



PL-08-14

Codice di condotta dei Fornitori del gruppo DGS

POLITICA

Emissione del documento

Redazione	Team Compliance
Verifica	Stefano Granati <i>Group Chief Procurement Officer</i>
Approvazione	Vincenzo Fiengo <i>Amministratore Delegato</i>

Revisione 02 approvata il 30 luglio 2025

Storia del documento

Rev.	Data	Motivo	Riferimento
01	07.09.2020	Nessuna (prima emissione)	Tutte
02	30.07.2025	Aggiornamento riferimenti normativi e procedurali	Tutte

Sommario

1	Introduzione e scopo del Codice di Condotta dei Fornitori	4
2	Principi etici fondamentali	4
3	Conformità alle normative vigenti	5
3.1	Gestione e responsabilità nell'utilizzo dei Subfornitori	6
3.2	Riservatezza e proprietà intellettuale	7
4	Prevenzione e gestione della corruzione	7
4.1	Divieto di attività non contrattualizzate	9
4.2	Governance delle segnalazioni	9
5	Prevenzione del conflitto di interessi	10
6	Parità di genere e inclusione	10
7	Impegno per la Responsabilità sociale	10
8	Ambiente, salute e sicurezza	11
9	Gestione responsabile delle tecnologie avanzate e dell'intelligenza artificiale	12
10	Privacy	12
10.1	Privacy e protezione dei dati personali dei Fornitori da parte del gruppo DGS	12
10.2	Trattamento dei dati personali come Responsabile o Sub-responsabile	13
11	Regole comportamentali e per l'accesso alla rete delle aziende del gruppo DGS	14
11.1	Uso delle risorse informatiche e dei servizi di rete	16
11.2	Condizioni di utilizzo della connessione remota	17
12	Monitoraggio, verifica della conformità e audit	18
12.1	Tipologie di verifiche	18
12.2	Ambiti oggetto di audit	18
12.3	Gestione delle non conformità	18
12.4	Collaborazione del Fornitore	18
12.5	Audit su Subfornitori	19
12.6	Impegno alla trasparenza	19
13	Sanzioni e conseguenze delle violazioni	19
	Dichiarazione di impegno e conformità	20

1 Introduzione e scopo del Codice di Condotta dei Fornitori

Il presente **Codice di Condotta dei Fornitori** rappresenta uno strumento per garantire la coerenza tra i valori aziendali del gruppo DGS e le attività svolte dai propri Fornitori. Questo codice non solo promuove la trasparenza e la fiducia reciproca, ma rafforza il rispetto di principi etici e standard internazionali che sono fondamentali per la sostenibilità e la responsabilità sociale dell'intera filiera produttiva.

Il codice si basa su un quadro normativo che comprende il Decreto Legislativo 231/2001, il quale disciplina la responsabilità amministrativa da reato degli Enti, e su standard certificativi come la ISO 37001 per la prevenzione della corruzione, la SA8000 per la responsabilità sociale, la UNI/PdR 125 sulla parità di genere, la ISO/IEC 27001 per la sicurezza delle informazioni, la ISO/IEC 27701 per la gestione delle informazioni personali e privacy, e la ISO 22301 per la continuità operativa. Questi riferimenti normativi richiedono che i Fornitori operino in conformità alle leggi applicabili e promuovano buone pratiche in termini di etica, sicurezza e sostenibilità.

Il gruppo DGS si impegna a garantire che i Fornitori non si trovino in condizione di forte dipendenza economica dalle società del gruppo DGS, che potrebbe mettere a rischio la loro attività e stabilità. Analogamente, le società del gruppo DGS non favoriscono il rapporto con Fornitori che hanno una rilevante dipendenza economica da uno specifico Cliente, condizione che potrebbe mettere a rischio le forniture con le società del gruppo DGS.

Inoltre, il codice si collega alle politiche di sostenibilità del gruppo DGS, le quali mirano a ridurre l'impatto ambientale, promuovere l'inclusione sociale e rispettare i diritti fondamentali dei lavoratori. Per questo motivo, tutti i Fornitori devono rispettare le linee guida stabilite nel codice e adottare comportamenti che riflettano tali valori, garantendo che l'intera catena di approvvigionamento operi in modo responsabile e sostenibile.

Un elemento fondamentale di questo sistema è rappresentato dall'Albo fornitori "**jAlbo**", il cui utilizzo è obbligatorio per accedere alle opportunità di collaborazione con il gruppo DGS. Il processo di iscrizione, gestito tramite il portale digitale dedicato, consente di verificare l'idoneità tecnica, economica e reputazionale del Fornitore, nonché di monitorare la conformità agli standard richiesti. Il mancato rispetto delle disposizioni del codice o delle normative di riferimento può determinare l'esclusione dall'Albo fornitori e la risoluzione dei contratti in essere.

Il gruppo DGS richiede inoltre la completa adesione ai principi derivanti dal **sistema di gestione per la qualità** definito dalla **ISO 9001**, che pone l'accento sulla **tracciabilità** dei processi, sul presidio delle **non conformità** e sull'adozione di procedure organizzate per il **miglioramento** delle attività produttive e operative. I fornitori sono tenuti a documentare in modo sistematico ogni fase del proprio ciclo di lavoro, così da agevolare le **verifiche interne** e assicurare che le registrazioni riflettano in modo accurato i risultati ottenuti. Questo approccio facilita la creazione di un sistema armonizzato di gestione della **qualità**, orientato alla soddisfazione del gruppo DGS e al rispetto degli impegni assunti.

Il Fornitore si impegna a segnalare prontamente all'Ufficio Acquisti del gruppo DGS qualsiasi **Non Conformità** relativa ai temi trattati nel presente Codice di Condotta, tramite i canali previsti, in particolare rispetto alle tematiche della Responsabilità Sociale e della Sostenibilità.

2 Principi etici fondamentali

Tutti i Fornitori sono tenuti ad aderire ai principi stabiliti dal **Codice Etico** del gruppo DGS, disponibile sul sito ufficiale all'indirizzo:

<https://www.dgspa.com/wp-content/uploads/2024/12/Codice-Etico-Gruppo-DGS.pdf>

Questi principi guidano le relazioni commerciali e stabiliscono standard chiari per il comportamento etico. I valori cardine includono:

- **Legalità:** i Fornitori devono rispettare tutte le leggi e normative applicabili. Ad esempio, ogni transazione economica deve essere documentata in modo trasparente, evitando qualsiasi pratica che possa configurarsi come evasione fiscale. Durante gli audit, i Fornitori devono garantire la tracciabilità delle operazioni e dei flussi finanziari, fornendo la documentazione richiesta.
- **Onestà e trasparenza:** è essenziale fornire informazioni veritiere durante il processo di qualifica nell'Albo fornitori "jAlbo", evitando omissioni o dichiarazioni false che possano compromettere la fiducia reciproca. Ad esempio, i Fornitori sono chiamati a comunicare tempestivamente eventuali cambiamenti societari o modifiche significative nei processi produttivi che possano influire sui contratti in essere.
- **Responsabilità sociale:** il rispetto dei diritti umani e delle condizioni lavorative deve essere garantito in ogni fase delle attività. Ad esempio, conformemente ai requisiti dello standard SA8000, i Fornitori devono assicurare che nei propri stabilimenti non siano presenti lavoro minorile o forzato e che i lavoratori godano di condizioni di sicurezza adeguate. Questo può includere, ad esempio, l'installazione di sistemi di ventilazione nei luoghi di lavoro e la fornitura di dispositivi di protezione individuale (DPI).
- **Molestie e discriminazioni:** i Fornitori devono garantire un ambiente lavorativo sicuro, vietando e prevenendo attivamente molestie, mobbing e discriminazioni, trattando tutti i dipendenti con rispetto e dignità. Ogni processo di selezione, assunzione e gestione del personale deve rispettare il principio di equità, evitando qualsiasi forma di pregiudizio legata a razza, genere, età, orientamento sessuale, religione o altre caratteristiche personali. I Fornitori sono tenuti ad offrire pari opportunità a tutti i lavoratori e candidati.
- **Riservatezza:** la tutela delle informazioni sensibili e dei dati personali è un obbligo imprescindibile. I Fornitori devono adottare misure per proteggere i dati aziendali e personali nonché i dati dei propri clienti. Ciò include l'uso di sistemi di crittografia per proteggere i dati trasmessi e archiviati, oltre all'implementazione di procedure per mitigare i rischi emergenti nei sistemi informativi.
- **Sostenibilità ambientale:** ogni attività deve essere svolta minimizzando l'impatto ambientale. Ad esempio, è richiesto un utilizzo responsabile delle risorse naturali e l'implementazione di programmi per il riciclo dei materiali, in linea con le certificazioni ambientali del gruppo DGS. Se richiesto loro, i Fornitori devono inoltre collaborare a predisporre i report annuali sui progressi compiuti in termini di riduzione delle emissioni di CO₂. Si incoraggia inoltre l'adozione di strategie per l'ottimizzazione dei processi produttivi, incluse iniziative per ridurre la plastica monouso e migliorare la sostenibilità degli imballaggi.
- **Pratiche di pagamento e registri aziendali:** i Fornitori sono tenuti ad adottare pratiche di pagamento corrette e a rispettare i termini contrattuali concordati, garantendo la trasparenza e la puntualità nelle transazioni economiche. Inoltre, devono assicurare che tutti i registri aziendali siano accurati e rappresentino fedelmente le transazioni effettuate, prevenendo qualsiasi forma di alterazione o falsificazione dei dati.
- **Sistemi di gestione e qualità dei prodotti:** per garantire la sicurezza e la qualità dei prodotti o servizi forniti, i Fornitori devono implementare sistemi di gestione conformi agli standard internazionali applicabili. Questi sistemi devono includere controlli periodici per garantire la conformità agli standard concordati, prevenendo la distribuzione di prodotti difettosi o non conformi.

