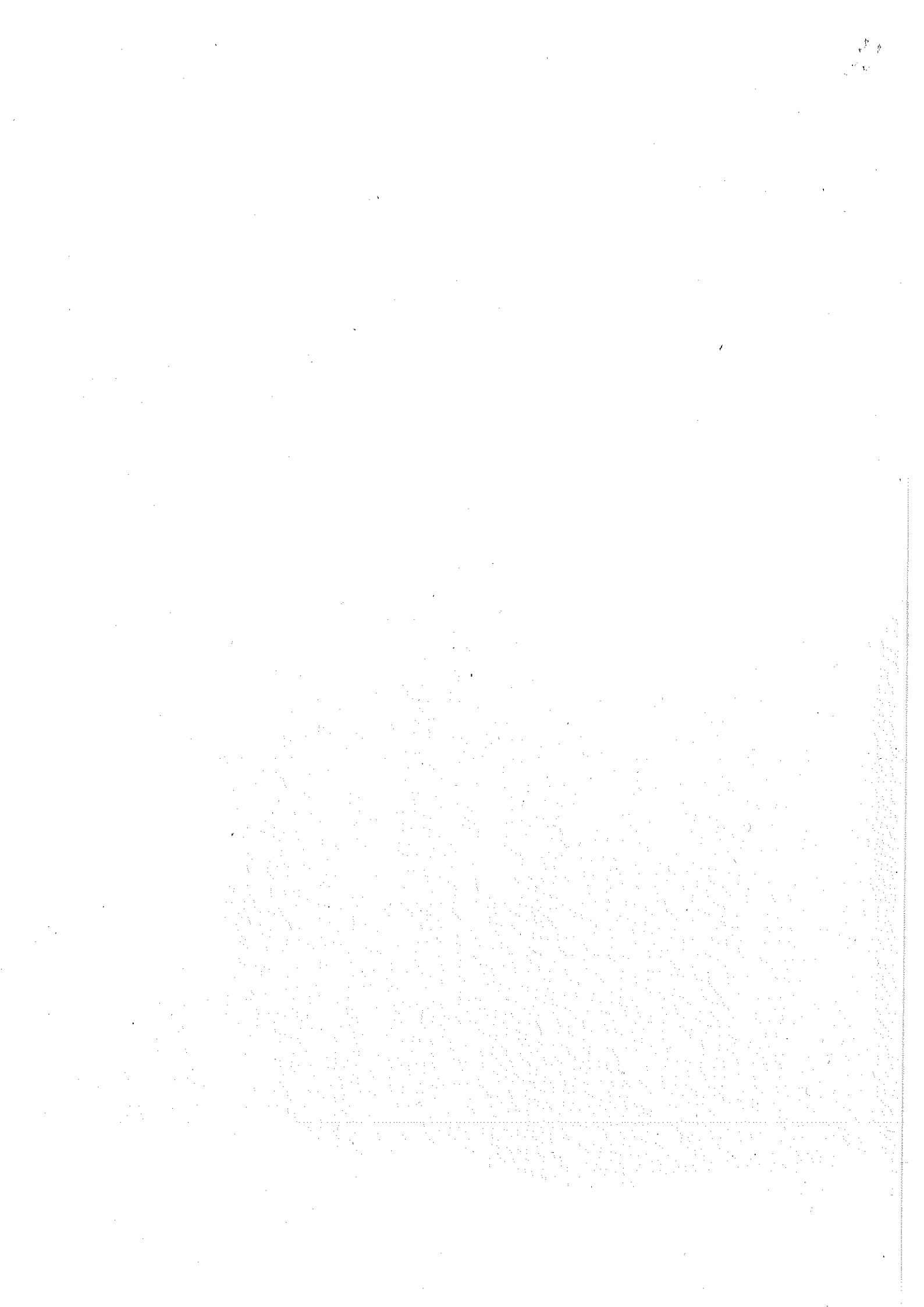
L'interessato, nelle persone del Segnalante o del Facilitatore, ha diritto di accedere in ogni momento ai dati che lo riguardano e di esercitare i diritti previsti dagli articoli da 15 al 22 del GDPR, per quanto applicabili (diritto di accesso ai dati personali, diritto a rettificarli, diritto di ottenerne la cancellazione o cd. diritto all'oblio, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati personali o quello di opposizione al trattamento), inviando una e-mail all'indirizzo: a.panetta@mrstudiolegale.it.

Inoltre, l'interessato ha diritto di proporre un reclamo al Garante della protezione dei dati personali.

I suddetti diritti non sono esercitabili dalla persona coinvolta o dalla persona menzionata nella segnalazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, ai sensi dell'art. 2-undecies del Codice Privacy in quanto dall'esercizio di tali diritti potrebbe derivare un pregiudizio effettivo e concreto alla tutela della riservatezza dell'identità della persona segnalante.

Luogo e data, Verbania, 19/12/2023

L'Agente Generale Di Sante Antonio



ATTIVITA' DI TRATTAMENTO	DESCRIZIONE DELL'ATTIVITÀ DI TRATTAMENTO	MODALITA' DI TRATTAMENTO	FINALITÀ	OPERAZIONI DI TRATTAMENTO	BASE GIURIDICA DEL TRATTAMENTO
In questo campo sono indicate la tipologia di attività nell'ambito della quale vengono trattati i dati personali. L'attività di trattamento è rappresentata dalla tipologia di attività effettuata.	In questo campo sono inserite una descrizione sintetica dell'attività nell'ambito della quale vengono trattati i dati personali. Inserire una breve descrizione dell'attività nell'ambito della quale è effettuato il trattamento dei dati, con indicazione delle sue principali caratteristiche	In questo campo sono indicati i mezzi e gli strumenti attraverso i quali viene effettuato il trattamento. Indicare una o più modalità di trattamento. Le modalità di trattamento sono: - Utilizzo di servizi ICT (il trattamento è effettuato attraverso l'utilizzo di applicativi informatici) - Utilizzo di strumenti di office automation (il trattamento è effettuato utilizzando gli strumenti di Office, come Word, Excel, etc., presenti su una postazione di lavoro) - Gestione Manuale (il trattamento è effettuato mediante l'utilizzo di supporti cartacei)	In questo campo è indicato lo scopo determinato, esplicito e legittimo, perseguito nell'ambito dell'attività di trattamento di dati personali. Si precisa che il trattamento è strettamente legato alla finalità.	Le operazioni di trattamento sono: - Raccolta - Registrazione - Conservazione - Estrazione - Consultazione - Elaborazione - Modifica - Comunicazione - Diffusione - Limitazione - Cancellazione - Distruzione	Le basi giuridiche del trattamento sono: - Consenso dell'interessato - Esecuzione di un contratto con l'interessato o esecuzione di misure precontrattuali adottate su richiesta dello stesso - Obbligo legale per il titolare - Salvaguardia interessi vitali dell'interessato o altra persona fisica - Altri fondamenti connessi al trattamento di categorie particolari di dati personali - art. 9 par. 2 del Regolamento - Legittimo interesse
Trattamento dei dati in esecuzione del D. Lgs. n. 24 del 10 marzo 2023	La gestione delle informazioni funzionali all'adempimento ed all'esecuzione del D.Lgs. N. 24 del 10 marzo 2023 viene effettuata attraverso un canale esterno alle risorse informatiche del titolare. Il trattamento avviene infatti mediante un'apposita piattaforma attivata dal titolare e basata sul software opensource "GlobalLeaks"	Utilizzo di servizi ICT; Gestione manuale	I dati personali saranno trattati per finalità correlate alla gestione della segnalazione e all'adempimento degli obblighi legali previsti dalla normativa vigente in materia di whistleblowing (D.Lgs. N. 24 del 10 marzo 2023).	Raccolta; Registrazione; Estrazione; Conservazione; Limitazione; Consultazione; Elaborazione; Cancellazione; Distruzione; Comunicazione; Limitazione	Obbligo legale per il titolare - Motivi di interesse pubblico rilevante

INFORMATIVA	CATEGORIA DI INTERESSATI	DATI COMUNI	CATEGORIE PARTICOLARI DI DATI PERSONALI	DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI	TERMINI DI CANCELLAZIONE (ove possibile)
Le opzioni su "Informativa" sono: - SI, Informativa ex art. 13 del Regolamento UE 679/2016 (Dati raccolti presso l'interessato) - SI, Informativa ex art. 14 del Regolamento UE 679/2016 (Dati ottenuti da soggetto diverso dall'interessato)	Le categorie di interessati sono: - Contraenti e loro familiari - Assicurati e loro familiari - Beneficiari - Clienti potenziali - Dipendenti e collaboratori o altro personale impiegato - Candidati ad una posizione di lavoro - Subagenti e altri intermediari - Professionisti (consulenti del lavoro, avvocati, commercialisti, ecc.)	I dati comuni sono: - Dati anagrafici - Dati contabili, fiscali e finanziari - Dati inerenti il rapporto di lavoro - Dati derivanti da tracciamenti (log) - Dati inerenti situazioni giudiziarie civili, amministrative, tributarie - Dati che consentono la geolocalizzazione - Dati audio/foto/video - Dati di profilazione	Le categorie particolari di dati personali sono le informazioni che rivelano: - L'origine razziale ed etnica - Le convinzioni religiose, filosofiche o di altro genere - Le opinioni politiche - L'adesione a partiti - L'adesione a sindacati - L'adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale - Lo stato di salute (Assistenza sanitaria) - La vita sessuale - Dati biometrici	I dati personali relativi a condanne penali e reati sono: - Iscrizione nel casellario giudiziale - Condizione di indagato/imputato o altre situazioni giudiziarie (condanne penali e reati o connesse misure di sicurezza) - Sottoposizione a misure detentive carcerarie	In questo campo sono indicati i termini di cancellazione dei dati personali trattati, ove possibile, in mesi o anni oppure i criteri oggettivi utilizzati per determinare tale periodo.
SI, Informativa ai sensi dell'art. 13 del Regolamento UE 679/2016 (Dati raccolti presso l'interessato)	Soggetto segnalante e persone indicate come possibili responsabili delle condotte illecite	Dati anagrafici; Dati contabili, fiscali e finanziari; Dati inerenti il rapporto di lavoro; Dati inerenti situazioni giudiziarie civili, amministrative, tributarie; Dati audio/foto/video;Dati che consentono la geolocalizzazione; Dati derivanti da tracciamenti (log)	Tutte le categorie particolari di dati personali	Tutti dati riferibili a condanne penali e reati	I dati personali dell'interessato sono trattati fino alla data di comunicazione dell'esito finale della procedura di segnalazione e per un periodo massimo di 5 anni

