

PARTE SPECIALE

- | -

DELITTI IN VIOLAZIONE DEL DIRITTO D'AUTORE

Versione approvata dal Consiglio di Amministrazione in data 14 settembre 2022



PARTE SPECIALE “I” – DELITTI IN VIOLAZIONE DEL DIRITTO D’AUTORE

I.1 Le tipologie dei delitti in violazione del diritto d’autore (art. 25-novies del Decreto)

La Legge n. 99/2009 ha disposto (con l'art. 15, comma 7, lettera c) l'introduzione nel Decreto dell'art. 25-novies - successivamente modificato con la L. 116/2009 e con il d.lgs. 121/2011 – in materia di delitti in violazione del diritto d’autore. Nel seguito si riporta una breve descrizione dei reati ivi contemplati, suddivisi tra:

- reati potenzialmente realizzabili;
- reati la cui commissione, per quanto non si possano escludere del tutto, è stata ritenuta remota in considerazione delle attività svolte dalla Società ed in ogni caso ragionevolmente gestita dal rispetto dei principi etici e delle regole comportamentali enunciate nel Codice Etico adottato dalla Società; nonché reati la cui commissione risulta non ipotizzabile.

REATO	RIFERIMENTO	REALIZZABILITÀ
<i>File sharing e Upload/download</i>	art. 171, comma 1, lett. a-bis) e comma 3 L. 633/1941-	possibile
<i>Underlicensing e Hard disk loading</i>	art. 171-bis L. 633/1941	possibile
Duplicazione, riproduzione, trasmissione o diffusione abusiva in pubblico di un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio	art. 171-ter L. 633/1941	remota
Violazioni nei confronti della SIAE	art. 171-septies L. 633/1941	remota
Distribuzione e installazione di dispositivi di decodificazione per l'accesso a un servizio criptato, senza pagamento del canone	art. 171-octies L. 633/1941	non ipotizzabile



I reati che sono stati considerati potenzialmente realizzabili sono i seguenti:

Art. 171, comma 1, lett. a-bis) e comma 3 L. 633/1941- File sharing e Upload/download

“1. Salvo quanto previsto dall'art. 171-bis e dall'art. 171-ter, è punito con la multa da euro 51 a euro 2.065 chiunque, senza averne diritto, a qualsiasi scopo e in qualsiasi forma:

a) riproduce, trascrive, recita in pubblico, diffonde, vende o mette in vendita o pone altrimenti in commercio un'opera altrui o ne rivela il contenuto prima che sia reso pubblico, o introduce e mette in circolazione nel regno esemplari prodotti all'estero contrariamente alla legge italiana;

a-bis) mette a disposizione del pubblico, immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta, o parte di essa;

b) rappresenta, esegue o recita in pubblico o diffonde con o senza variazioni od aggiunte, una opera altrui adatta a pubblico spettacolo od una composizione musicale. La rappresentazione o esecuzione comprende la proiezione pubblica dell'opera cinematografica, l'esecuzione in pubblico delle composizioni musicali inserite nelle opere cinematografiche e la radiodiffusione mediante altoparlante azionato in pubblico;

c) compie i fatti indicati nelle precedenti lettere mediante una delle forme di elaborazione previste da questa legge;

d) riproduce un numero di esemplari o esegue o rappresenta un numero di esecuzioni o di rappresentazioni maggiore di quello che aveva il diritto rispettivamente di produrre o di rappresentare;

e) in violazione dell'art. 79 ritrasmette su filo o per radio o registra in dischi fonografici o altri apparecchi analoghi le trasmissioni o ritrasmissioni radiofoniche o smercia i dischi fonografici o altri apparecchi indebitamente registrati.

2. Chiunque commette la violazione di cui al primo comma, lettera a-bis), è ammesso a pagare, prima dell'apertura del dibattimento, ovvero prima dell'emissione del decreto penale di condanna, una somma corrispondente alla metà del massimo della pena stabilita dal primo comma per il reato commesso, oltre le spese del procedimento. Il pagamento estingue il reato.

3. La pena è della reclusione fino ad un anno o della multa non inferiore a euro 516 se i reati di cui sopra sono commessi sopra un'opera altrui non destinata alla pubblicazione, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera medesima, qualora ne risulti offesa all'onore od alla reputazione dell'autore.