3 Conformità alle normative vigenti

I Fornitori devono garantire piena conformità alle disposizioni normative applicabili e agli standard internazionali adottati dal gruppo DGS, tra cui ISO 37001, SA8000, UNI/PdR 125, ISO/IEC 27001, ISO/IEC 27701 e ISO 22301 e alle normative specifiche di settore, inclusa la direttiva NIS2 (Dir. UE n. 2022/2555 del 14 dicembre 2022, recepita dal d. lgs. 4 settembre 2024, n. 138) e il Codice degli Appalti (d. lgs. 36/2023). Tra le principali normative e certificazioni rilevanti si includono:

- **Decreto Legislativo 231/2001:** i Fornitori devono assicurare che la loro attività sia conforme al Modello Organizzativo 231 di DGS o delle altre società del gruppo DGS che ha adottato il

decreto. Tale Modello è stato adottato e implementato sia da DGS S.p.A., società controllante che gestisce l'Albo fornitori "jAlbo", sia dalle altre società controllate del gruppo (We.Do Advisory Srl, Porini Srl, Vista Technology Srl, SMC Treviso Srl). Pertanto, è richiesta l'esplicita accettazione del Modello di Organizzazione, Gestione e Controllo (MOGC) disponibile sul sito ufficiale del gruppo DGS:

<https://www.dgsspa.com/chi-siamo/governance-e-compliance/modello-organizzativo-231-01-e-codice-etico/>

e l'impegno a rispettarne i principi e le disposizioni in ogni fase delle attività svolte.

- **ISO 37001**: per la prevenzione della corruzione, i Fornitori devono dimostrare di aver adottato politiche e procedure adeguate a identificare e mitigare i rischi di corruzione. Inoltre, è richiesta l'esplicita accettazione della **Politica per la Prevenzione della Corruzione** del gruppo DGS, che definisce le misure necessarie per prevenire comportamenti illeciti e garantire trasparenza nelle relazioni commerciali.
- **Regolamento UE 2016/679 (GDPR)**: il Trattamento dei dati personali svolto dal Fornitore in qualità di Titolare o Responsabile del Trattamento deve essere conforme al GDPR, garantendo la sicurezza, la riservatezza e la protezione dei diritti degli interessati. I Fornitori devono implementare misure come la crittografia, controlli di accesso e protocolli per la gestione dei dati personali trattati.
- **SA8000**: i Fornitori devono rispettare i requisiti dello standard sulla Responsabilità sociale, inclusa la garanzia di condizioni di lavoro sicure e dignitose, l'assicurazione di retribuzioni adeguate e il divieto di discriminazione e sfruttamento lavorativo. Le attività di monitoraggio devono essere documentate e messe a disposizione del gruppo per verifiche periodiche.
- **UNI/PdR 125**: i Fornitori sono tenuti a promuovere politiche per la parità di genere e l'inclusione, conformi alle linee guida della prassi di riferimento UNI/PdR 125. Questo include l'adozione di misure per garantire pari opportunità e la valorizzazione della diversità nei luoghi di lavoro.

3.1 Gestione e responsabilità nell'utilizzo dei Subfornitori

Ogni **Fornitore** che intenda avvalersi di **Subfornitori** ha l'obbligo di richiedere e ottenere preventivamente un'**approvazione formale** dal gruppo **DGS**, al fine di garantire che l'intera filiera operi nel rispetto dei principi etici, legali e tecnici descritti nel presente Codice di Condotta. Questo requisito non riguarda esclusivamente le clausole contrattuali, poiché include la verifica dell'aderenza agli **standard di salute e sicurezza** nei luoghi di lavoro, di **protezione dei dati personali**, di **sicurezza informatica** e di **rispetto dell'ambiente** anche da parte dei Subfornitori segnalati. Un'inosservanza o un disallineamento da parte dei Subfornitori, infatti, costituisce un **rischio reputazionale e legale** per l'intero gruppo, in quanto comportamenti difforni potrebbero ledere l'immagine dell'azienda e generare responsabilità in capo al Fornitore che ne ha autorizzato l'impiego.

Inoltre, considerando che i requisiti previsti dai Clienti del gruppo DGS si trasferiscono lungo tutta la catena del valore, ai Fornitori sarà richiesto di **possedere le medesime certificazioni richieste a DGS dai propri Clienti**. In assenza di tali certificazioni, i fornitori non potranno essere coinvolti nelle attività relative a Clienti che prevedano requisiti specifici come condizione obbligatoria per la partecipazione a gare o appalti. In particolare, per tutte le attività in cui è espressamente richiesta la **certificazione ISO 9001 come requisito obbligatorio di partecipazione**, tipicamente previsto dalla Pubblica Amministrazione, non sarà consentito l'impiego di Fornitori o Subfornitori privi di tale certificazione.

Ferma restando la facoltà di controllo da parte del gruppo DGS di cui al § 12, è onere del Fornitore svolgere un'analisi continuativa delle prestazioni dei propri Subfornitori e comunicarne tempestivamente gli esiti al gruppo DGS tramite il portale jAlbo, garantendo la trasparenza e la tempestività delle informazioni. L'analisi deve includere verifiche e controlli in ambiti strategici come la **sicurezza sul lavoro**, la gestione delle **informazioni personali**, la robustezza dei sistemi di

cybersecurity e l'implementazione di politiche di **tutela ambientale**. In questo quadro, i Fornitori devono mantenere traccia delle non conformità eventualmente rilevate, predisporre **azioni correttive** e informare il gruppo **DGS** su ogni situazione che possa incidere sui requisiti minimi di conformità. In tal modo, si assicura una filiera trasparente, coerente e in linea con i valori e gli **standard** del gruppo.

Nel caso in cui un Subfornitore non aderisca alle **misure** definite o si renda responsabile di violazioni gravi, il Fornitore principale dovrà procedere con interventi rapidi per ripristinare la conformità, concordando con il gruppo DGS i termini di risoluzione delle criticità. Qualora la situazione non trovi una soluzione idonea entro i tempi prestabiliti, il gruppo DGS valuterà provvedimenti che possono includere, in linea con quanto indicato al capitolo 13, la **sospensione** o l'**esclusione** del Fornitore dall'**Albo**, nonché la **risoluzione** dei contratti in essere ed il **risarcimento** dei danni subiti.

Questa impostazione preserva l'**integrità** e la **credibilità** dell'intera filiera, tutelando le prerogative di **legalità**, **qualità** e **responsabilità** che contraddistinguono il sistema di gestione del gruppo DGS.

3.2 Riservatezza e proprietà intellettuale

Qualunque informazione (ad esempio, progetti, formule, documenti, dati finanziari, ecc.) portata a conoscenza del Fornitore per l'adempimento dei suoi obblighi contrattuali verso le società del gruppo DGS interessate deve essere considerata **confidenziale**: pertanto, dovrà essere trattata come tale e non dovrà essere divulgata a Terzi. In particolare, i Fornitori dovranno:

- adoperarsi al meglio per preservare la segretezza di tutte le informazioni riservate;
- adoperarsi al meglio per mantenere tutte le informazioni riservate al sicuro e protette da furto, danno, perdita o accesso non autorizzato;
- adoperarsi al meglio per non utilizzare alcuna informazione riservata per scopi diversi da quelli previsti dall'accordo siglato con le società del gruppo DGS di volta in volta coinvolte;
- informare i propri dipendenti, collaboratori, consulenti, subfornitori che ricevono informazioni dalle società del gruppo DGS che queste sono **riservate e non divulgabili**, se non nei limiti dell'attività da svolgere.