DESTINATARI ESTERNI DEI DATI	TRASFERIMENTI EXTRA_UE	PAESI EXTRA-UE O ORGANIZZAZIONI INTERNAZIONALI VERSO I QUALI VENGONO TRASFERITI I DATI
In questo campo sono indicati i soggetti cui vengono comunicati i dati personali trattati al fine di specificare il flusso di informazioni dal titolare verso l'esterno. I destinatari esterni dei dati sono, quindi, i soggetti ai quali i dati personali possono essere comunicati da parte del titolare. I destinatari esterni dei dati sono tipicamente raggruppati nelle seguenti categorie: - Autorità pubbliche (ad esempio, IVASS) - Soggetti privati (persone fisiche o giuridiche)	Le condizioni che autorizzano il trasferimento all'estero sono: - Trasferimento sulla base di una decisione di adeguatezza (art. 45 del Regolamento) - Trasferimento soggetto a garanzie adeguate (art. 46 del Regolamento) - Consenso dell'interessato al trasferimento - Esecuzione di un contratto tra titolare e interessato - Esecuzione di un contratto tra titolare e soggetto che agisce per conto dell'interessato - Interesse pubblico - Accertamento, esercizio o difesa di un diritto in sede giudiziaria - Tutela degli interessi vitali dell'interessato o di terzi	Nel caso in cui nel campo "Trasferimenti all'estero" sia stata indicata al presenza di una condizione che autorizza il trasferimento all'estero dei dati personali, in questo campo è indicata la denominazione del paese extra-UE o dell'organizzazione internazionale verso i quali sono trasferiti i dati personali
I dati potranno essere comunicati alle Autorità pubbliche, ad Avvocati e Professionisti.	N/A	N/A

MISURE DI SICUREZZA (Rif. Regolamento UE 679/2016 art. 32)	TITOLARE PER IL QUALE E' EFFETTUATO IL TRATTAMENTO	RESPONSABILE ESTERNO DEL TRATTAMENTO
Le misure di sicurezza sono: - Minimizzazione della quantità di dati personali - Cifratura - Pseudonimizzazione - Controllo degli accessi logici ed autenticazione - Cancellazione sicura - Sicurezza dell'ambiente operativo - Sicurezza della rete e delle comunicazioni - Tracciatura e monitoraggio - Policy di gestione sicura dell'hardware, delle risorse e dei dispositivi - Sistemi di Backup e Continuità operativa - Protezione delle fonti di rischio ambientali - Politiche e procedure per la protezione dei dati personali - Accordi con i Responsabili del trattamento e terze parti - Gestione degli incidenti di sicurezza e delle Violazioni dei dati personali - Gestione e formazione del personale - Controllo degli accessi fisici - Procedure di archiviazione e distruzione dei documenti cartacei	In questo campo sono indicati i Titolari per conto dei quali sono effettuate determinate operazioni di trattamento, in veste di responsabile esterno.	In questo campo sono indicati i nominativi dei responsabili esterni del trattamento. Il responsabile esterno del trattamento è la persona fisica o giuridica che tratta dati personali per conto del titolare del trattamento.
Si rinvia alla descrizione delle misure adottate contenuta nella DPIA ""TRATTAMENTO CONSISTENTE NELL'ADOZIONE DI UNA PIATTAFORMA ON LINE PER LA GESTIONE DELLE SEGNALAZIONI DI CUI AL D.LGS. N. 24/2023"	N/A	Avv. Antonio Mammone, C.F. MMMNTN74E18M2085, con Studio Legale in 00198 Roma alla via Reno n. 30

Responsabile del trattamento	Indirizzo	Email	Rappresentante del Responsabile
Per assistenza negli adempimenti di cui al D. Lgs. n. 24 del 10 marzo 2023: Avv. Antonio Mammone, C.F. MMMNTN74E18M208S, con Studio in via Reno n. 30 - 00198 Roma			

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

DI SANTE SAS DI ALICE DI SANTE E ANDREA DI SANTE

Agenzia Generale di Generali Italia S.p.a. di Verbania

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO *EX*D.LGS.N. 231, 8 GIUGNO 2001

PARTE GENERALE

Allegato 3

Sistema Sanzionatorio

Sommario

1. Principi generali

L'efficace attuazione del Modello da parte dell'Agenzia richiede l'introduzione di un sistema disciplinare idoneo a sanzionare il mancato rispetto dei principi, delle prescrizioni e degli standard di comportamento indicati nel Modello stesso e nel Codice Etico come previsto dagli artt. 6, comma 2, lett. e) e 7, comma 4, lett. b) del Decreto.

Il Sistema Sanzionatorio si applica all'Organo Amministrativo, ai dipendenti della Società, ai consulenti esterni, ai collaboratori esterni, all'Organismo di Vigilanza nonché ai *partner* commerciali della Società.

L'accertamento delle infrazioni, i procedimenti disciplinari e l'irrogazione delle sanzioni sono affidati alla competente Funzione aziendale anche su impulso dell'OdV, il quale dovrà essere costantemente aggiornato in ordine alle violazioni accertate e alle sanzioni irrogate.

Il presente Modello prevede, infine, provvedimenti sanzionatori per i soggetti, anche esterni alla Società, che devono comunque ritenersi destinatari delle norme medesime.

L'applicazione delle sanzioni previste rimane del tutto indipendente dall'inizio e dall'esito di eventuali procedimenti penali ed è ispirata alla necessità di una tempestiva applicazione.

Nell'ottica preventiva ispirata dal Decreto, invero, si ritengono condotte sanzionabili quelle che, pur non essendo penalmente rilevanti, sono dirette a ledere ovvero a indebolire l'efficacia organizzativa e di controllo del Modello, compromettendone la funzione normativa.

Il rispetto delle disposizioni e delle regole comportamentali di cui al Modello e al Codice Etico rappresenta un obbligo per i dipendenti ai sensi degli artt. 2104 e 2105 c.c.

Gli obblighi definiti nel Modello sono vincolanti per tutti i destinatari e formeranno oggetto di apposita comunicazione.

È previsto, altresì, che le disposizioni relative agli obblighi vengano costantemente pubblicizzate all'interno e all'esterno dell'Agenzia, attraverso, ad esempio, attività di formazione e informazione in materia, ovvero, mediante affissione della regolamentazione in luoghi accessibili a tutti.

La verifica dell'adeguatezza del Sistema Disciplinare, il costante monitoraggio degli eventuali procedimenti di irrogazione delle sanzioni nei confronti dei dipendenti, nonché degli interventi nei confronti dei soggetti esterni sono affidati all'OdV, che procede alla segnalazione delle carenze riscontrate.

Costituiscono, a titolo esemplificativo, violazione degli obblighi definiti nel Modello i seguenti comportamenti:

a) mancato rispetto delle prescrizioni contenute nel Modello e nel Codice Etico;
b) mancato rispetto delle prescrizioni inerenti alle modalità di documentazione, di conservazione e di controllo degli atti, volte a garantirne la trasparenza, veridicità e verificabilità;

c) violazione e/o elusione del sistema di controllo, mediante sottrazione, distruzione o alterazione della documentazione relativa alle procedure istituite;

d) impedito controllo o accesso alle informazioni e alla documentazione nei confronti dei soggetti preposti, incluso l'Organismo di Vigilanza;

e) mancata Segnalazione di situazioni di conflitto di interessi, soprattutto con riguardo ai rapporti con la Pubblica Amministrazione;

f) omissione di controlli e/o di informazioni attinenti al bilancio e alle altre comunicazioni sociali;

g) omessa vigilanza sul comportamento del personale operante all'interno della propria sfera di responsabilità, al fine di verificarne le azioni poste in essere nell'ambito delle aree a rischio;

h) effettuazione di Segnalazioni ai sensi del D.lgs. nr. 24/23 infondate, quando si accerti che il Segnalante ha agito dolosamente nella consapevolezza della falsità della Segnalazione;

i) violazione delle misure di tutela del segnalante e degli altri soggetti tutelati dal D.lgs. nr. 24/23 contro ogni forma di ritorsione, discriminazione o penalizzazione;

j) violazione del divieto di riservatezza dell'identità del segnalante, salvo i casi in cui la diffusione dell'identità sia consentita dal D.lgs. nr. 24/23;

k) mancato rispetto delle procedure di gestione delle segnalazioni di cui al D.lgs. nr. 24/23;

l) comportamenti che integrino le fattispecie di reato contemplate nel Decreto;

m) comportamenti che, sebbene non rientranti nelle fattispecie di reato di cui al Decreto, siano diretti in modo univoco alla loro commissione.

Inoltre, il mancato rispetto delle previsioni dell'art. 20 del D. Lgs. n. 81/2008[1], nonché delle procedure connesse alla tutela della salute e sicurezza sul lavoro, costituisce motivo di applicazione dei provvedimenti sanzionatori previsti dal presente Sistema Disciplinare.