4. La violazione delle disposizioni di cui al terzo ed al quarto comma dell'articolo 68 comporta la sospensione della attività di fotocopia, xerocopia o analogo sistema di riproduzione da sei mesi ad un anno nonché la sanzione amministrativa pecuniaria da euro 1.032 a euro 5.164.”

L'art. 171, comma 1, lett. a bis) si riferisce alle attività di *File sharing* (condivisione o scambio di file in violazione della normativa del diritto d'autore e, comunque, al di fuori degli ordinari e leciti circuiti commerciali dei beni oggetto di proprietà intellettuale) e di *Upload/download* di documentazione (immissione o condivisione, senza averne diritto, di contenuti protetti da diritti d'autore in un sistema di reti telematiche). Il comma 3 dell'art. 171, si riferisce, invece, alle attività di riproduzione, messa a disposizione, diffusione, vendita, rappresentazione di un'opera altrui non destinata alla pubblicazione.

Art. 171-bis L. 633/1941 - Underlicensing e Hard disk loading

“1. Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o



concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

2. Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità."

Il reato si riferisce alle attività di *Underlicensing* (violazioni delle condizioni di licenza di un software), di *Hard disk loading* (vendita e relativo acquisto per l'azienda di computer sui quali sono installati software piratati) e di utilizzazione non autorizzata di banche dati.

* * *

I reati la cui commissione è stata ritenuta remota o non ipotizzabile sono i seguenti:

Art. 171-ter L. 633/1941

"1. È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 chiunque a fini di lucro:

a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;

b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;

c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);

d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;

e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;



f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto;

f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;

h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102-quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.

2. È punito con la reclusione da uno a quattro anni e con la multa da euro 2.582 a euro 15.493 chiunque:

a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;

a-bis) in violazione dell'articolo 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;

b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1;

c) promuove o organizza le attività illecite di cui al comma 1.

3. La pena è diminuita se il fatto è di particolare tenuità.

4. La condanna per uno dei reati previsti nel comma 1 comporta:

a) l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;

b) la pubblicazione della sentenza ai sensi dell'articolo 36 del codice penale;

c) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.

5. Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici."

Il reato si riferisce alle attività di duplicazione, riproduzione, trasmissione o diffusione abusiva in pubblico con qualsiasi procedimento, in tutto o in parte, di un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio.

Art. 171-septies L. 633/1941

"1. La pena di cui all'articolo 171-ter, comma 1, si applica anche:

a) ai produttori o importatori dei supporti non soggetti al contrassegno di cui all'articolo 181-bis, i quali non comunicano alla SIAE entro trenta giorni dalla data di immissione in commercio sul



territorio nazionale o di importazione i dati necessari alla univoca identificazione dei supporti medesimi;

b) salvo che il fatto non costituisca più grave reato, a chiunque dichiari falsamente l'avvenuto assolvimento degli obblighi di cui all'articolo 181-bis, comma 2, della presente legge.”

La pena di cui all'articolo 171-ter, comma 1, si applica anche alle violazioni nei confronti della SIAE.

Art. 171-octies L. 633/1941

“1. Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 25.822 chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

2. La pena non è inferiore a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.”

Il reato si riferisce alle attività di distribuzione e installazione di dispositivi di decodificazione per l'accesso a un servizio criptato, senza pagamento del canone.

I.2 Attività a Rischio Reato

L'attività a rischio reato rappresenta “un'attività riferita ad uno o più processi aziendali, nel cui ambito si potrebbero in linea di principio configurare le condizioni, le occasioni o i mezzi per la commissione di reati, anche in via strumentale alla concreta realizzazione della fattispecie”. Nell'ambito del Risk assessment integrato (RAI) - svolto dalle strutture interne competenti ed aggiornato annualmente, anche attraverso interviste alle risorse delle Divisioni/Aree interessate, a conoscenza dello specifico ambito analizzato - sono individuate tutte le attività a rischio reato inerenti la presente parte speciale e riferite ai macro-processi ed ai processi aziendali.