Gli obblighi di riservatezza e non divulgazione entrano sempre in vigore a partire dalla data di firma del Contratto di fornitura/Ordine d'acquisto o qualunque altra tipologia di accordo, per l'intera durata dell'accordo, nonché per un ulteriore periodo di 24 mesi. Su richiesta dell'Acquirente, il Fornitore è tenuto a distruggere tutte le informazioni in suo possesso (dando conferma scritta dell'avvenuta distruzione) e/o a restituire all'Acquirente tutte le copie di tali informazioni di cui abbia a qualunque titolo disponibilità.

Qualsiasi diritto d'autore o diritto di proprietà intellettuale su quanto realizzato dal Fornitore nell'esecuzione di un Ordine è della società del gruppo DGS acquirente. L'uso di tali elementi al di fuori dell'ambito definito dal gruppo DGS costituisce violazione della proprietà intellettuale e può dare luogo alle azioni legali ritenute più opportune al fine di tutelare il gruppo DGS nei confronti del Fornitore.

4 Prevenzione e gestione della corruzione

Il gruppo DGS adotta una politica di **tolleranza zero nei confronti della corruzione**, applicabile a tutti i Fornitori e all'intera filiera. Qualsiasi comportamento che possa configurare episodi di corruzione, favoritismo o tentativo di influenzare indebitamente decisioni aziendali è severamente vietato e potrà comportare l'esclusione immediata dall'Albo fornitori del gruppo DGS, nonché ulteriori azioni legali.

I Fornitori devono garantire che le proprie attività vengano svolte in maniera trasparente, correttamente documentata e sempre conforme alle normative vigenti, in particolare al **Decreto Legislativo 231/2001** e allo standard internazionale **ISO 37001**.

Nello specifico, sono rigorosamente vietati i seguenti comportamenti, sia diretti che indiretti (anche tramite interposta persona):

- offrire, promettere, richiedere o accettare tangenti, somme di denaro, regali o altri benefici economici finalizzati a influenzare o alterare decisioni aziendali, favorendo indebitamente gli interessi propri o di terzi;
- attuare pratiche illecite o non etiche, come falsificazione documentale o manipolazione di informazioni, per ottenere vantaggi indebiti o privilegi;
- esercitare pressioni indebite o coercitive nei confronti di dipendenti del gruppo DGS, collaboratori, Clienti, Fornitori, pubbliche amministrazioni o qualsiasi altro soggetto coinvolto nelle attività aziendali;
- promettere o offrire omaggi, ospitalità (come pranzi, cene, soggiorni alberghieri, partecipazioni a eventi) o altre forme di liberalità a Fornitori, potenziali Fornitori, partner commerciali, esponenti della Pubblica Amministrazione o qualsiasi soggetto che abbia rapporti con il gruppo DGS, salvo che tali attività rientrino nelle normali pratiche commerciali, abbiano valore simbolico e siano preventivamente autorizzate e documentate;
- offrire regali o altre utilità quando non correlati a uno specifico e legittimo scopo commerciale o in assenza di trasparenza e documentazione scritta;
- effettuare liberalità, sponsorizzazioni od omaggi in favore di soggetti terzi (persone fisiche o organizzazioni) qualora vi sia il fondato sospetto che ciò possa esporre il gruppo DGS al rischio di commissione di reati previsti dal d. lgs. 231/2001;
- concedere sponsorizzazioni o liberalità a soggetti con cui si configuri o possa configurarsi un conflitto di interessi, anche solo potenziale;
- invitare esponenti della Pubblica Amministrazione a eventi commerciali o di co-marketing qualora vi sia il sospetto che ciò possa esporre il gruppo a rischi di commissione di reati.

In particolare, riguardo a eventuali omaggi e regalie ai dipendenti o collaboratori del gruppo DGS, valgono i seguenti **principi rigorosi**:

- Gli omaggi devono essere limitati a occasioni quali festività, eventi o iniziative commerciali specifiche, chiaramente riconducibili alle attività di comunicazione e marketing dell'azienda.
- Sono consentiti esclusivamente regali di cortesia, simbolici e di modico valore economico (non superiore a euro 150,00). Tali regalie devono:
 - non generare, nel destinatario o in un terzo imparziale, l'impressione che siano finalizzate ad acquisire indebiti vantaggi;
 - non indurre alcun dubbio o sospetto di illegalità o immoralità;
 - non compromettere l'integrità, la reputazione o l'autonomia di giudizio del destinatario;
 - non avere l'intento implicito o esplicito di influenzare decisioni aziendali o commerciali.
- Qualora un dipendente, collaboratore o dirigente del gruppo DGS riceva un omaggio di valore superiore a euro 150,00, avrà l'obbligo di rifiutarlo e darne tempestiva informazione scritta al proprio diretto Responsabile e/o agli Amministratori Delegati.

Inoltre, per assicurare la completa conformità agli obblighi normativi e prevenire in maniera proattiva i rischi di corruzione, i Fornitori devono obbligatoriamente:

- implementare e mantenere aggiornato un sistema interno efficace di controlli preventivi, capace di monitorare e intercettare tempestivamente pratiche illecite o non conformi al presente Codice di Condotta;
- documentare dettagliatamente e in modo tracciabile ogni transazione economica rilevante;
- formare periodicamente i propri dipendenti e collaboratori sulla prevenzione della corruzione, assicurando che siano consapevoli delle norme applicabili, degli standard richiesti dal gruppo DGS, e delle relative procedure di segnalazione di eventuali comportamenti non conformi;
- assicurare piena collaborazione durante le attività di audit e verifica svolte dal gruppo DGS o da enti terzi incaricati.

I Fornitori dovranno inoltre garantire che tali obblighi vengano estesi e rispettati anche da parte di eventuali Subfornitori coinvolti nella filiera.

La violazione di tali disposizioni può comportare l'immediata sospensione o esclusione dall'Albo fornitori del gruppo DGS, la risoluzione immediata dei contratti in essere e l'attivazione delle azioni legali previste dalla normativa vigente, inclusa la richiesta di risarcimento dei danni eventualmente subiti.

Questo approccio rigoroso mira a garantire la massima integrità e trasparenza in tutte le attività del gruppo DGS e dei suoi Fornitori, preservando la reputazione aziendale e contribuendo attivamente alla prevenzione della corruzione lungo tutta la catena di valore.

4.1 Divieto di attività non contrattualizzate

È fatto assoluto divieto ai Fornitori di eseguire attività per nome, per conto o in favore del gruppo DGS senza che l'attività stessa sia stata formalmente contrattualizzata tramite un Ordine di Acquisto (OdA) emesso dall'Ufficio Acquisti di gruppo (UA). Qualsiasi attività svolta senza un accordo formale scritto sarà considerata una violazione grave del presente Codice di Condotta.

In casi eccezionali, e unicamente dietro specifica e preventiva autorizzazione scritta da parte del gruppo DGS, i fornitori potranno avviare attività in anticipata esecuzione. Tali situazioni devono essere limitate a brevi periodi e giustificate da cause straordinarie, documentate ed approvate preventivamente dalla Direzione. Anche in questi casi, il Fornitore è tenuto a garantire il pieno rispetto delle disposizioni contrattuali e dei principi del presente Codice.

4.2 Governance delle segnalazioni

Il gruppo DGS promuove un ambiente organizzativo in cui le violazioni del presente Codice di condotta o delle normative applicabili possano essere segnalate senza timore di ritorsioni, anche in conformità al **Decreto Legislativo 24/2023** sulla protezione delle persone che segnalano violazioni di disposizioni normative nazionali e dell'Unione Europea (c.d. whistleblowing).

Per tale ragione, il gruppo DGS si è dotato di un sistema unico di segnalazione e, in particolare, dei canali interni di segnalazione:

- piattaforma informatica dedicata raggiungibile al link: <https://report.whistleb.com/it/dgsspa>;
- richiesta di incontro diretto con il Gestore del sistema di segnalazione, da trasmettere via email all'indirizzo compliance@dgsspa.com.

Attraverso questi canali, possono essere segnalati eventuali comportamenti scorretti, illeciti o non conformi alle prescrizioni del presente Codice e alle disposizioni normative di riferimento, anche in forma anonima, con la garanzia assoluta di riservatezza dell'identità del segnalante e delle informazioni fornite.