---

[1] D. Lgs. n. 81/2008: art. 20 - Obblighi dei lavoratori:

"1. Ogni lavoratore deve prendersi cura della propria salute e di quella delle altre persone presenti sul luogo di lavoro, su cui ricadono gli effetti delle sue azioni o omissioni, conformemente alla sua formazione, alle istruzioni e ai mezzi forniti dal datore di lavoro.

2. I lavoratori devono in particolare:

a) contribuire, insieme al datore di lavoro, ai dirigenti e ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro;

b) osservare le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva e individuale;

c) utilizzare correttamente le attrezzature di lavoro, le sostanze e i preparati pericolosi, i mezzi di trasporto nonché i dispositivi di sicurezza;

d) utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione;

e) segnalare immediatamente al datore di lavoro, al dirigente o al preposto le deficienze dei mezzi e dei dispositivi di cui alle lettere c) e d), nonché qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità, e fatto salvo l'obbligo di cui alla successiva lettera f), per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza;

f) non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di Segnalazione o di controllo;

g) non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori;

h) partecipare ai programmi di formazione e di addestramento organizzati dal datore di lavoro;

i) sottoporsi ai controlli sanitari previsti nei loro confronti dal presente Decreto Legislativo o comunque disposti dal medico competente.

3. I lavoratori di aziende che svolgono attività in regime di appalto o subappalto, devono esporre apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro. Tale obbligo grava anche in capo ai lavoratori autonomi che esercitano direttamente la propria attività nel medesimo luogo di lavoro, i quali sono tenuti a provvedervi per proprio conto".

Il tipo e l'entità delle sanzioni disciplinari per il personale dipendente saranno irrogate alla luce del principio di proporzionalità previsto dall'art. 2106 del Codice Civile, secondo la gravità dell'infrazione e valutati in base ai seguenti criteri generali:

1. intensità del dolo/gravità della colpa (negligenza, imprudenza, imperizia);
2. mansioni e livello gerarchico del dipendente;
3. rilevanza degli obblighi violati;
4. potenzialità ed entità del danno derivante alla Società;
5. presenza di circostanze aggravanti o attenuanti;
6. reiterazione delle condotte inosservanti;
7. livello di responsabilità gerarchica o tecnica del soggetto interessato.

2. Sanzioni nei confronti dei dipendenti

I comportamenti tenuti dai lavoratori dipendenti in violazione delle singole regole comportamentali previste nel presente Modello costituiranno illeciti disciplinari.

Le sanzioni irrogabili nei riguardi dei lavoratori dipendenti sono quelle previste dal CCNL applicato in Agenzia, nel rispetto delle procedure previste dall'art. 7 della Legge 30 maggio 1970, n. 300 (Statuto dei Lavoratori), nonché in linea con i contenuti del Codice Disciplinare emanato da Generali. Le sanzioni disposte dalla Società saranno comunicate all'OdV.

Le condotte sopra indicate, se poste in essere dai dipendenti, possono dar luogo, secondo la gravità dell'infrazione, ai seguenti provvedimenti:

a) **rimprovero verbale** in caso di lieve inosservanza, da parte del dipendente, delle prescrizioni contenute nel Modello e nel Codice Etico;
b) **censura per iscritto** qualora le violazioni di cui al punto precedente siano gravi o reiterate;
c) **sospensione dal servizio e dallo stipendio**, non superiore a quanto indicato nel CCNL, nei confronti del dipendente che violi dolosamente le prescrizioni comportamentali disciplinate nel Modello e nel Codice Etico che non integrino reato presupposto, nonché nei casi di reiterata violazione colposa di obblighi rilevanti;
d) **licenziamento per giustificato motivo con preavviso** al lavoratore che adotti, nell'espletamento delle attività sensibili, un comportamento non conforme alle prescrizioni del Modello e diretto in modo univoco al compimento di un reato sanzionato dal Decreto, ovvero al lavoratore che commetta infrazioni alla disciplina ed alla diligenza del lavoro, le quali, pur essendo di maggiore rilievo di quelle contemplate dal punto c) non siano così gravi da rendere applicabile la sanzione di cui alla lett. e);
e) **licenziamento per giusta causa senza preavviso** per il dipendente che adotti, nell'espletamento delle attività nelle aree sensibili, un comportamento in violazione del Modello, tale da determinare l'applicabilità a carico della Società delle sanzioni previste dal Decreto, ovvero il verificarsi delle infrazioni richiamate ai punti precedenti con la determinazione di un grave pregiudizio materiale o morale alla Società o, ancora, nell'ipotesi in cui la violazione dei doveri discendenti dalla legge o dal rapporto di lavoro non consenta la prosecuzione del rapporto stesso neppure in via provvisoria, a norma dell'art. 2119 c.c., fermo il rispetto del procedimento disciplinare. Con la contestazione può essere disposta la revoca delle eventuali procedure affidate al soggetto interessato.

Il datore di lavoro non potrà adottare alcun provvedimento disciplinare nei confronti del lavoratore senza avergli preventivamente contestato l'addebito e senza averlo sentito a sua difesa.

Salvo che per il rimprovero verbale, la contestazione dovrà essere effettuata per iscritto ed i provvedimenti disciplinari non potranno essere comminati prima che siano trascorsi 5 giorni, nel corso dei quali il lavoratore potrà presentare le sue giustificazioni.

Il lavoratore potrà farsi assistere da un rappresentante dell'Associazione sindacale cui aderisce o conferisce mandato.

3. Misure nei confronti degli Amministratori

La Società valuta con estremo rigore le infrazioni al presente Modello poste in essere dai Soci amministratori, rappresentando gli stessi l'immagine della Società verso i dipendenti, i collaboratori, i soci, i clienti, i creditori, le Autorità di Vigilanza e il pubblico in generale.

I valori della correttezza e della trasparenza devono essere innanzitutto fatti propri, condivisi e rispettati da coloro che guidano le scelte aziendali, in modo da costituire esempio e stimolo per tutti i soggetti che, a qualsiasi livello, operano per la Società.

Le violazioni dei principi e delle misure previste dal Modello di organizzazione, gestione e controllo adottato dalla Società ad opera di un Amministratore sono segnalate dall'Organismo di Vigilanza all'Assemblea dei soci, la quale valuta le azioni più opportune, sentito l'OdV.

4. Misure nei confronti di collaboratori, consulenti, *partner*, controparti e altri soggetti esterni

Ogni comportamento posto in essere nell'ambito di un rapporto contrattuale dai collaboratori, consulenti, *partners*, controparti e altri soggetti esterni in contrasto con le linee di condotta indicate dal presente Modello e nel Codice Etico costituisce inadempimento grave delle obbligazioni contrattuali ai sensi dell'art. 1453 c.c. e può determinare la risoluzione del rapporto contrattuale per giusta causa, fatta salva la facoltà di agire per il risarcimento del danno.

Si provvederà, ove necessario, all'elaborazione, all'aggiornamento e all'inserimento nelle lettere di incarico o negli accordi negoziali o di *partnership* di tali specifiche clausole contrattuali che prevedano anche l'eventuale richiesta di risarcimento di danni derivanti alla Società dall'applicazione da parte del giudice delle misure previste dal Decreto anche indipendentemente dalla risoluzione del rapporto contrattuale.

Con particolare riferimento ai subagenti e produttori valgono altresì le disposizioni civilistiche vigenti nonché, rispettivamente, le disposizioni dell'Accordo Nazionale subagenti del 1986 e del CCNL produttori 1939.

5. Misure nei confronti dell'Organismo di Vigilanza

In ipotesi di negligenza e/o imperizia dell'Organismo di Vigilanza nel vigilare sulla corretta applicazione del Modello e sul loro rispetto e nel non aver saputo individuare casi di violazione allo stesso procedendo alla loro eliminazione, l'Organo Amministrativo assumerà gli opportuni provvedimenti secondo le modalità previste dalla normativa vigente, inclusa la revoca dell'incarico.

Al fine di garantire il pieno esercizio del diritto di difesa deve essere previsto un termine entro il quale l'interessato possa far pervenire giustificazioni e/o scritti difensivi e possa essere ascoltato. In caso di presunti comportamenti illeciti da parte di membri dell'Organismo di Vigilanza, l'Organo Amministrativo, una volta ricevuta la Segnalazione, indaga circa l'effettivo illecito occorso e quindi determina la relativa sanzione da applicare.

DI SANTE SAS DI ALICE DI SANTE E ANDREA DI SANTE

Agenzia Generale di Generali Italia S.p.a. di Verbania

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO *EX* D.LGS.N.231, 8 GIUGNO 2001

CODICE ETICO

Sommario

1. - Premessa

La Società impronta la propria attività ai principi di corretta gestione societaria, fondata sull'adeguatezza dei propri assetti organizzativi, amministrativi e contabili e svolge le proprie attività nel rispetto delle norme nazionali e sovranazionali secondo una condotta improntata ai principi di onestà, integrità e rispetto degli interessi dei clienti, dipendenti, *partner* commerciali e finanziari.

2. - Il Codice Etico

Il presente Codice Etico rappresenta uno strumento di autoregolazione, volontario e unilaterale, volto a rendere trasparente l'attività aziendale e a indirizzarne eticamente lo svolgimento, rispettando quanto stabilito dalle norme vigenti, dai contratti di lavoro, da regolamenti e procedure interne.

Il presente Codice Etico, inoltre, si conforma al Codice Etico del Gruppo Generali e al Codice di Comportamento di Gruppo.

La struttura organizzativa ed il sistema di regole della Società devono, in ogni momento, essere coerenti con il presente Codice e facilitarne la piena applicazione.

Il Codice Etico è stato approvato dall'Organo Amministrativo della Società.