Le aree di attività ritenute più specificamente a rischio ai fini della presente Parte speciale “I”, sono:

Rif. Rischio	Attività a rischio reato	Descrizione rischio	Reati
R_84	Gestione contenuti sito portale acquisti	Mancata, non corretta gestione dei contenuti del portale acquisti: - al fine di omettere la diffusione di dati/informazioni in violazione degli obblighi in materia di trasparenza; - al fine di diffondere	- File sharing e Upload/download (art. 171, comma 1, lett. a-bis) e comma 3 L. 633/1941)



Rif. Rischio	Attività a rischio reato	Descrizione rischio	Reati
		dati/informazioni non corrette o riservate; - diffondendo abusivamente opere dell'ingegno protette	
R_85	Gestione contenuti sito internet / intranet	Mancata, non corretta gestione dei contenuti del sito internet della Società e/o della Intranet aziendale: - al fine di omettere la diffusione di dati/informazioni in violazione degli obblighi in materia di trasparenza; - al fine di diffondere dati/informazioni non corrette o riservate; - diffondendo abusivamente opere dell'ingegno protette	- <i>File sharing e Upload/download (art. 171, comma 1, lett. a-bis) e comma 3 L. 633/1941)</i>
R_194	Gestione banche dati e software aziendali	Abusiva duplicazione o detenzione di programmi per elaboratori o illecito utilizzo di banche dati, con lo scopo di: - consentire un risparmio alla Società in termini di costi legati al mancato acquisto di prodotti informatici o banche dati muniti di regolare licenza	- <i>Underlicensing e Hard disk loading (art. 171-bis L. 633/1941)</i>
R_207	Gestione attività testata registrata	Gestione impropria delle pubblicazioni effettuate in qualità di testata registrata, diffondendo/utilizzando impropriamente opere di ingegno protette (es. con i quaderni Consip)	- <i>File sharing e Upload/download (art. 171, comma 1, lett. a-bis) e comma 3 L. 633/1941)</i>

Per i dettagli inerenti l'evento di rischio ed i presidi di controllo si rimanda alle schede di rischio, elaborate per le singole attività, nelle quali sono dettagliatamente indicati:

- ✓ **Anagrafica evento rischio:** (i) Risk owner, contributor; (ii) Macro processo, Processo e Fase; (iii) Area e Sotto Area;
- ✓ **Dettaglio rischio:** (iv) Fattori abilitanti; (v) Conseguenze; (vi) Riferimenti normativa esterna ed interna; (vii) Anomalie significative; (viii) KRI; (ix) Indicatori di rischio;
- ✓ **Controlli:** (x) Sintesi misure di controllo; (xi) Misure generali; (xii) Misure specifiche.

I.3 Principi di comportamento

Al fine di prevenire i reati sopra enunciati, tutti i destinatari devono rispettare, oltre i principi di comportamento già previsti ed espressi nel Codice Etico, anche quelli riportati nei documenti



organizzativi adottati dalla Società, nonché tenere comportamenti conformi a quanto previsto dalle vigenti norme di legge. Inoltre i Destinatari del Modello, competenti per le attività oggetto di regolamentazione della presente Parte speciale, sono tenuti ad osservare i seguenti ulteriori principi:

- assicurare il regolare funzionamento delle attività di competenza;
- garantire l'attuazione del principio di segregazione dei compiti e delle funzioni anche attraverso la predisposizione di specifiche procedure;
- garantire la tracciabilità e la documentabilità di tutte le operazioni effettuate, prevedendo specifici obblighi di archiviazione;
- garantire che le attività a rischio prevedano i necessari controlli gerarchici, che devono essere tracciati/documentati;
- garantire la piena collaborazione agli organi di controllo e alla Divisione Internal audit nell'ambito degli audit/controlli inseriti nel PIC, oltre che nell'ambito di eventuali indagini/accertamenti da parte di organi esterni;
- garantire la corretta applicazione del Sistema disciplinare, in caso di mancato rispetto dei principi e dei protocolli contenuti nel Modello;
- assicurare la corretta gestione dei contenuti dei siti internet impiegati e della intranet aziendale;
- assicurare la corretta gestione delle attività svolte in qualità di testata registrata;
- definire e comunicare a tutti i dipendenti e collaboratori le modalità di comportamento che debbono essere assunte per un corretto e lecito utilizzo dei software e delle banche dati in uso;
- controllare periodicamente la regolarità delle licenze dei prodotti in uso e procedendo, ove necessario, ai rinnovi;
- censire i prodotti in uso su ciascuna postazione.