Le segnalazioni ricevute saranno gestite dal gruppo DGS attraverso procedure rigorose e tempestive, che garantiscono l'imparzialità nell'indagine, la tracciabilità degli interventi e l'applicazione di eventuali azioni correttive.

Per i dettagli sul funzionamento del sistema di segnalazione interno, si rinvia alla **PO-10-04 Ethica. Procedura di segnalazione unificata** disponibile sull'area Compliance del sito di DGS.

In conformità agli obblighi derivanti dal Decreto Legislativo 24/2023, è altresì richiesta l'implementazione di sistemi interni adeguati a ricevere, gestire e documentare eventuali segnalazioni whistleblowing nei confronti dei Fornitori: a) con almeno 50 dipendenti; b) che – anche se hanno impiegato meno di 50 lavoratori subordinati nell'ultimo anno solare – abbiano adottato un proprio Modello 231; c) che, anche con meno di 50 lavoratori subordinati impiegati nell'ultimo anno solare e senza un Modello 231, operino in uno dei settori specifici indicati dal d. lgs. 24/2023, Parti I.B e II dell'Allegato 1 al predetto decreto. Per i Fornitori non tenuti all'implementazione di tali sistemi di segnalazione ai sensi della normativa vigente, tale implementazione resta comunque fortemente raccomandata come buona pratica aziendale.

5 Prevenzione del conflitto di interessi

I Fornitori sono tenuti a rispettare tutte le leggi applicabili in materia di conflitto di interessi e compiere ogni sforzo necessario a prevenire il verificarsi di situazioni che creino un conflitto di interessi nell'ambito delle loro relazioni commerciali con le società del gruppo DGS, evitando di omettere o celare situazioni di conflitto di interessi potenziali o confermate o che potrebbero interferire con la capacità di prendere decisioni imparziali ed etiche nel miglior interesse del gruppo DGS.

I Fornitori dovranno informare le società del gruppo DGS acquirenti in merito a qualsiasi situazione potenziale o confermata di conflitto di interessi, in modo da consentire al gruppo DGS di valutare eventuali azioni correttive e/o provvedimenti.

Inoltre, i Fornitori, si impegnano a rifiutare di partecipare, supervisionare o influenzare qualsiasi decisione professionale in merito a familiari, relazioni personali o persone impiegate presso le società del gruppo DGS, con le quali il Fornitore sia impegnato finanziariamente.

6 Parità di genere e inclusione

Il gruppo DGS promuove politiche di **diversità, uguaglianza e inclusione**, richiedendo ai propri Fornitori di adottare principi e pratiche in linea con le norme **UNI/PdR125** e la **ISO 30415**. I Fornitori devono impegnarsi a creare un ambiente lavorativo equo, rispettoso e inclusivo, che valorizzi le differenze e promuova opportunità uguali per tutti.

In particolare, i Fornitori devono:

- Garantire pari opportunità a tutti i lavoratori, indipendentemente da genere, età, orientamento sessuale, etnia, disabilità o credo religioso.
- Assicurare che i processi di assunzione, promozione e retribuzione siano equi e privi di qualsiasi discriminazione.
- Promuovere la partecipazione attiva delle donne e delle minoranze nei ruoli chiave dell'organizzazione.
- Prevedere programmi di formazione e sensibilizzazione per favorire la comprensione e l'adozione di politiche inclusive.

Il rispetto di queste disposizioni sarà oggetto di monitoraggio da parte del gruppo DGS, che potrà richiedere ai Fornitori report periodici o condurre verifiche dirette per assicurarsi della conformità agli standard richiesti.

7 Impegno per la Responsabilità sociale

In conformità ai requisiti dello **standard SA8000**, i Fornitori devono adottare politiche e procedure che tutelino i **diritti umani** e garantiscano condizioni di lavoro dignitose lungo l'intera filiera produttiva. Lo **standard SA8000**, basato sulla **Dichiarazione Universale dei Diritti Umani** e sulle Convenzioni dell'**International Labour Organization (ILO)**, prescrive un sistema di gestione che coinvolge sia gli aspetti contrattuali sia le pratiche quotidiane di ogni operatore economico che collabori con il gruppo DGS. Lo scopo di tale sistema consiste nell'assicurare che ogni processo produttivo rispetti la **centralità della persona**, la **sicurezza** e la **salubrità** del luogo di lavoro, la **libertà** di associazione, la **retribuzione** dignitosa e l'assenza di qualsiasi forma di **sfruttamento**.

I Fornitori sono obbligati a:

- **Vietare il lavoro minorile**, garantendo che nei propri stabilimenti non vi siano impiegati bambini, e adottando sistemi di verifica dell'età dei lavoratori per impedire l'inserimento di minori nelle mansioni lavorative.
- **Impedire il lavoro forzato e coercitivo**, assicurando che ogni lavoratore operi su base volontaria, senza forme di minaccia, intimidazione o ritenzione di documenti personali, in conformità alle disposizioni dell'**ILO** sul lavoro forzato.
- **Vietare di impiegare manodopera sottoponendola a condizione di sfruttamento** o approfittando del loro stato di bisogno, quali: (i) la corresponsione di retribuzioni in modo palesemente difforme dai contratti collettivi nazionali o sproporzionato rispetto alla quantità

e qualità del lavoro prestato ovvero; (ii) la reiterata violazione della normativa relativa all'orario lavorativo, al riposo, all'aspettativa obbligatoria e alle ferie; (iii) violazione delle norme in materia di salute, sicurezza e igiene sul lavoro; (iv) sottoposizione del lavoratore a condizioni di lavoro, metodi di sorveglianza o situazioni alloggiative degradanti.

- **Promuovere condizioni di lavoro sicure e salubri**, introducendo misure documentate e regolarmente aggiornate per prevenire rischi e incidenti, programmando corsi di formazione obbligatori, fornendo dispositivi di protezione individuale (**DPI**) e strutturando piani di emergenza e manutenzione degli impianti.
- **Rispettare il diritto di associazione e contrattazione collettiva**, consentendo ai lavoratori di costituire o aderire liberamente a sindacati, senza temere discriminazioni o ripercussioni, in linea con le Convenzioni fondamentali dell'**ILO**.
- **Assicurare una retribuzione equa**, garantendo salari conformi almeno ai minimi legali previsti dalla legislazione nazionale, così da coprire i bisogni essenziali del lavoratore e della sua famiglia, e promuovendo, ove possibile, condizioni retributive migliorative.
- **Eliminare ogni forma di discriminazione**, rispettando i principi di pari opportunità durante la selezione, la formazione, i percorsi di carriera e ogni altra decisione relativa all'impiego, senza differenziare il trattamento in base a genere, età, etnia, orientamento sessuale, religione o disabilità.
- **Gestire correttamente gli orari di lavoro**, rispettando la normativa nazionale e contrattuale in materia di orario giornaliero e settimanale, ferie retribuite e giorni di riposo, evitando carichi eccessivi che possano danneggiare il benessere psicofisico dei lavoratori.

Lo standard **SA8000** richiede inoltre che i Fornitori si dotino di procedure interne volte a monitorare e migliorare nel tempo il rispetto di questi principi, attraverso verifiche periodiche, la definizione di ruoli di responsabilità e l'istituzione di canali di comunicazione che assicurino la **segnalazione** di eventuali problematiche o violazioni.

I Fornitori devono diffondere i principi della **SA8000** anche a eventuali **Subfornitori** e garantire che l'intera catena di approvvigionamento adotti la medesima attenzione alla Responsabilità sociale. Ogni constatata violazione potrà tradursi nell'avvio di un percorso correttivo, finalizzato a risolvere le irregolarità entro tempi definiti. In assenza di interventi risolutivi, il gruppo DGS adotterà misure sanzionatorie, in linea con quanto indicato al capitolo 13.

8 Ambiente, salute e sicurezza

I Fornitori sono tenuti a condurre le proprie attività garantendo elevati standard di tutela dell'ambiente, della salute e della sicurezza nei luoghi di lavoro. Devono implementare un sistema di gestione ambientale conforme alle normative vigenti, con particolare attenzione alla riduzione delle emissioni inquinanti e alla gestione responsabile dei rifiuti.

È necessario adottare misure preventive per garantire la sicurezza e la salute dei dipendenti e di tutte le persone coinvolte nelle attività lavorative. Ciò include:

- L'identificazione e la valutazione dei rischi per la sicurezza e la salute.
- La messa in atto di piani di emergenza per prevenire e gestire incidenti.
- La fornitura di formazione continua ai dipendenti su temi di sicurezza e salute sul lavoro.
- L'adozione di dispositivi di protezione individuale (**DPI**) adeguati alle attività svolte.