3. - Destinatari

I principi espressi nel presente Codice Etico, unitamente a quelli previsti dal Codice Etico e dal Codice di Comportamento adottato dal Gruppo Generali S.p.A., rappresentano la base valoriale comune e presupposto essenziale, non derogabile, che deve guidare i comportamenti di tutti i Destinatari nella conduzione degli affari e nella gestione delle attività aziendali.

Il Codice Etico è da intendersi vincolante per l'Organo Amministrativo, i dipendenti, i subagenti, i produttori nonché per i consulenti esterni e i collaboratori legati alla Società da rapporti contrattuali a qualsiasi titolo, anche occasionali e/o soltanto temporanei.

La conoscenza e l'adeguamento ai principi del presente Codice rappresentano un requisito indispensabile ai fini dell'instaurazione e del mantenimento di rapporti con collaboratori e terzi.

La Società si impegna a promuovere la diffusione, la conoscenza e la condivisione dei principi del presente Codice Etico, per tutti coloro che operano nella Società e per gli altri *stakeholder*, affinché tali principi costituiscano il pilastro di una solida cultura d'impresa comune.

4. - Comunicazione e diffusione

Il Codice Etico è portato a conoscenza dei Destinatari mediante apposite attività di comunicazione/informazione.

In particolare, sono predisposti appositi programmi di formazione introduttiva e di aggiornamento. La Società si impegna altresì a:

- consegnare copia del Codice Etico ai Destinatari;
- affiggere il Codice Etico in luogo facilmente accessibile (ad esempio, bacheca aziendale);
- inserire, nei contratti conclusi con i terzi, una nota informativa in ordine alla adozione del Codice Etico;
- pubblicare il Codice Etico sul proprio sito internet aziendale.

5. - Norme di condotta

5.1. - Criteri di condotta nelle relazioni con il personale

Il capitale umano costituisce un fattore fondamentale per lo sviluppo e la crescita della Società.

La politica di gestione del personale è, da sempre, contraddistinta da una grande attenzione verso tutte le azioni che possono contribuire a creare, per i propri dipendenti e/o collaboratori, delle condizioni migliori di vita personale e familiare, al di là della retribuzione economica.

Il benessere dei soggetti che operano all'interno della Agenzia si realizza anche attraverso la costante attenzione all'ambiente, alla organizzazione del lavoro, alla mutua solidarietà e ad ogni iniziativa capace di creare coesione e identità aziendale.

5.1.1. - Selezione e gestione dei rapporti con il personale

I criteri di selezione del personale da inserire nell'organico societario riflettono esclusivamente la rispondenza dei profili dei candidati rispetto a quelli ricercati dalla Società.

La Società consente a tutti i potenziali candidati pari opportunità di ingresso ed effettua le proprie selezioni soltanto sulla base di principi oggettivi e meritocratici, senza discriminazioni di sesso, razza, età, stato di salute, orientamento sessuale, opinioni politiche, sindacali e religiose.

La Società adotta tutte le misure possibili, limitatamente alle informazioni in suo possesso o ragionevolmente ottenibili, per evitare che nel processo di selezione si sviluppino pratiche di clientelismo e impiega tutti i mezzi necessari affinché i processi decisionali relativi ad avanzamenti di carriera rispondano esclusivamente a criteri di merito.

La Agenzia ritiene di fondamentale importanza la formazione del personale, quale elemento strategico per lo sviluppo dell'organizzazione e la crescita dei propri dipendenti e/o collaboratori.

Per tali ragioni, vengono fornite al personale di nuova assunzione precise informazioni sulle mansioni da svolgere, sulle procedure aziendali e sulle norme del Codice Etico.

La Agenzia si impegna a valorizzare le professionalità e la crescita del proprio personale attraverso specifiche sedute formative.

Ogni responsabile non deve abusare della propria posizione per richiedere prestazioni non riconducibili allo svolgimento delle normali attività lavorative e non può pretendere dai propri subordinati favori personali o attività in aperta violazione del presente Codice e delle norme vigenti.

La Società non ammette alcuna forma di emarginazione e/o persecuzione, sfruttamento o molestia di qualsiasi natura, per motivi di lavoro o personali, da parte di chiunque, a prescindere dal livello di responsabilità o dalla funzione ricoperta, svolga la sua attività nell'ambito dell'Agenzia; si impegna, inoltre, a tutelare i propri dipendenti e/o collaboratori da atti lesivi della dignità della persona, da atti di violenza psicologica, da molestie di qualsiasi natura e da ogni comportamento discriminatorio.

In ogni caso, differenze di trattamento che siano giustificate o giustificabili sulla base di criteri oggettivi (esperienza, competenza, impegno, ecc.) non sono da considerare discriminazioni.

L'Agenzia vieta, infine, qualsiasi comportamento lesivo della persona, della libertà o della dignità umana.

Sul punto, si richiamano i contenuti delle Disposizioni Attuative "Promozione delle diversità e dell'inclusione" di Generali.

5.1.2. - Salute e sicurezza

Salute e sicurezza dei lavoratori, sia dipendenti che collaboratori, presso la sede della Società o dei clienti, hanno la massima priorità per la Agenzia.

L'Agenzia si impegna a diffondere e consolidare una cultura della salute e sicurezza sul lavoro, sviluppando la consapevolezza dei lavoratori circa i rischi correlati alle attività svolte e promuovendo comportamenti responsabili da parte di tutti i dipendenti e collaboratori.

Per questo motivo, la Agenzia dedica particolare attenzione alla valutazione ed alla gestione dei rischi al fine di massimizzare la prevenzione e la protezione sui luoghi di lavoro.

5.1.3. - Doveri dei dipendenti e dei collaboratori

Il dipendente e i collaboratori devono osservare un comportamento improntato ai principi di buona fede, diligenza, lealtà; devono attenersi alle prescrizioni inserite nel contratto e/o nella lettera di nomina sottoscritti, al presente Codice Etico e ai protocolli aziendali, oltre che alle disposizioni normative e sono tenuti a svolgere le rispettive mansioni con impegno, onestà e spirito di collaborazione.

Ai dipendenti e/o collaboratori è fatto obbligo di intrattenere eventuali rapporti con i soggetti pubblici nel rispetto delle disposizioni di legge e regolamentari e mediante modalità che ne garantiscano la trasparenza e la totale collaborazione.

Tutti i dipendenti e/o collaboratori devono collaborare, per quanto di loro competenza, al mantenimento di un ambiente di lavoro sano, efficiente e sicuro, osservando le norme in tema di sicurezza sui luoghi di lavoro così come disciplinate dal D. Lgs. 81/2008; inoltre, non devono porre in essere condotte che possono produrre rischi di incolumità per i colleghi, nonché per i clienti, altri collaboratori della Società e *partner*. Devono utilizzare con cura e diligenza i beni aziendali, i locali messi a disposizione dalla Azienda, nonché gli strumenti di lavoro.

5.1.4. - Prevenzione dei conflitti di interesse

Il personale è tenuto ad agire sempre nell'interesse della Società ed evitare situazioni in cui propri interessi personali possano entrarne in conflitto.

Per "conflitto di interessi" si intende sia il caso in cui un individuo persegua un interesse diverso dalla *mission* aziendale, anche avvantaggiandosi in proprio o per altre persone di opportunità economiche in ragione del ruolo aziendale ricoperto, sia il caso in cui i rappresentanti dei clienti o dei fornitori agiscano in contrasto con i doveri fiduciari legati alla loro posizione, nei loro rapporti con la Agenzia.

Qualora il dipendente e/o collaboratore si trovi in una situazione di conflitto di interessi, anche soltanto potenziale, deve immediatamente darne comunicazione al proprio superiore gerarchico ovvero all'Organo amministrativo e deve in ogni caso astenersi dallo svolgere, in assenza di specifica autorizzazione, qualsiasi tipo di attività decisionale riferibile ai soggetti di cui è portatore di interessi diretti o indiretti.

Si fa espresso rinvio, sul punto, a quanto contenuto nelle Disposizioni Attuative sul "conflitto di interessi" di Generali

5.2. Criteri di condotta con i clienti

I contratti con i clienti devono essere conformi alle norme di legge vigenti nonché alle prescrizioni di Generali Italia S.p.a. e devono essere definiti in maniera chiara e completa.

I dipendenti e/o collaboratori, nei rapporti con i clienti, rappresentano l'Agenzia e devono tenere un comportamento improntato a cortesia, professionalità, correttezza, trasparenza e disponibilità, salvaguardando l'immagine aziendale.

La Società si impegna ad erogare servizi ad alto contenuto qualitativo ed è fortemente orientata alla soddisfazione del cliente, alla corretta interpretazione delle relative esigenze e alla ricerca della soluzione ottimale che consenta il raggiungimento degli obiettivi quantitativi e qualitativi richiesti.

È garantito il trattamento dei dati personali dei clienti nel rispetto della normativa vigente in merito e del presente Codice Etico. La Società assicura, inoltre, che i dati e le informazioni siano registrati ed elaborati in modo completo, tempestivo e nel rispetto della dovuta riservatezza.

5.3. Criteri di condotta con i fornitori

I processi di approvvigionamento sono improntati alla massima trasparenza, alla efficiente allocazione delle risorse aziendali, nonché alla verifica preventiva e tracciabile che i fornitori siano in possesso dei requisiti oggettivi e soggettivi di natura professionale, reputazionale e legale di abilitazione per l'esercizio dell'attività/professione esercitata.

Nei rapporti di appalto, di approvvigionamento e, in genere, di fornitura di beni e/o servizi e di collaborazione/consulenza esterna , è fatto obbligo al personale addetto, in virtù di apposite clausole contrattuali, di aderire formalmente ai principi contenuti nel presente Codice Etico e nella normativa vigente in materia.