In generale, è fatto dunque divieto ai Destinatari del Modello di porre in essere comportamenti che possano rientrare, anche potenzialmente, nelle fattispecie di reato richiamate dall'art. 25-novies d.lgs. 231/2001, ovvero di collaborare o dare causa alla relativa realizzazione. Nell'ambito dei citati comportamenti è dunque fatto divieto, in particolare, di:

- violare i principi previsti nella presente Parte Speciale e tutti quelli previsti ed espressi nella Parte Speciale B- Reati Informatici, cui si fa integrale rimando;
- procedere all'installazione di prodotti software sul personal computer che gli è stato assegnato, in violazione degli accordi contrattuali di licenza d'uso e, in generale, di tutte le leggi ed i regolamenti che disciplinano e tutelano la licenza d'uso;
- utilizzare software e/o banche dati in assenza di valida licenza, anche nel caso in cui la stessa sia solamente scaduta;
- diffondere immagini, documenti o altro materiale tutelato dalla normativa in materia di diritto d'autore, tramite mezzi di comunicazione aziendali, tra cui, in particolare, il sito internet aziendale e la intranet.



I.4 Owner del rischio: referente aziendale

Sulla base della metodologia adottata per la costruzione del Modello, fondata sull'analisi dei processi per rischio-reato, ciascun referente aziendale è responsabile dell'effettiva applicazione delle attività di controllo poste in essere per la prevenzione dei reati previsti dal Decreto che, a livello teorico, è possibile siano commessi dai dipendenti di Consip, come riportato nell'Allegato "Matrice Rischio reato/referenti".

Tali referenti sono individuati nei responsabili delle Divisioni aziendali/Aree coinvolte in ciascuna area a rischio-reato individuata.

I.5 Presidi di controllo e ruolo dell'Organismo di Vigilanza

Al fine di mitigare i rischi connessi alla realizzazione delle fattispecie di reato previste dal Decreto, la Società, nell'ambito del sistema di presidi di controllo, prevede l'attività di monitoraggio dell'Organismo di Vigilanza, che vigila sulla efficacia del Modello e sul rispetto delle prescrizioni ivi contenute.

L'OdV, nello svolgimento delle proprie funzioni, ha la facoltà, ove lo ritenga opportuno, di verificare il rispetto dei canoni comportamentali e dei protocolli aziendali da parte dei Destinatari, oltre che di richiedere tutte le informazioni e la documentazione ritenute necessarie per tali attività. A tal fine, l'OdV riceve anche appositi flussi informativi dalle strutture aziendali individuate sia nel Modello e relative Parti speciali, sia nelle procedure aziendali di riferimento.

Le attività di controllo sono condotte in un'ottica di integrazione e di coordinamento tra gli organi di controllo (Collegio sindacale - OdV – RPCT – DPO – GSOS); viene pertanto definito annualmente il Piano Integrato dei Controlli correttamente bilanciato tra i vari organi, che tiene conto degli audit effettuati dall'Internal Audit e delle verifiche verticali effettuate dai diversi organi di controllo, alternando la tipologia di analisi; tale Piano prevede una gestione integrata delle raccomandazioni e dei follow-up nonché controlli ciclici dei maggiori centri di rischio.