I Fornitori devono inoltre monitorare e migliorare continuamente le condizioni lavorative, documentando gli interventi effettuati e i progressi ottenuti.

I Fornitori devono, inoltre, adoperarsi per garantire che eventuali **Subfornitori**, di cui si avvalgono per l'esecuzione dei contratti con il gruppo DGS, operino nel rispetto dei medesimi standard di tutela dell'ambiente, della salute e della sicurezza sui luoghi di lavoro a loro applicabili.

9 Gestione responsabile delle tecnologie avanzate e dell'intelligenza artificiale

I Fornitori del gruppo DGS devono garantire che l'uso di tecnologie avanzate, inclusa l'intelligenza artificiale (IA), sia allineato a principi etici, rispettando i diritti umani, la trasparenza e la responsabilità. Devono implementare sistemi e procedure per garantire che tali tecnologie non siano utilizzate in modo discriminatorio o per scopi contrari alle normative vigenti.

Tra i requisiti specifici:

- **Etica e trasparenza:** le applicazioni tecnologiche devono essere sviluppate e utilizzate in modo trasparente, garantendo che i processi decisionali automatizzati siano comprensibili e spiegabili.
- **Rispetto della privacy:** ogni tecnologia implementata deve rispettare pienamente le normative in materia di protezione dei dati personali, come il GDPR, evitando utilizzi impropri o raccolte non autorizzate di dati.
- **Responsabilità nell'uso dell'IA:** i Fornitori devono evitare applicazioni che possano causare danni sociali, economici o ambientali, garantendo un controllo rigoroso sulle finalità di utilizzo. L'impiego di strumenti di intelligenza artificiale nello svolgimento delle attività di trattamento svolte per conto del gruppo deve essere oggetto di preventiva richiesta scritta da parte del Fornitore e di preventiva approvazione scritta da parte di DGS.
- **Sostenibilità tecnologica:** le soluzioni tecnologiche devono essere progettate per ottimizzare l'efficienza energetica e minimizzare l'impatto ambientale, con un focus sull'innovazione responsabile.

Il gruppo DGS si riserva il diritto di verificare l'uso di tali tecnologie durante gli audit di conformità, al fine di assicurare che rispettino i requisiti stabiliti. I Fornitori sono incoraggiati a intraprendere attività di formazione continua per il personale coinvolto nello sviluppo e nella gestione delle tecnologie avanzate.

10 Privacy

Il gruppo DGS considera la privacy e la protezione dei dati personali come elementi fondamentali per garantire la conformità normativa e la fiducia nelle relazioni commerciali. A tal fine, il gruppo richiede che i propri Fornitori operino in conformità alla **ISO/IEC 27701**, integrando e applicando rigorosamente i principi e le misure tecniche e organizzative previsti dallo standard, oltre che dal Regolamento Generale sulla Protezione dei Dati (GDPR). In linea con il GDPR e le migliori pratiche internazionali, il gruppo ha sviluppato un quadro di requisiti chiaro e rigoroso, rivolto a tutti i Fornitori che trattano dati personali, sia in qualità di autonomi Titolari del Trattamento, sia come Responsabili o Sub-responsabili designati dal gruppo.

L'obiettivo del gruppo è promuovere l'adozione di pratiche sicure e trasparenti lungo l'intera catena di approvvigionamento, garantendo che tutte le attività di Trattamento dei dati siano condotte nel rispetto dei diritti degli interessati e con un alto livello di protezione.

10.1 Privacy e protezione dei dati personali dei Fornitori da parte del gruppo DGS

Il Trattamento dei dati personali dei Fornitori è regolato dalle Informativa privacy del gruppo DGS, conformi al **GDPR**, per garantire il rispetto dei diritti degli interessati e la tutela delle informazioni trattate. In particolare, i Fornitori devono:

- **Consultare l'informativa privacy Fornitori**, disponibile sul sito istituzionale del gruppo DGS (<https://www.dgspa.com/informativa-privacy-fornitori/>) ed inviata anche congiuntamente all'emissione di ogni Ordine d'Acquisto da parte delle società del gruppo. L'informativa specifica le finalità e le modalità del trattamento dei dati dei Fornitori.

- **Adottare misure di sicurezza adeguate:** i Fornitori devono implementare sistemi di protezione dei dati sensibili, ad esempio tramite crittografia, controllo degli accessi, firewall e procedure di backup regolari. Queste misure sono fondamentali per evitare accessi non autorizzati, perdite o alterazioni dei dati.
- **Rispettare i diritti degli interessati:** i Fornitori devono garantire il diritto di accesso, rettifica, cancellazione e limitazione del trattamento, oltre alla portabilità dei dati, come previsto dagli articoli 15-22 del GDPR.

Per quanto riguarda l'**Informativa relativa alla registrazione al portale "jAlbo"**, i dati personali raccolti al momento dell'iscrizione all'albo sono trattati al fine di:

- qualificare i Fornitori in base ai requisiti normativi e tecnici richiesti dal gruppo DGS;
- verificare l'idoneità economica, finanziaria e reputazionale dei candidati;
- garantire la gestione amministrativa e tecnica dei rapporti contrattuali instaurati.

L'informativa prevede inoltre l'utilizzo dei dati per scopi di monitoraggio e audit, al fine di assicurare la conformità ai requisiti del presente Codice. I Fornitori sono obbligati a mantenere aggiornate le informazioni trasmesse attraverso "jAlbo" e a fornire documentazione di supporto, se richiesta. La mancata comunicazione o aggiornamento dei dati può determinare la sospensione o l'esclusione dall'Albo fornitori.

10.2 Trattamento dei dati personali come Responsabile o Sub-responsabile

Nel caso in cui un Fornitore tratti dati personali per conto del gruppo DGS in qualità di Responsabile o Sub-responsabile del Trattamento, il gruppo DGS fornirà un **Data Processing Agreement (DPA)** in relazione a ciascun contratto stipulato o stipulando. Questa DPA dovrà essere sottoscritta dal Fornitore come integrazione agli obblighi contrattuali esistenti e conterrà le disposizioni dettagliate per il trattamento dei dati personali.

Il Fornitore, in qualità di Responsabile o Sub-responsabile, si impegna a:

- Trattare i dati personali esclusivamente per le finalità indicate dal gruppo DGS e in conformità alle istruzioni documentate ricevute.
- Garantire che tutte le persone autorizzate al Trattamento dei dati dal Fornitore siano vincolate da obblighi di riservatezza, anche per il periodo successivo all'eventuale cessazione del rapporto di lavoro con il Fornitore.
- Mettere in atto misure tecniche e organizzative adeguate al fine di garantire un livello di sicurezza adeguato al rischio, come richiesto dall'articolo 32 del GDPR.
- Collaborare con il gruppo DGS per consentire l'esercizio dei diritti degli interessati, come accesso, rettifica, cancellazione e portabilità dei dati.
- Informare tempestivamente il gruppo DGS di qualsiasi richiesta, reclamo o ispezione ricevuta da parte di un'autorità di controllo o di un interessato in merito al trattamento dei dati.
- Consentire e facilitare audit o ispezioni periodiche da parte del gruppo DGS per verificare la conformità alle disposizioni della DPA e del GDPR.

Il gruppo DGS richiede ai propri Fornitori di implementare pratiche rigorose per garantire la protezione dei dati personali e la conformità alle normative applicabili, tra cui il GDPR. I Fornitori devono adottare misure organizzative e tecnologiche avanzate per assicurare che il Trattamento dei dati personali avvenga in modo sicuro, trasparente e nel rispetto dei diritti degli interessati.

Tra le principali misure richieste:

- **Crittografia e sicurezza dei dati:** tutti i dati personali trattati devono essere protetti attraverso meccanismi di crittografia avanzata sia durante la trasmissione che durante l'archiviazione.
- **Accesso controllato:** l'accesso ai dati personali deve essere limitato esclusivamente al personale autorizzato, con l'implementazione di controlli di accesso basati sul principio del "need to know".

- **Gestione delle violazioni dei dati:** i Fornitori devono disporre di un piano documentato per la gestione di eventuali violazioni dei dati personali, incluso l'obbligo di notifica al gruppo DGS nei tempi indicati in DPA.
- **Audit periodici:** è richiesto che i Fornitori conducano verifiche regolari sui propri sistemi di gestione dei dati personali per garantire la conformità alle normative e l'efficacia delle misure di sicurezza implementate.
- **Formazione del personale:** i dipendenti dei Fornitori coinvolti nel trattamento dei dati personali devono ricevere una formazione specifica e continua sulla protezione dei dati e sulle normative applicabili.