5.4. Criteri di condotta con la Pubblica Amministrazione

I rapporti con la pubblica amministrazione, nonché con le istituzioni pubbliche centrali o periferiche, sono riservate alle funzioni aziendali preposte e autorizzate.

La Società opera nei rapporti con la pubblica amministrazione nel rispetto dei principi e dei criteri di buon andamento ed imparzialità che devono guidarne l'azione.

Pratiche di corruzione, favori illegittimi, comportamenti collusivi sono ritenuti inaccettabili e, pertanto, proibiti e sanzionati. Al pari, sono vietate sollecitazioni attraverso terzi per l'ottenimento di vantaggi personali e aziendali di carattere sia economico che professionale.

Qualunque atto che contrasti con la correttezza nei rapporti con la pubblica amministrazione va prontamente segnalato alle funzioni interne competenti, con le modalità indicate dalla Società stessa.

Si vedano, sul punto, le Disposizioni Attuative "Lotta alla corruzione" di Generali Italia S.p.a..

5.5. Rapporti con la stampa e gli organi di comunicazione

L'Agenzia ritiene che la comunicazione verso l'esterno debba essere sempre veritiera, trasparente e tale da preservare la reputazione della Agenzia attraverso la corretta diffusione dei programmi realizzati e delle *performance* ottenute.

I rapporti con i mezzi di comunicazione sono riservati esclusivamente alla funzione allo scopo preposta.

Ogni dipendente, contattato da un rappresentante dei mezzi di comunicazione, deve astenersi dal fornire qualsiasi tipo di dato ed informare tempestivamente la Funzione allo scopo preposta.

Gli amministratori ed i dipendenti della Società non possono in nessun caso offrire pagamenti, regali ed opportunità d'affari per influenzare l'etica professionale e l'imparzialità degli operatori del mondo dell'informazione e della comunicazione.

6. Gestione delle informazioni

6.1. Riservatezza

La Società assicura e garantisce la riservatezza delle informazioni in proprio possesso.

È tutelata, fatti salvi gli obblighi di legge e contrattuali, la riservatezza delle informazioni relative al proprio personale e ai propri *stakeholders* e garantisce la riservatezza della corrispondenza e della documentazione personale dei propri dipendenti in tutte le possibili forme.

Ciascun dipendente deve conoscere e attuare quanto previsto dalle politiche aziendali in tema di sicurezza delle informazioni per garantirne l'integrità, la riservatezza e la disponibilità.

6.2. Privacy

È tutelata la *privacy* di ciascun dipendente, in conformità alla normativa applicabile, e la Società adotta standard che prevedono il divieto, fatte salve le eccezioni previste dalla legge, di comunicare e diffondere i dati personali senza previo consenso dell'interessato.

È esclusa qualsiasi forma d'indagine sulle idee e, in generale, sulla vita privata di ciascuno.

I dati personali riguardanti soggetti terzi, siano essi clienti, dipendenti, fornitori o altri, sono trattati nel rispetto della normativa vigente in materia, con modalità idonee ad assicurarne la massima trasparenza ai diretti interessati e l'inaccessibilità a terzi, se non per giustificati ed esclusivi motivi professionali e di legge.

La Società vigila affinché il trattamento dei dati personali avvenga in modo lecito e secondo correttezza e che gli stessi siano raccolti e registrati solo per scopi determinati, espliciti e legittimi e conservati per un periodo di tempo non superiore a quello necessario agli scopi della raccolta.

L'Agenzia si impegna, inoltre, ad adottare idonee e preventive misure di sicurezza per tutte le banche-dati nelle quali sono raccolti e custoditi dati personali, al fine di evitare rischi di distruzione e perdite oppure di accessi non autorizzati o di trattamenti non consentiti.

7. Comportamento negli affari

7.1. Diligenza e correttezza nell'esecuzione dei compiti e dei contratti

I doveri derivanti da tutti i contratti e gli incarichi di lavoro devono essere adempiuti con la diligenza del buon padre di famiglia e secondo quanto stabilito dalle parti.

L'instaurazione e la gestione dei rapporti con controparti esterne devono avvenire nel rispetto delle disposizioni di legge e regolamentari.

La Agenzia ritiene importante evitare che, nei rapporti in essere, chiunque operi in nome e per conto della stessa possa trarre profitto da lacune contrattuali o da eventi imprevisti per negoziare il contratto al solo scopo di sfruttare la posizione di dipendenza o di debolezza nelle quali la controparte si sia venuta a trovare.

7.2. Concorrenza leale

La Società riconosce il valore della concorrenza leale come strumento di efficiente allocazione delle risorse della collettività e si impegna a non tenere comportamenti collusivi, profittatori e tali da abusare di eventuali posizioni dominanti.

I dipendenti e/o collaboratori sono tenuti a rispettare tutte le leggi vigenti a tutela del commercio equo e ad astenersi da azioni che potrebbero comportare pratiche commerciali sleali.

7.3. Prevenzione della corruzione

La Società non tollera alcuna forma di corruzione, attiva o passiva, ivi compresa la corruzione tra privati, il traffico di influenze illecite e la concessione di vantaggi/pagamenti di incentivazione; in particolare, a titolo esemplificativo e non esaustivo, vieta qualunque azione nei confronti o da parte di terzi tesa a promuovere o favorire i propri interessi o a trarne vantaggio; inoltre, non ammette la dazione di denaro o altre utilità o vantaggio a favore di singole persone facenti parte o riconducibili alla struttura aziendale di terzi per ottenere commesse o altro vantaggio.

Infine, condanna l'utilizzo improprio dello strumento delle liberalità, donazioni e sponsorizzazioni finalizzate alla creazione di disponibilità finanziarie destinate alla commissione di reati di corruzione.

La Società si impegna a mettere in atto tutte le misure necessarie utili a prevenire e ad evitare fenomeni di corruzione; a tal fine, ogni azione, operazione, transazione, nonché ogni registrazione contabile, deve essere gestita con la massima correttezza, completezza, trasparenza e veridicità.

Si vedano, sul punto, le Disposizioni Attuative "Lotta alla corruzione" di Generali.

7.4. Lotta al riciclaggio e al finanziamento del terrorismo

L'Agenzia è attenta alla lotta internazionale contro il riciclaggio di denaro e il finanziamento del terrorismo. Quale Agente di Generali, l'Agenzia si conforma a tutta la regolamentazione interna in tema antiriciclaggio e alla normativa secondaria emanata da IVASS.

8. Comportamento nell'ambito della Società

8.1. Correttezza contabile

La Società garantisce la completezza, l'accuratezza e l'attendibilità delle informazioni utili per l'elaborazione dell'informativa societaria, anche nel rispetto degli standard relativi alla redazione e tenuta dei documenti contabili societari ed alla comunicazione all'esterno dell'informativa societaria.

La Società rispetta le leggi e le regolamentazioni in materia di redazione dei bilanci annuali e infrannuali nonché relativamente ad ogni tipo di documentazione assimilabile richiesta dalla normativa vigente.

Il personale è tenuto a garantire la massima collaborazione affinché i fatti di gestione siano rappresentati correttamente e tempestivamente all'interno del sistema di rilevazione contabile aziendale.

Qualsiasi tipo di comunicazione falsa o ingannevole all'interno della Società o ad altre organizzazioni o persone è severamente vietato.

Per ciascuna transazione dovrà essere conservata adeguata documentazione di supporto, che garantisca l'individuazione della appropriata autorizzazione e della motivazione economica sottostante la transazione. La documentazione di supporto dovrà essere agevolmente reperibile ed archiviata secondo opportuni criteri che ne consentano una facile consultazione sia dagli organi interni preposti al controllo che da parte di enti ed istituzioni esterne autorizzati.

8.2. Regali e omaggi

La Società non autorizza alcuna forma di omaggio o regalia finalizzata ad acquisire trattamenti di favore collegabili all'attività svolta, se non quelli, comunque di modico valore, rientranti nella normale prassi commerciale o in una forma di cortesia. In ogni caso, le iniziative necessitano dell'approvazione da parte di un predefinito livello gerarchico.

In particolare, è vietata ogni tipo di offerta a funzionari pubblici italiani ed esteri, o loro familiari, che potrebbe influenzare la loro indipendenza di giudizio o indurli ad assicurare un qualsiasi vantaggio economico diretto o indiretto alla Società.

La norma non è derogabile nemmeno in quei paesi in cui sia consuetudine offrire doni a *partner* commerciali e funzionari pubblici.

In caso di regalie ricevute eccedenti gli usi, le consuetudini ed i codici etici delle organizzazioni offerenti, amministratori e dipendenti devono rifiutare con cortesia, ma allo stesso tempo con fermezza e comunicare l'evento al responsabile che provvederà a stimare la congruità del valore degli omaggi.

Si vedano, sul punto, le Disposizioni Attuative "Lotta alla corruzione" di Generali.

8.3. Tutela dei beni aziendali e sicurezza informatica

Ogni dipendente, in conformità alle regole aziendali, è tenuto ad utilizzare i beni aziendali nella sua disponibilità in base ai principi di massima diligenza, buona fede e correttezza e rispettandone le finalità per cui gli sono stati concessi.

Con riferimento all'utilizzo degli strumenti informatici e, in particolare, dei servizi di posta elettronica ed accesso ad internet, il comportamento deve essere ispirato a canoni di correttezza ed essere conforme alla regolamentazione di legge e alla specifica normativa aziendale sul tema. I dipendenti operano sui computer aziendali esclusivamente per lo svolgimento delle attività lavorative autorizzate dalle società, salve specifiche autorizzazioni rilasciate dal responsabile aziendale di riferimento.