R.84

ANAGRAFICA EVENTO RISCHIO											
Codice rischio	84	Attività	Gestione contenuti portale acquisti	Descrizione Rischio	Mancata, non corretta gestione dei contenuti del portale acquisti: - al fine di omettere la diffusione di dati/informazioni in violazione degli obblighi in materia di trasparenza; - al fine di diffondere dati/informazioni non corrette o riservate; - diffondendo abusivamente opere dell'ingegno protette						
Risk-owner	→ DPGSA- Marketing e Customer Experience → DEPSI – Area Cybersecurity e Infrastrutture		Contributor	//	<table border="1"> <tr> <td>Macro-Processo</td> <td>Supporto Iniziative e Customer Care</td> </tr> <tr> <td>Processo</td> <td>Promozione e CRM</td> </tr> <tr> <td>Fase</td> <td>Gestione contenuti portale</td> </tr> </table>	Macro-Processo	Supporto Iniziative e Customer Care	Processo	Promozione e CRM	Fase	Gestione contenuti portale
Macro-Processo	Supporto Iniziative e Customer Care										
Processo	Promozione e CRM										
Fase	Gestione contenuti portale										
Area	Generale Affidamento di lavori, servizi e forniture		Sotto Area	//							
DETTAGLIO RISCHIO											
Fattori abilitanti	<ul style="list-style-type: none"> ✓ Scarsa proceduralizzazione del processo ✓ Esercizio prolungato ed esclusivo di responsabilità di una fase da parte di uno o pochi soggetti ✓ Errore operativo ✓ Accordi illeciti ✓ Eccesso di discrezionalità da parte di un singolo soggetto ✓ Mancato rispetto delle regole procedurali interne ✓ Mancato/ errato recepimento della normativa di settore ✓ Assenza controlli 			Conseguenze	<ul style="list-style-type: none"> ✓ perdita economica ✓ danno erariale ✓ sanzioni ✓ inefficienza ✓ contenzioso ✓ danno reputazionale 						
Riferimenti normativa esterna	<ul style="list-style-type: none"> • L. n. 190/2012 • D.Lgs. n. 33/2013 • D.Lgs. n. 231/2001 • DL n. 32/2019 • D.Lgs. n. 50/2016 • GDPR • L.633/41 e s.m.i. • D.Lgs. 35/2005 		Riferimenti normativa interna	<ul style="list-style-type: none"> ○ Modalità operative per la gestione del portale degli Acquisti in rete PA ○ Politica per la classificazione delle informazioni ○ Procedura per la gestione degli aspetti di sicurezza nel ciclo di vita delle informazioni 							
Anomalie significative	//		KRI	//	Indicatori di rischio	//					

CONTROLLI	
Sintesi misure di controllo	
<ul style="list-style-type: none"> ✓ Politiche di gestione del rischio (MOG/PTPC/CE) ✓ Politiche di gestione del rischio privacy ✓ Segregazione compiti/funzioni ✓ Controlli gerarchici ✓ Audit/ Controlli ✓ Sistema deleghe/procure ✓ Tracciabilità del processo ✓ Archiviazione documentazione rilevante 	<ul style="list-style-type: none"> ✓ Rotazione ✓ Flussi informativi ✓ Informatizzazione processo ✓ Formazione ✓ Whistleblowing ✓ Sistema disciplinare ✓ Sistema procedurale interno ✓ Accesso civico
Misure generali	Misure specifiche
<p>La Società si è dotata:</p> <ul style="list-style-type: none"> - PTPC, Codice etico e Modello ex D.Lgs. 231/2001 - Sistema Privacy Consip, che disciplina le modalità di trattamento dei dati, le figure che operano in tale ambito e gli obblighi cui sono soggetti i destinatari del Sistema stesso - Sistema disciplinare interno finalizzato a sanzionare il mancato rispetto del sistema procedurale interno e dei principi contenuti nel PTPC, del Codice etico e del Modello ex D.Lgs. 231/2001 - Regolamento per la gestione dell'accesso civico semplice e generalizzato - Piano Integrato dei Controlli - Sistema di whistleblowing - Flussi informativi vs organi di controllo sia periodici che ad evento - Piano integrato di Formazione (d.lgs 231/2001, L. 190/12, d.lgs. 231/07 e GDPR) - Piano Pluriennale di rotazione 	<ul style="list-style-type: none"> - La società si è dotata di una procedura interna che disciplina le modalità operative per la gestione del portale degli Acquisti in rete PA, elaborata nel rispetto della segregazione dei compiti e delle funzioni - per ciascuna fase sono individuati (i) i ruoli e le responsabilità di tutti i soggetti coinvolti; (ii) i controlli gerarchici nell'ambito dell'autorizzazione al pagamento, sia da parte del responsabile di Area che del responsabile di Divisione, che prevede <ul style="list-style-type: none"> o un gruppo di lavoro (Redazione Portale) che redige i testi per l'aggiornamento del Portale, in base alle informazioni pervenute dalle Divisioni detentrici del dato/informazione, che sono responsabili dei contenuti trasmessi o condivisione dei testi con gli owner dell'informazione
PIANI D'AZIONE SUGGERITI	
//	

SCORING PER FAMIGLIA DI RISCHIO														
190/12			231/ 01			50/16			Trasparenza			Privacy		
Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo
MEDIO ALTO	ADEGUATO	MOLTO BASSO	MEDIO ALTO	ADEGUATO	MOLTO BASSO	MEDIO ALTO	ADEGUATO	MOLTO BASSO	ALTO	ADEGUATO	BASSO	ALTO	ADEGUATO	BASSO