Il gruppo DGS si riserva il diritto di condurre audit presso i Fornitori per verificare la conformità agli standard di protezione dei dati personali e adottare misure correttive in caso di non conformità. La mancata osservanza di tali standard potrebbe comportare l'esclusione dall'Albo fornitori e la risoluzione dei contratti in essere, oltre al risarcimento dei danni subiti.

Il Fornitore è tenuto a garantire che eventuali Sub-responsabili coinvolti nel trattamento rispettino pienamente obblighi analoghi a quelli contenuti nella DPA fornita dal gruppo DGS e delle normative vigenti.

In ogni caso i Fornitori devono:

- **Operare nel rispetto del GDPR**, della normativa sul Trattamento dei dati personali e dei provvedimenti del Garante o dell'EDPB (European Data Protection Board) in materia.
- **Adottare misure di sicurezza adeguate:** i Fornitori devono implementare sistemi di protezione dei dati personali, ad esempio tramite crittografia, controllo degli accessi, firewall e procedure di backup regolari. Queste misure sono fondamentali per evitare accessi non autorizzati, perdite o alterazioni dei dati.
- **Rispettare i diritti degli interessati:** i Fornitori devono garantire il diritto di accesso, rettifica, cancellazione e limitazione del Trattamento, oltre alla portabilità dei dati, come previsto dagli articoli 15-22 del GDPR.

11 Regole comportamentali e per l'accesso alla rete delle aziende del gruppo DGS

In relazione all'attività svolta per conto delle società del gruppo DGS il dipendente del fornitore esterno, in qualità di incaricato del trattamento dei dati e Persona Autorizzata, si impegna a mantenere il segreto professionale e l'assoluta riservatezza rispetto a tutte le informazioni apprese durante lo svolgimento dei compiti assegnati.

L'incaricato dovrà effettuare il trattamento dei dati nel rispetto della normativa in vigore e delle misure di sicurezza indicate nel presente documento e quelle che successivamente verranno fornite in aggiornamento e/o aggiunta a quelle ivi previste in modo lecito e secondo correttezza.

- a) Raccogliere e in qualsiasi modo trattare dati personali non oltre quanto necessario alle esigenze ed allo svolgimento delle proprie mansioni/attività lavorative;
- b) Sottoporsi agli interventi di formazione e aggiornamento sulla normativa in materia di trattamento dei dati personali che il Titolare e/o il Responsabile organizzeranno;
- c) Comunicare e/o diffondere dati personali esclusivamente ai soggetti indicati dal Titolare o del Responsabile del trattamento secondo le modalità fornite;
- d) Non estrarre copia di banche dati o di singoli dati o creare nuove ed autonome banche dati al di fuori di quanto necessario alle mansioni lavorative;
- e) Accertarsi che il dispositivo aziendale in dotazione sia protetto da una chiave di accesso composta da almeno otto caratteri alfanumerici e non contenga riferimenti agevolmente riconducibili all'incaricato;
- f) Modificare il proprio codice d'accesso al primo utilizzo e, successivamente, ogni 3 mesi; in caso di dubbi, anche minimi, sulla possibilità che la segretezza della password sia stata

- compromessa dovrà immediatamente procedere alla sostituzione della stessa e darne comunicazione al Titolare o al Responsabile del trattamento;
- g) Non comunicare o rendere conoscibile a terzi il proprio codice di accesso e/o consentire a terzi di utilizzare il dispositivo aziendale e/o accedere ai dati per nessun motivo; senza previa autorizzazione del Titolare o del Responsabile del trattamento;
 - h) Non salvare i dati in locale sul dispositivo aziendale;
 - i) Il dispositivo aziendale è assegnato per utilizzo esclusivamente lavorativo; non utilizzarlo a scopo personale, non consultare internet e la posta elettronica a fini privati da tali dispositivi ovvero ascoltare o scaricare file audio o video, se non a fini prettamente lavorativi;
 - j) Non modificare le configurazioni preimpostate sul proprio dispositivo e/o scaricare ulteriori applicazioni o programmi senza previa espressa autorizzazione del Titolare o del Responsabile del trattamento;
 - k) Non lasciare incustodito o accessibile a terzi il dispositivo aziendale;
 - l) Con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate senza mantenerne copia; quando tali atti e i documenti contengano speciali categorie di dati personali e sono affidati all'Incaricato per lo svolgimento dei relativi compiti, quest'ultimo deve controllare e custodire i medesimi atti e documenti fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e deve restituirli al termine delle operazioni affidate;
 - m) Archiviare e custodire i documenti all'interno di armadi\mobili\cassetti muniti di serratura;
 - n) Conservare le chiavi con diligenza e restituirle al responsabile delle stesse; non lasciare le chiavi nella serratura o comunque in un luogo facilmente accessibile al termine della giornata lavorativa;
 - o) Chiudere a chiave l'archivio (armadio, cassetto ecc.) o l'ufficio durante la giornata, in caso di allontanamento dall'ufficio (es. in occasione di pausa, riunioni, ecc.), al fine di impedire l'accesso da parte di persone non autorizzate;
 - p) Prima di gettare nel cestino documenti cartacei contenenti eventuali dati personali, procedere alla loro distruzione, strappandoli o utilizzando un apposito distruggi documenti;
 - q) Non effettuare copie di dati personali tantomeno su supporti elettronici rimovibili, a meno di espressa autorizzazione del Titolare e/o del Responsabile. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
 - r) Conservare i supporti informatici e/o cartacei contenenti dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
 - s) Curare, in caso di utilizzo autorizzato di eventuali supporti di memorizzazione da parte del Titolare e/o del Responsabile, che i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori (devono essere utilizzati soltanto supporti vergini o vuoti);
 - t) Informare senza ritardo il proprio responsabile nel caso constati o sospetti un incidente di sicurezza;
 - u) Non raccogliere dati relativi alla salute dei clienti/interessati; a meno ch  sia strettamente necessario alla finalit  del trattamento dei dati in oggetto (es. assistenza clienti), e previo consenso adeguatamente informato dell'interessato al trattamento di dati sensibili;
 - v) Se del caso dare seguito alle richieste degli interessati ai sensi degli art. 15 e ss. del GDPR (tra cui le richieste di opposizione al trattamento, di limitazione, di rettifica dei dati o di loro cancellazione, etc.) nei tempi e nei modi previsti Titolare o del Responsabile del trattamento;
 - w) Qualora uno o pi  interessati denunci situazioni o fatti rilevanti di particolare gravit , informare tempestivamente il proprio responsabile affin  a sua volta comunichi la richiesta al Titolare e/al responsabile;
 - x) Segnalare, al Titolare e/o al Responsabile eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle gi  menzionate misure di sicurezza al fine di ridurre al

minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

- y) Informare tempestivamente il proprio responsabile affinché questi provveda ad informare il Titolare e/o il Responsabile quando, in considerazione della natura dei dati o, comunque, delle modalità del trattamento o degli effetti che esso può determinare, ritenga vi sia il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più Interessati.

11.1 Uso delle risorse informatiche e dei servizi di rete

Le risorse informatiche ed i relativi servizi di rete vengono messi a disposizione esclusivamente per attività legate ai rapporti professionali tra terze parti e le società del gruppo DGS.

È esplicitamente vietato l'utilizzo delle risorse informatiche e dei servizi di rete finalizzato a:

- attività commerciali non esplicitamente autorizzate;
- attività che possano compromettere la sicurezza dei dati e delle risorse messe a disposizione dal gruppo DGS;
- attività dirette a causare danno a terzi;
- attività contrarie alla legge o comunque proibite dai regolamenti interni;
- attività non conformi al rapporto instaurato tra le parti.