In particolare, al suddetto personale è severamente vietato accedere, copiare, modificare o divulgare *software* del cliente e/o informazioni inerenti alla sua organizzazione, o intercettare comunicazioni al di fuori delle autorizzazioni/abilitazioni concesse dal cliente e, in ogni caso, per scopi che esulano dalle finalità proprie della prestazione erogata dalla Società. È tassativamente vietato, inoltre, creare documenti informatici falsi e danneggiare dati ed informazioni aziendali o sistemi informatici e telematici.

Per il corretto utilizzo degli strumenti informatici e delle applicazioni in essi contenute il dipendente è tenuto ad osservare tutte le misure necessarie per preservarne la funzionalità.

9. Violazioni del Codice Etico: modalità di Segnalazione e sistema sanzionatorio

La violazione delle previsioni contenute nel presente Codice Etico costituisce illecito disciplinare, perseguibile ai sensi della legge e/o del CCNL applicato, e, per quanto riguarda i collaboratori esterni, contrattuale.

Ogni violazione dei principi e delle disposizioni contenute nel presente Codice dovrà essere senza indugio segnalata, da parte dei Destinatari dello stesso, all'Organismo di Vigilanza della Società.

A tale scopo, risultano a disposizione del segnalante i seguenti canali:

- a mezzo del servizio postale recapitata presso la sede della Società, o tramite corrispondenza interna: in tal caso, per poter usufruire della garanzia della riservatezza, è necessario che la segnalazione venga inserita in una busta chiusa che rechi all'esterno l'indicazione "ODV - riservata/personale";
- via e-mail al seguente indirizzo odv231veschini@gmail.com

L'OdV, verificata la Segnalazione, sottopone gli esiti all'Organo Amministrativo.

Le Segnalazioni di condotte illecite e di violazioni del Modello, di cui i Destinatari siano venuti a conoscenza in ragione delle funzioni svolte, c.d. Segnalazioni Whistleblowing, invece, sono inviate al Gestore della Segnalazione attraverso l'utilizzo della piattaforma informatica appositamente dedicata (Portale Segnalazioni – Whistleblowing).

Le sanzioni sono previste dal sistema disciplinare adottato dalla Società con il Modello Organizzativo di Gestione e Controllo *ex* D. Lgs. n. 231/2001 e non potranno in alcun modo derogare alle previsioni contenute nello Statuto dei lavoratori e nel CCNL applicato.

È comunque assicurata tutela al soggetto segnalante da ogni eventuale ritorsione e non consente l'adozione di alcun tipo di conseguenza disciplinare e/o sanzionatoria per Segnalazioni che siano state effettuate in buona fede.

Qualora le Segnalazioni pervenute richiedessero, nel rispetto delle normative vigenti, un trattamento confidenziale, verrà protetta tale confidenzialità, ferme restando le disposizioni di legge, il CCNL applicato, i regolamenti o i procedimenti applicabili al caso di specie.

Modello di organizzazione, gestione e controllo

ex D. Lgs. n. 231, 8 giugno 2001

PARTE SPECIALE "E"

I REATI INFORMATICI

Sommario

1. I Reati informatici: profili generali

Il presente Modello di Organizzazione e Gestione si applica, per l'effetto della previsione di cui all'art. 24 *bis* D. lgs. 231/2001, anche alle attività sensibili riconducibili al settore cyber security.

In un momento storico quale quello attuale, caratterizzato da un inevitabile e crescente impiego delle risorse informatiche, non ci si può in alcun modo sottrarre dal disciplinare tale ambito in maniera quanto più compiuta ed esaustiva, per poter mitigare i rischi connessi al perfezionarsi di reati, commessi anche attraverso condotte elusive e fraudolente, difficili da contrastare.

Pertanto, in un'ottica di omogeneità di azione e cooperazione a livello internazionale, il nostro ordinamento ha dapprima ratificato la "Convenzione sulla criminalità informatica", siglata dal Consiglio di Europa nel 2001, e sempre con l. n.48/2018 con modifica del D.lgs. 231/2001 ha previsto l'introduzione del già menzionato art. 24 *bis*, "Delitti informatici e trattamento illecito dei dati".

Da ultimo, la Legge 90/2024 "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e dei reati informatici" (cd. "legge sulla cybersicurezza") ha apportato modifiche sostanziali e procedurali ai reati informatici, inasprendo i trattamenti sanzionatori, prevedendo un diverso regime di applicazione delle circostanze, ampliando i confini del dolo specifico.

In particolare, La Legge 90/2024 ha abrogato l'articolo 615 - *quinquies c.p.*, introdotto gli articoli 635 - *quater*.1 c.p. e 629 c. 3 c.p. e modificato gli artt. 615 – *ter*, 615 – *quater*, 617 -*quater*, 617- *quinquies*, 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies* c.p.

Ancora, la "legge sulla cybersicurezza" ha apportato le seguenti modifiche all'art. 24 *bis* D.lgs. 231/2001:

- con modifica del comma 1 ha previsto l'applicazione all'ente della sanzione pecuniaria da duecento a settecento quote in relazione alla commissione dei delitti ivi menzionati;
- con introduzione del comma 1 *bis* ha disposto l'applicazione all'ente della sanzione pecuniaria da trecento a ottocento quote per la commissione del delitto di cui all'art. 629 c.3 c.p.;
- con modifica del comma 2 ha previsto la sanzione pecuniaria fino a quattrocento quote per i delitti di cui all'art. 615 *quater* e 635 *quater* 1;
- con modifica del comma 4 ha disposto l'applicazione delle sanzioni interdittive ex art. 9 c.2 D.lgs. 231/2001 nell'ipotesi di condanna per il delitto di cui al comma 1 *bis*.

La normativa posta a presidio della sicurezza informatica tutela il bene "domicilio informatico", da intendersi sia come contenitore dei dati informatici personali sia come un'espansione ideale dell'area di pertinenza del soggetto interessato (il legislatore riconosce lo *jus excludendi* del titolare che caratterizza il domicilio fisico) all'interno del quale il titolare ha diritto di esplicare liberamente qualsiasi attività.

In ragione di un bene giuridico siffatto, i reati informatici vengono generalmente ricompresi nella categoria relativa ai delitti contro la persona o il patrimonio, ad eccezione della fattispecie di cui all'art. 491-*bis* c.p., la quale mira a tutelare (oltre il complesso dei dati afferente ad un determinato domicilio informatico) anche la genuinità del valore probatorio degli atti e dei dati contenuti in detto sistema.

Trattasi di delitti a natura dolosa, quindi sussistono necessariamente in capo all'agente i due requisiti cardine: consapevolezza del reato che si vuole commettere e volontà di realizzarlo (intesa come proposito di introdursi in

un sistema precluso all'altrui accesso e/o accompagnato dall'intento di alterarne, distruggerne o diffonderne illegittimamente il contenuto).

Oggetto della presente Parte Speciale sono quelle fattispecie di reato poste a tutela del c.d. "domicilio informatico", inteso quale luogo contenente dati appartenenti alla sfera individuale, nei confronti del quale è preclusa l'indebita ingerenza altrui.

Il domicilio informatico viene concepito come una espansione ideale dell'area di pertinenza del soggetto interessato (il legislatore riconosce lo *jus excludendi* del titolare che caratterizza il domicilio fisico) nel quale il titolare ha diritto di esplicare liberamente qualsiasi attività lecita all'interno del luogo informatico.

In ragione di un bene giuridico siffatto, i reati informatici vengono generalmente ricompresi nella categoria relativa ai delitti contro la persona o il patrimonio, ad eccezione della fattispecie di cui all'art. 491-*bis* c.p., la quale mira a tutelare (oltre il complesso dei dati afferente ad un determinato domicilio informatico) anche la genuinità del valore probatorio degli atti e dei dati contenuti in detto sistema.

Trattasi di delitti a natura dolosa, quindi sussistono necessariamente in capo all'agente i due requisiti cardine: consapevolezza del reato che si vuole commettere e volontà di realizzarlo (intesa come proposito di introdursi in un sistema precluso all'altrui accesso e/o accompagnato dall'intento di alterarne, distruggerne o diffonderne illegittimamente il contenuto).

2. Reati di cui all'art. 24-*bis* del D. Lgs. n. 231/2001

2.1. Documenti informatici (art. 491-*bis* c.p.)

La norma - contenuta nel Libro II, Titolo VII, Capo III del Codice Penale che contempla i delitti contro la fede pubblica e si riferisce ai c.d. reati di falso, nella forma materiale[1] o ideologica[2] (artt. 476 e ss. c.p.) - stabilisce che *"se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici"*.

Il legislatore ha previsto tale ipotesi di reato per garantire il carattere probatorio di alcuni atti, quali quelli a c.d. fede privilegiata di cui agli artt. 2699 ss. c.c., nonché quello di qualsiasi documento cui l'ordinamento attribuisce un valore probante meritevole di tutela in virtù del contenuto dello stesso.

Ciò premesso, la fattispecie di cui all'art. 491-*bis* c.p. estende la punibilità prevista per i reati c.d. di falso anche quando, oggetto della condotta alternativa materiale o ideologica, siano i documenti informatici di appartenenza pubblica o privata.

2.2. Accesso abusivo ad un sistema informatico (art. 615-*ter* c.p.)

La norma punisce *"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.*

La pena è della reclusione da due a dieci anni:

1) *se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;*
2) *se il colpevole per commettere il fatto usa minaccia o violenza sulle cose o alle persone, ovvero se è palesemente armato;*
3) *se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare dei dati, delle informazioni o dei programmi in esso contenuti.*

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da tre a dieci anni e da quattro a dodici anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio."

---

[1] Per "falsità materiale" (artt. 476 e 482 c.p.) deve intendersi quella condotta che alteri l'atto in un momento successivo alla sua formazione (ad. esempio: le modifiche, le aggiunte al documento oppure quando vi sia difformità tra l'autore apparente e quello reale).

[2] Per "falsità ideologica" (artt. 479 e 483 c.p.) deve intendersi quella condotta contraffattiva mediante l'apposizione di dichiarazioni o attestazioni non veritiere all'interno dell'atto.

È un reato di pericolo concreto (richiede l'accertamento giudiziale dell'effettiva potenzialità lesiva del materiale istallato) a consumazione anticipata, pertanto, si perfeziona nel momento in cui l'impianto illecito viene predisposto o installato sul sistema preso di mira dall'agente.

2.6. Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* c.p.)

"Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da due a sei anni.

La pena è della reclusione da tre a otto anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato".

Il bene giuridico al quale la norma intende apprestare tutela è l'inviolabilità del possesso e della disponibilità dell'oggetto materiale della condotta ovvero l'integrità dei contenuti e dei *software*.

La condotta idonea a integrare il delitto in esame è a forma libera, nel senso che può consistere in qualsiasi comportamento che alteri un sistema informatico, ovvero ne modifichi lo stato originario o renda inservibile l'elaboratore, a nulla rilevando la possibilità che lo stesso possa essere ripristinato.

2.7. Danneggiamento di informazioni, dati o programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635-*ter* c.p.)

Salvo che il fatto costituisca più grave reato, è punito con la reclusione da due a sei anni *"chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico.*

La pena è della reclusione da tre a otto anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al legittimo titolare dei dati o dei programmi informatici.

La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3"

La struttura del delitto in oggetto si differenzia da quello di cui all'art. 635-*bis* c.p. esclusivamente per la circostanza che i sistemi informatici o telematici, presi di mira dall'agente e su cui si estende la condotta criminosa, sono

utilizzati o appartengono allo Stato o ad altro Ente Pubblico o comunque sono di pubblica utilità. La pena base è aumentata se si realizza il danno o uno degli eventi descritti nella fattispecie ed è altresì aggravata se il fatto è commesso con violenza o minaccia ovvero con abuso di qualità.

2.8. Danneggiamento di sistemi informatici o telematici (art. 635-*quater* c.p.)

La norma punisce, con la reclusione da due a sei anni, salvo che il fatto costituisca più grave reato, *"chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento [...]"*.

Al secondo comma prevede "La pena è della reclusione da tre a otto anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato.

La fattispecie di reato si configura come un delitto a forma vincolata, incentrato sulla determinazione dell'inservibilità del sistema ovvero su una grave compromissione del suo funzionamento.

Il delitto in esame è realizzabile attraverso un'ampia pluralità di condotte di danneggiamento con un rinvio espresso a quanto descritto dall'art. 635-*bis* nonché attraverso l'introduzione, la trasmissione di dati, informazioni o programmi, mediante programmi virus o dati maligni introdotti nella rete in grado di rendere totalmente o parzialmente inservibili i sistemi informatici e telematici altrui.

Ai fini della configurazione del delitto in esame, non sarà necessario che i dati aggrediti vengano totalmente distrutti, ma sarà sufficiente che ne venga alterata in maniera irreversibile l'ordinaria funzione e che la condotta posta in essere dall'agente renda irregolare e frammentario il funzionamento del sistema e dei servizi cui sono destinati.

2.9 Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (635 quater.1 c.p.)

La "legge sulla cybersicurezza" (l. 90/2024), in uno spirito di rafforzamento della normativa interna a presidio della sicurezza cibernetica, ha introdotto l'articolo 635 quater.1 c.p., a norma del quale "*Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici è punito con la reclusione fino a due anni e con la multa fino a euro 10.329.*

La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615 ter, secondo comma, numero 1).

La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma."

2.10. - Danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-*quinquies* c.p.)

"

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635 bis ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, compie atti diretti a distruggere, danneggiare o rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblico interesse ovvero ad ostacolarne gravemente il funzionamento è punito con la pena della reclusione da due a sei anni.

La pena è della reclusione da tre a otto anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita, anche abusivamente, la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa minaccia o violenza ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.

La pena è della reclusione da quattro a dodici anni quando taluna delle circostanze di cui ai numeri 1) e 2) del secondo comma concorre con taluna delle circostanze di cui al numero 3. La norma, inserita dalla L. 48//2008 e poi sostituita con L. 90/2024, tutela il patrimonio informatico sanzionando anche le condotte propedeutiche al danneggiamento di un sistema informatico di pubblica utilità. La pena è aumentata in caso di realizzazione dell'evento dannoso o di altra ipotesi delittuosa; è prevista un'aggravante qualora il fatto sia commesso da un soggetto che abusi di proprie qualità.

2.11. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* c.p.)

"Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro".

Tale reato si configura quando un soggetto che presta servizi di certificazione di firma elettronica, al fine di procurare a sé o ad altri un ingiusto profitto, ovvero arrecare ad altri danno, violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

Come risulta evidente si tratta di reato c.d. proprio, realizzabile solo da soggetti che possiedano la qualifica richiesta dalla norma.

2.12. Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 105/2019)

"Chiunque, allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b), o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c), fornisce informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto, è punito con la reclusione da uno a tre anni".

2.13. Estorsione (629 c.3 c.p.)

La l.90/2024 ha previsto la modifica dell'art. 629 c.2 c.p. e l'introduzione del comma 3, a norma del quale *"Chiunque, mediante le condotte di cui agli articoli 615 ter, 617 quater, 617 sexies, 635 bis, 635 quater e 635 quinquies ovvero con la minaccia di compierle, costringe taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei a dodici anni e con la multa da euro 5.000 a euro 10.000. La pena è della reclusione da otto a ventidue anni e della multa da euro 6.000 a euro 18.000, se concorre taluna delle circostanze indicate nel terzo comma dell'articolo 628 nonché nel caso in cui il fatto sia commesso nei confronti di persona incapace per età o per infermità."*

2.14 Trattamento sanzionatorio per le fattispecie di cui all'art. 24-*bis* del Decreto

In relazione alla commissione dei delitti di cui agli articoli 615-*ter*, 617-*quater*, 617-*quinquies*, 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies* del Codice Penale, si applica all'Ente la sanzione pecuniaria da duecento a settecento quote. In relazione alla commissione del delitto di cui all'articolo 629, terzo comma, del codice penale, si applica all'ente la sanzione pecuniaria da trecento a ottocento quote.

In relazione alla commissione dei delitti di cui agli articoli 615-*quater* e 635-*quater* del Codice Penale, si applica all'Ente la sanzione pecuniaria sino a quattrocento quote.

In relazione alla commissione dei delitti di cui agli articoli 491-*bis* e 640-*quinquies* del Codice Penale, salvo quanto previsto dall'articolo 24 del presente Decreto per i casi di frode informatica in danno dello Stato o di altro Ente Pubblico, si applica all'Ente la sanzione pecuniaria sino a quattrocento quote.

Nei casi di condanna per uno dei delitti indicati al comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati al comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati al comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

3. Aree a rischio

Tenuto conto dell'attività principalmente svolta dall'Agenzia, sono state individuate le seguenti aree a rischio:

- Uso dei sistemi informatici aziendali;
- Trattamento degli incidenti e dei problemi relativi alla sicurezza informatica;
- Misure di sicurezza per il trattamento informatico dei dati e il corretto utilizzo delle risorse informatiche onde evitarne un uso improprio;
- Gestione del sito internet aziendale;
- Utilizzo di *software* e banche dati;
- Pubblicizzazione dei prodotti assicurativi

Le aree indicate assumono rilevanza anche nell'ipotesi in cui le attività sopra elencate siano eseguite, in tutto o in parte, da persone fisiche o giuridiche in nome e per conto della Agenzia, in virtù di apposite deleghe o per la sottoscrizione di specifici rapporti contrattuali, dei quali deve essere tempestivamente informato l'OdV.

4. Principi generali di comportamento e modalità di attuazione

Scopo della presente Parte Speciale è quello di fornire adeguati sistemi comportamentali da adottare per scongiurare la concretizzazione del rischio di commissione dei reati elencati, dai quali deriverebbe l'attivazione del Sistema Sanzionatorio previsto dal Decreto ove venisse riscontrata la responsabilità dell'Ente.

Tali regole di condotta si applicano a tutti i Destinatari del Modello e, in particolare, a tutti coloro che svolgono le proprie mansioni nelle aree di rischio segnalate nel paragrafo precedente, inclusi i soggetti esterni all'Agenzia.

La diffusione e l'attuazione di detti sistemi sono rimessi al Titolare dell'Agenzia, in collaborazione con l'OdV.

I Destinatari sono tenuti a conoscere e rispettare tutte le regole di cui alla presente Parte Speciale, nonché:

- il Codice Etico;
- il Sistema Disciplinare;
- Regolamento sull'utilizzo dei sistemi informatici
- le procedure interne dell'Agenzia e le Policy di Generali Italia S.p.A., che l'Agenzia è tenuta ad osservare, in particolare: CR.GI 18.2019 IDD del 25.02.2019 "Novità del rilascio sui sistemi del 25 febbraio"; NOL.GI 24.2019 del 15.04.2019 "Raccomandazioni sull'utilizzo dei profili personali operanti nelle Agenzie, Subagenzie e Filiali di Direzione"; NOL. GI. 22.2025 del 9.04.2025: "Linee guida in materia di presenza digitale delle Agenzia, con focus su gestione dei siti web e dei profili social";

Infine, il Titolare dell'Agenzia potrà prevedere ulteriori misure a maggiore tutela delle aree di rischio individuate, ad integrazione degli adempimenti di seguito indicati.

Si passa, quindi, ad indicare i presidi di controllo e i principi generali di comportamento inerenti alle aree sensibili indicate nel paragrafo precedente.