In particolare, è vietato:

- Cedere ad altri le proprie credenziali (user-id e password) di accesso ai servizi di rete;
- L'utilizzo di qualsiasi software o sistema finalizzato a nascondere la propria identità in rete;
- Predisporre connessioni non autorizzate alla rete aziendale di qualsiasi apparecchio che possa essere utilizzato anche indirettamente per realizzare un collegamento dall'esterno, compresi router, access-point, RAS Server, modem;
- Connettere o permettere la connessione in rete di computer su cui non sia presente un antivirus aggiornato e funzionante. In caso di sospetta presenza di un Virus è obbligatorio disconnettere immediatamente il Pc dalla rete;
- Fare copia, in qualunque forma e su qualunque tipo di Dispositivo analogico e/o digitale di Dati Personali e/o informazioni riservate e/o file della Società nella disponibilità dell'utente al fine di farne un uso personale o per trasferirle a terzi;
- Utilizzare programmi informatici o strumenti per intercettare, falsificare, alterare o cancellare per finalità illecite il contenuto di comunicazioni e/o documenti informatici;
- Modificare le configurazioni aziendali impostate sugli Strumenti Aziendali, salvo autorizzazione preventiva della Società;
- Collocare, anche temporaneamente, sugli Strumenti Aziendali o nella Rete qualsiasi file che non sia attinente allo svolgimento dell'attività lavorativa;
- Utilizzare, per la propria attività lavorativa, Strumenti Personali non previamente autorizzati;
- Ascoltare e/o visionare e/o scaricare programmi, film, file audio/musicali personali su strumenti aziendali, salvo autorizzazione preventiva della Direzione ,

Per quanto concerne l'utilizzo degli **smartphone aziendali** sui quali vengano immesse informazioni aziendali rilevanti, fermo restando quanto sopra, l'utente ove applicabile:

- deve sempre salvare i dati sugli share aziendali nella Rete;
- non può concedere in uso lo smartphone aziendale a soggetti terzi;
- al momento della restituzione del supporto, deve cancellare o comunque rimuovere i Dati Personali o le informazioni aziendali rilevanti in esso presenti.
- in caso di furto o smarrimento dello smartphone aziendali utilizzato per erogare la prestazione nei confronti della Società, l'utente deve denunciare, senza indugio, l'accaduto al Titolare o del Responsabile del trattamento ed alle competenti Autorità di Pubblica Sicurezza, consegnando copia della denuncia entro tre giorni dall'evento al referente della Società.

All'utente di una **casella di posta Aziendale** non è consentito:

- utilizzare l'indirizzo aziendale di posta elettronica per inviare e/o ricevere allegati contenenti filmati o brani musicali (es.mp3) non correlati all'attività lavorativa;
- inviare messaggi a carattere personale, se non nei limiti della normalità e cioè per un limitato numero di messaggi di cortesia od inerenti a rapporti parentali o amicali, sempre nel rispetto delle norme di comportamento di cui alla presente policy;
- inviare a soggetti terzi, tramite posta elettronica aziendale, messaggi con allegati file eseguibili, salvo espressa autorizzazione dalla Società;
- utilizzare la posta elettronica aziendale in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore.

È consigliato utilizzare il formato PDF per i documenti inviati all'esterno in formato elettronico.

La casella di posta elettronica aziendali è uno strumento di lavoro assegnato all'utente dall'Azienda, va quindi utilizzato per lo scambio di comunicazioni e dati utili all'esercizio della propria attività e secondo le norme di utilizzo sotto riportate.

I messaggi di posta elettronica sono filtrati in ricezione da prodotti antivirus; per evitare infezioni da virus ed altri rischi si raccomandano comunque i seguenti comportamenti:

- impostare il browser di posta in modo da mostrare solo le intestazioni dei messaggi, senza aprirli automaticamente;
- in caso di ricezione di messaggi da destinatari sconosciuti, controllare i file allegati prima del loro utilizzo e nel dubbio evitare la loro apertura;
- evitare di rispondere a messaggi di dubbia provenienza e contenuto (ad esempio quelli che invitano a rispondere per annullare eventuali iscrizioni mai avvenute);
- considerato che la posta elettronica diretta all'esterno della rete aziendale può essere intercettata da estranei, il suo utilizzo per inviare documenti di lavoro riservati o la cui conoscenza da parte di terzi possa procurare danni all'Azienda, è consentito solo se adeguatamente protetto con cifratura dei contenuti;

Ogni comunicazione inviata o ricevuta per posta elettronica che abbia contenuti rilevanti o che contenga impegni contrattuali o precontrattuali per l'Azienda, ovvero che contenga documenti da considerarsi riservati, dovrà essere trattato secondo le procedure in essere per la corrispondenza ordinaria, inviando copia del messaggio al proprio Responsabile gerarchico o funzionale;

- assicurarsi prima di inviare un messaggio che i destinatari specificati sono corretti;
- mantenere in ordine la propria casella di posta cancellando documenti inutili e ingombranti;

Resta inteso che i restanti messaggi relativi a vicende professionali della Società verranno conservati solo per il tempo necessario a perseguire la finalità di seguito specificata: tutela dei diritti in sede giudiziaria nei limiti del GDPR.

11.2 Condizioni di utilizzo della connessione remota

Nel caso in cui nell'ambito della prestazione erogata per conto di una società del gruppo DGS sia concesso l'utilizzo di una connessione remota alla intranet Aziendale l'utente prende atto che l'accesso alla Rete è consentito esclusivamente per lo svolgimento delle attività inerenti alle attività lavorative.

L'accesso alla Rete è fornito esclusivamente ad utenti riconosciuti ed identificabili secondo le policy interne alla Società ed è condizionato all'accettazione integrale della presente policy.

In caso di accertata inosservanza di una qualsiasi delle precedenti disposizioni, la Società del gruppo DGS ha il diritto di intraprendere tutte le azioni e/o misure opportune per impedire il perdurare di tale uso illecito della Rete, ivi inclusa l'eventuale sospensione (in via temporanea o definitiva) dell'accesso alla Rete e il rivalersi per eventuali danni cagionati, se del caso, anche per mezzo dell'Azienda con la quale è stato sottoscritto l'accordo di distacco.

L'utente sarà in ogni caso l'unico soggetto responsabile dell'accesso alla Rete tramite connessione remota e, pertanto, si impegna a tenere indenne e manlevare la Società da qualsiasi danno, reclamo, costo e/o pretesa da chiunque avanzato in relazione all'attività svolta per conto della Società, restando inteso che l'utente sarà, altresì, tenuto, ove correr possa, a risarcire la Società di tutti i danni eventualmente subiti a seguito di tali predette richieste.

12 Monitoraggio, verifica della conformità e audit

Il gruppo DGS si riserva il diritto di monitorare e verificare le attività dei propri Fornitori al fine di garantire il rispetto dei requisiti stabiliti dal presente Codice di Condotta. Queste attività di controllo sono parte integrante della gestione dei rapporti contrattuali e mirano ad assicurare l'aderenza agli standard etici, legali e tecnici richiesti.

12.1 Tipologie di verifiche

Le attività di monitoraggio e verifica, svolte da auditor interni o enti certificatori terzi con frequenza almeno annuale, possono includere, ma non si limitano a:

- **Audit periodici:** il gruppo DGS o enti terzi incaricati condurranno controlli regolari per accertare la conformità dei Fornitori alle normative applicabili, agli standard internazionali e alle disposizioni contrattuali.
- **Valutazioni documentali:** i Fornitori devono produrre tutta la documentazione necessaria per dimostrare l'implementazione delle misure previste, incluse certificazioni, rapporti di conformità e politiche interne.
- **Ispezioni in loco:** sopralluoghi presso i siti produttivi, logistici o amministrativi per verificare direttamente l'aderenza agli standard di sicurezza, sostenibilità, etica e qualità.
- **Verifiche specifiche su tecnologie e dati:** controlli sui sistemi di gestione delle tecnologie avanzate, inclusa l'intelligenza artificiale, e sui processi di trattamento dei dati personali per garantire il rispetto delle normative applicabili.

12.2 Ambiti oggetto di audit

Gli audit possono riguardare, a titolo esemplificativo:

- **Salute e sicurezza sul lavoro:** verifica delle condizioni di sicurezza dei dipendenti e delle misure preventive adottate.
- **Responsabilità sociale:** accertamento del rispetto dei diritti umani e delle condizioni lavorative, in conformità agli standard SA8000.
- **Protezione dei dati personali:** controlli sui sistemi di gestione dei dati personali per assicurare il rispetto del GDPR, dello standard ISO/IEC 27701 e delle disposizioni incluse nei Data Processing Agreement (DPA) sottoscritti.
- **Sostenibilità ambientale:** valutazione dell'adozione di pratiche sostenibili e della conformità agli obiettivi di riduzione dell'impatto ambientale, come l'ottimizzazione delle risorse naturali e la gestione dei rifiuti.
- **Prevenzione della corruzione:** verifica dell'implementazione di politiche e procedure anticorruzione, in linea con la ISO 37001 e con la normativa vigente.

12.3 Gestione delle non conformità

In caso di rilevamento di non conformità durante le attività di verifica:

1. Verrà richiesto al Fornitore di presentare un **piano di azione correttiva** entro un termine specifico.
2. Il gruppo DGS monitorerà l'attuazione delle azioni correttive e valuterà i risultati ottenuti.
3. Se le criticità non saranno risolte entro i tempi stabiliti, il gruppo potrà adottare provvedimenti in linea con quanto indicato al successivo capitolo 13.