I seguenti principi di carattere generale si applicano ai Dipendenti e agli Organi Sociali della Agenzia.

È fatto divieto di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate;
- porre in essere comportamenti in violazione dei principi previsti nella presente Parte Speciale.

È, altresì, vietato:

- diffondere le *password* o altre credenziali per l'accesso ai sistemi informatici dell'Agenzia a chiunque - interno o esterno all'Agenzia - non sia autorizzato all'utilizzo di detti impianti;
- possedere o utilizzare *software* e/o *hardware* che potrebbero danneggiare o compromettere la sicurezza dei sistemi e dei dati in essi contenuti;
- accedere e/o intrattenersi all'interno del sistema per scopi diversi da quelli prettamente lavorativi e/o in violazione delle prescrizioni imposte dal titolare dell'impianto informatico;
- modificare i *software* e/o gli *hardware* delle postazioni di lavoro in violazione dei precetti aziendali, ovvero senza autorizzazione della Agenzia;

- sfruttare *password* e/o credenziali per manomettere le misure di sicurezza previste dal sistema per accaparrarsi dati o notizie riservate;
- alterare i dati pubblicati sul sito internet dell'Agenzia;
- inviare dal proprio sistema informatico dati falsificati nel loro contenuto o in qualunque modo alterati;
- esercitare attività di *spamming* o qualsiasi risposta alla medesima;
- diffondere, a seguito di accesso non autorizzato nel sistema informatico dell'Azienda, informazioni o dati per i quali è vietata la pubblicazione.

L'Agenzia, a ulteriore presidio delle aree a rischio sopra indicate **si impegna a**:

- prevedere misure di sicurezza per il trattamento informatico dei dati, nonché per il corretto utilizzo delle risorse informatiche in conformità alla normativa vigente;
- definire regole finalizzate a evitare che un uso improprio dei software possa causare illeciti o arrecare danni a terzi e/o ai soggetti pubblici; minacciare la sicurezza e la integrità delle informazioni e dei dati trasmessi a terzi e/o a soggetti pubblici.

In particolare, per quanto concerne **l'uso dei sistemi informatici aziendali**:

Nello svolgimento della sua attività di intermediazione assicurativa, l'Agente ed i suoi dipendenti e collaboratori sono obbligati ad utilizzare, per l'emissione dei contratti (sia in formato cartaceo che in formato digitale) e per la gestione degli stessi, la piattaforma informatica di Generali Italia spa.

L'utilizzo della piattaforma è riservato ad Agenti, dipendenti e collaboratori cui sono assegnate password specifiche di accesso.

I Dipendenti ed i Consulenti esterni devono:

i. utilizzare la *user* ID e la *password* individuale di autorizzazione all'accesso al sistema informatico o gli eventuali sistemi di identificazione e autenticazione alternativi, in modo personale, garantendone la segretezza;
ii. utilizzare personalmente le credenziali che consentono l'accesso alla rete intranet aziendale e ai relativi servizi, senza condividerle o cederle a terzi;
iii. operare sui computer aziendali esclusivamente per lo svolgimento di attività lavorative autorizzate dalla Impresa;
iv. utilizzare la navigazione internet e la posta elettronica per finalità legate ai propri compiti lavorativi;
v. non interferire intenzionalmente con le normali operazioni dalla rete, ad esempio con un continuo ed elevato volume di traffico che impedisca ad altri l'uso della rete;
vi. controllare i file allegati alla posta elettronica prima del loro utilizzo, al fine di prevenire lo scarico di *file* indesiderati e dannosi per la rete informatica;
vii. non utilizzare il servizio di posta elettronica per condurre attacchi a computer esterni alla rete o inficiare la corretta operatività di sistemi altrui o per diffondere *software* illegali;

viii. non utilizzare programmi non distribuiti e/o installati ufficialmente dalla Impresa;

ix. non detenere, all'interno delle strutture della Impresa e nelle relative risorse informatiche, materiale pornografico in qualsiasi forma e su qualunque supporto, a prescindere dai contenuti e dall'età delle persone coinvolte per la sua realizzazione;

x. non utilizzare anche occasionalmente la Impresa o una sua unità organizzativa allo scopo di consentire o agevolare la commissione dei reati di Razzismo e Xenofobia di cui all'art. 25-*terdecies* del Decreto con particolare riferimento agli strumenti di comunicazione informatica (*social network*) utilizzati dalla Impresa.

Deve essere previsto un sistema di controllo sull'accesso alle informazioni, al sistema informatico, alla rete, agli applicativi e alla relativa infrastruttura, che assicuri:

- l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e *password* od altro sistema di autenticazione sicura;
- la chiusura di sessioni inattive dopo un limitato periodo di tempo;
- la sospensione delle utenze in seguito ad un numero predefinito di tentativi di accesso fallito;
- i procedimenti di registrazione e deregistrazione delle utenze per accordare e revocare, in caso di cessazione o cambiamento del tipo di rapporto o dei compiti assegnati, l'accesso a tutti i sistemi e servizi informativi, anche di Terzi;
- l'adozione e l'attuazione di strumenti organizzativi e tecnologie che prevedano che la protezione del sistema informatico e telematico da *software* pericoloso (ad es. *worm* e virus) venga garantita attraverso l'utilizzo di antivirus. Qualsiasi modifica alle configurazioni di sicurezza perimetrale (ad es. apertura di porte verso l'esterno) è sottoposta ad adeguati controlli autorizzativi.

È fatto obbligo di:

- utilizzare gli strumenti informatici in conformità alle previsioni contenute nel Regolamento sull'utilizzo degli stessi adottato dall'Agenzia

In riferimento al **trattamento degli incidenti e dei problemi relativi alla sicurezza informatica** l'Agenzia prevede:

a) l'obbligo di comunicazione degli incidenti e problemi (relativamente a tutta la catena tecnologica);
b) la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva (relativamente a tutta la catena tecnologica);
c) la produzione e l'analisi di *report* e *trend* sugli incidenti e sui problemi e l'individuazione di azioni preventive (relativamente a tutta la catena tecnologica).

L' Agenzia, inoltre, attua **strumenti di *backup* dei dati, *recovery hardware* e *software* e *business continuity*.**

In relazione alla **gestione del sito internet aziendale,** si seguono i seguenti principi di comportamento.
L'apertura e l'utilizzo di siti internet da parte dell'Agente con la spendita del nome e del marchio della Compagnia deve avvenire nel rispetto delle disposizioni emanate da Generali Italia spa volte a presidiare esigenze di uniformità, riconducibilità alla Compagnia ed integrazione con i contenuti web della Compagnia stessa. Anche la partecipazione dell'Agente ai social network deve rispettare la Normativa Interna in materia tempo per tempo vigente.
È vietata la pubblicazione di materiale coperto da diritto d'autore senza pagamento dei relativi diritti e di materiale denigratorio nei confronti di competitor.
Per la gestione del sito e dei social network è delegata una risorsa interna che verifica il rispetto delle disposizioni impartite da Generali Italia spa.
Ogni pubblicazione viene preventivamente autorizzata dall'Agente Generale.

L'Agenzia si impegna a fare in modo che le attività e le modalità operative per la pubblicazione e/o l'aggiornamento dei contenuti del sito internet siano svolti in modo da scongiurare il rischio di realizzazione dei reati di Razzismo e Xenofobia di cui all'art. 25-*terdecies* del Decreto.

In relazione **all'utilizzo di *software* e banche dati,** è fatto divieto a tutti i Destinatari:

- di scaricare, senza espressa autorizzazione da parte della funzione competente, *software* gratuiti (*freeware* e *shareware*) prelevati da siti internet; di caricare o trasmettere in qualsiasi modo *software* e altro materiale in violazione delle leggi sul *copyright* o dei diritti riservati del legittimo proprietario;
- di utilizzare il servizio di posta elettronica per condurre attacchi a computer esterni alla rete o inficiare la corretta operatività di sistemi altrui o per diffondere *software* illegali;
- di utilizzare e/o installare *software* atti ad intercettare, falsificare o alterare il contenuto di documenti informatici;
- di modificare autonomamente la configurazione *hardware* e *software* della postazione di lavoro aggiungendo o rimuovendo componenti rispetto allo *standard* definito e fornito dall'Agenzia;
- disabilitare o inibire il corretto funzionamento dei *software* antivirus installati.

Al contempo, l'Agenzia:

- adotta misure specifiche che impediscano l'installazione e l'utilizzo di *software* non approvati dalla Agenzia, non correlati con l'attività professionale espletata per la stessa o per i quali non si possiede la necessaria licenza d'uso;
- richiama periodicamente in modo inequivocabile i propri Dipendenti e/o Consulenti, anche attraverso apposita attività di formazione/informazione, ad un corretto utilizzo degli strumenti informatici in proprio possesso;
- in generale, predispone e mantiene adeguate difese a protezione dei sistemi informatici aziendali.

Per quanto concerne la **pubblicizzazione dei prodotti assicurativi** l'Agenzia deve:

- rispettare le disposizioni dell'IVASS e di Generali Italia spa;
- adottare misure tali da consentire che l'utilizzo di materiale coperto da altrui diritto d'autore in occasione delle campagne pubblicitarie avvenga solamente in presenza di un diritto all'utilizzazione dello stesso;
- verificare l'eventuale utilizzo, in ogni campagna pubblicitaria di materiale non autorizzato.

L'Agenzia si impegna a promuovere tra tutti i Destinatari, la diffusione e la conoscenza delle regole adottate in relazione alla gestione e al funzionamento dei sistemi informatici.
Si impegna, altresì, a predisporre un apparato di controllo interno al fine di vigilare sulla sicurezza del sistema contro manomissioni o qualsivoglia comportamento lesivo di detti impianti e dei dati in esso contenuti.