12.4 Collaborazione del Fornitore

I Fornitori sono obbligati a:

- Garantire pieno accesso ai dati, ai documenti e ai siti produttivi rilevanti per le attività di verifica.
- Facilitare la comunicazione con i rappresentanti del gruppo DGS o degli enti terzi incaricati.
- Assicurare la disponibilità del personale responsabile delle aree oggetto di controllo.

12.5 Audit su Subfornitori

Qualora il Fornitore si avvalga di Subfornitori, dovrà garantire che anche questi ultimi rispettino gli standard stabiliti dal presente Codice di Condotta. Il gruppo DGS si riserva il diritto di condurre audit diretti sui Subfornitori o di richiedere documentazione comprovante la loro conformità.

12.6 Impegno alla trasparenza

Il gruppo DGS adotta un approccio di trasparenza e collaborazione con i Fornitori, comunicando tempestivamente i risultati degli audit e supportando il Fornitore nell'attuazione delle azioni necessarie per garantire la conformità agli standard richiesti.

13 Sanzioni e conseguenze delle violazioni

Il mancato rispetto dei principi e delle disposizioni contenute nel presente Codice di Condotta comporta gravi conseguenze per i Fornitori, in linea con l'impegno del gruppo DGS a mantenere elevati standard etici, legali e operativi nella propria catena di approvvigionamento.

- **Esclusione dall'Albo fornitori:** i Fornitori che non rispettano i requisiti delineati nel Codice di Condotta saranno esclusi dall'Albo fornitori "jAlbo". Tale esclusione è **definitiva** salvo diversa indicazione da parte del gruppo DGS, che potrà valutare eventuali richieste di riammissione solo a seguito dell'attuazione di piani di miglioramento documentati e verificabili.
- **Risoluzione del contratto:** in caso di violazioni gravi o reiterate, il gruppo DGS si riserva il diritto di risolvere immediatamente i contratti in essere con i Fornitori interessati, senza alcun obbligo di preavviso e senza incorrere in responsabilità legali o contrattuali. Il gruppo DGS si riserva inoltre il diritto di chiedere il risarcimento dei danni subiti. La risoluzione del contratto sarà notificata formalmente e motivata sulla base delle violazioni rilevate.
- **Segnalazione alle autorità:** qualora si riscontrino comportamenti che configurino reati o violazioni normative, il gruppo DGS procederà con la segnalazione alle autorità competenti. Ciò include, ma non si limita a, casi di corruzione, frode, lavoro minorile, sfruttamento lavorativo, violazioni delle normative sulla sicurezza e inadempienze in materia di protezione dei dati personali.

Tutte le sanzioni applicate saranno documentate e comunicate al Fornitore interessato, con indicazione chiara delle motivazioni e delle azioni richieste per sanare eventuali criticità. Il gruppo DGS si impegna a gestire tali comunicazioni in modo riservato, limitando la divulgazione delle informazioni alle sole parti interessate.

Dichiarazione di impegno e conformità

Con l'accettazione del presente Codice di condotta dei Fornitori del gruppo DGS (**PL-08-14**), il Fornitore dichiara formalmente quanto segue:

- Presa visione e accettazione del Codice Etico.** Il Fornitore dichiara di avere preso atto del **Codice Etico** adottato dal gruppo DGS, consultabile sul sito internet ufficiale del gruppo DGS all'indirizzo <https://www.dgsspa.com/wp-content/uploads/2024/12/Codice-Etico-Gruppo-DGS.pdf> e di impegnarsi a rispettare e diffondere tali principi presso i propri dipendenti, collaboratori e Subfornitori.
- Presa visione e accettazione del MOGC e della Politica Anticorruzione.** Il Fornitore accetta il **Modello di Organizzazione, Gestione e Controllo (MOGC)** ai sensi del Decreto Legislativo 231/2001, nonché la **Politica Anticorruzione** del gruppo DGS, consultabile sul sito internet ufficiale del gruppo DGS all'indirizzo: <https://www.dgsspa.com/chi-siamo/governance-e-compliance/modello-organizzativo-231-01-e-codice-etico/>
impegnandosi a rispettarne pienamente i principi e le prescrizioni e a farli rispettare anche da eventuali Subfornitori. Il Fornitore si impegna inoltre a collaborare attivamente durante eventuali verifiche o richieste di audit relative all'applicazione di tali normative, anche nei confronti dei Subfornitori.
- Responsabilità sociale.** Il Fornitore si impegna a rispettare i seguenti principi cardine della **Responsabilità sociale**:
 - Divieto di lavoro minorile e forzato, garantendo il rispetto delle normative locali e internazionali in materia.
 - Promozione di condizioni di lavoro dignitose e sicure, attraverso l'adozione di misure preventive e di protezione adeguate.
 - Divieto di impiego di manodopera in condizioni di sfruttamento o approfittando del loro stato di bisogno.
 - Pari opportunità e non discriminazione, assicurando trattamenti equi e politiche di inclusione per tutti i lavoratori.
 - Rispetto dei diritti umani fondamentali in tutte le operazioni aziendali, inclusa la protezione dei diritti dei lavoratori nelle catene di approvvigionamento.
- Aggiornamento delle informazioni fornite.** Il Fornitore si impegna a mantenere veritiere e aggiornate le informazioni trasmesse con la presente dichiarazione, per tutta la durata della permanenza nell'**Albo Fornitori del gruppo DGS** ("jAlbo"). Qualsiasi variazione significativa delle informazioni fornite dovrà essere comunicata tempestivamente al gruppo DGS.
- Conformità al Decreto Legislativo 231/2001.** Il Fornitore dichiara che:
 - Nei suoi confronti **NON** è stata emessa sentenza di condanna passata in giudicato ai sensi del Decreto Legislativo 231/2001.
 - Nei suoi confronti **NON** è in corso alcun procedimento ai sensi del Decreto Legislativo 231/2001.
 - Nei confronti delle persone fisiche che lo rappresentano **NON** sono state pronunciate sentenze di condanna passate in giudicato e/o **NON** sono in corso procedimenti penali per uno dei reati previsti dal Decreto Legislativo 231/2001.
- Dichiarazione sui collegamenti con Paesi e controparti non cooperativi.** Il Fornitore dichiara:
 - di **NON** avere sede o residenza, ovvero alcun collegamento con Paesi considerati non cooperativi dal **Gruppo di Azione Finanziaria Internazionale (GAFI)** o classificati come "paradisi fiscali" da organismi nazionali e/o internazionali riconosciuti (es. Agenzia delle Entrate, OCSE).

- Che l'azienda del Fornitore **NON** risulta inserita nelle liste pubblicate da organismi nazionali e/o internazionali riconosciuti (es. ONU, UE, OFAC) nel contesto del sistema di prevenzione e contrasto al finanziamento del terrorismo.
7. **Impegno a supportare verifiche e audit.** Il Fornitore si impegna a fornire piena collaborazione durante le attività di monitoraggio, verifica o audit condotte dal gruppo DGS o da enti terzi incaricati, assicurando la trasparenza e l'accesso a documenti, dati e siti produttivi rilevanti. Il Fornitore si impegna a garantire i medesimi obblighi anche nei confronti dei Subfornitori.
8. **Adesione ai principi di sostenibilità ambientale.** Il Fornitore si impegna a promuovere pratiche sostenibili, incluse:
- La riduzione delle emissioni di CO₂ e l'ottimizzazione dell'utilizzo delle risorse naturali.
 - La gestione responsabile dei rifiuti e l'adozione di politiche di riciclo.
 - L'integrazione di criteri ambientali nella selezione dei materiali e nei processi produttivi.

Il Fornitore accetta il presente Codice di Condotta nella sua interezza ed espressamente quanto previsto dai § 6, 7, 10 e 11, riconoscendo che il mancato rispetto di quanto dichiarato potrà comportare l'esclusione immediata dall'Albo fornitori, la risoluzione dei contratti in essere e ulteriori azioni legali, ove applicabili.

Il Fornitore si impegna altresì a segnalare prontamente all'Ufficio Acquisti del gruppo DGS qualsiasi Non Conformità relativa ai temi trattati nel presente Codice di Condotta, tramite i canali previsti in via contrattuale o di quelli di cui al § 4.2, in particolare rispetto alle tematiche della Salute e Sicurezza, Responsabilità Sociale e della Sostenibilità.

PER ACCETTAZIONE

Ragione sociale _____
Nome e Cognome _____
Ruolo _____

Firma

FINE DEL DOCUMENTO