SCORING PER FAMIGLIA DI RISCHIO														
262/ 05			Sicurezza informazioni			Sicurezza fisica			AML			Rischio operativo		
Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo
												ALTO	ADEGUATO	BASSO

SCORING COMPLESSIVO					
Scoring Inerente complessivo			Scoring Residuo complessivo		
Minimo	Medio	Massimo	Minimo	Medio	Massimo
MEDIO ALTO	ALTO	ALTO	MOLTO BASSO	BASSO	BASSO

R.85

ANAGRAFICA EVENTO RISCHIO					
Codice rischio	85	Attività	Gestione contenuti sito internet / intranet	Descrizione Rischio	<p>Mancata, non corretta gestione dei contenuti del sito internet della Società e/o della Intranet aziendale:</p> <ul style="list-style-type: none"> - al fine di omettere la diffusione di dati/informazioni in violazione degli obblighi in materia di trasparenza; - al fine di diffondere dati/informazioni non corrette o riservate; - diffondendo abusivamente opere dell'ingegno protette
Risk-owner	→ DEPSI – Area Cybersecurity Infrastrutture → DRC - Comunicazione	Contributor	//	Macro-Processo	Servizi di funzionamento
				Processo	Comunicazione
				Fase	Gestione sito istituzionale – Comunicazione interna
Area	Generale		Sotto Area	Generale	
DETTAGLIO RISCHIO					
Fattori abilitanti	<ul style="list-style-type: none"> ✓ Scarsa procedimentalizzazione del processo ✓ Esercizio prolungato ed esclusivo di responsabilità di una fase da parte di uno o pochi soggetti ✓ Errore operativo ✓ Accordi illeciti ✓ Eccesso di discrezionalità da parte di un singolo soggetto ✓ Mancato rispetto delle regole procedurali interne ✓ Mancato/ errato recepimento della normativa di settore ✓ Assenza controlli 			Conseguenze	<ul style="list-style-type: none"> ✓ perdita economica ✓ danno erariale ✓ sanzioni ✓ inefficienza ✓ contenzioso ✓ danno reputazionale
Riferimenti normativa esterna	<ul style="list-style-type: none"> • L. n. 190/2012 • D.Lgs. n. 33/2013 • D.Lgs. n. 231/2001 • DL n. 32/2019 • D.Lgs. n. 50/2016 • GDPR • L.633/41 e s.m.i. • D.Lgs. 35/2005 	Riferimenti normativa interna	<ul style="list-style-type: none"> ○ Politica per la classificazione delle informazioni ○ Procedura per la gestione degli aspetti di sicurezza nel ciclo di vita delle informazioni 		
Anomalie significative	//	KRI	//	Indicatori di rischio	//

CONTROLLI	
Sintesi misure di controllo	
<ul style="list-style-type: none"> ✓ Politiche di gestione del rischio (MOG/PTPC/CE) ✓ Politiche di gestione del rischio privacy ✓ Segregazione compiti/funzioni ✓ Controlli gerarchici ✓ Audit/ Controlli ✓ Sistema deleghe/procure ✓ Tracciabilità del processo ✓ Archiviazione documentazione rilevante 	<ul style="list-style-type: none"> ✓ Rotazione ✓ Flussi informativi ✓ Informatizzazione processo ✓ Formazione ✓ Whistleblowing ✓ Sistema disciplinare ✓ Sistema procedurale interno ✓ Accesso civico
Misure generali	Misure specifiche
<p>La Società si è dotata:</p> <ul style="list-style-type: none"> - PTPC, Codice etico e Modello ex D.Lgs. 231/2001 - Sistema Privacy Consip, che disciplina le modalità di trattamento dei dati, le figure che operano in tale ambito e gli obblighi cui sono soggetti i destinatari del Sistema stesso - Sistema disciplinare interno finalizzato a sanzionare il mancato rispetto del sistema procedurale interno e dei principi contenuti nel PTPC, del Codice etico e del Modello ex D.Lgs. 231/2001 - Regolamento per la gestione dell'accesso civico semplice e generalizzato - Piano Integrato dei Controlli - Sistema di whistleblowing - Flussi informativi vs organi di controllo sia periodici che ad evento - Piano integrato di Formazione (d.lgs 231/2001, L. 190/12, d.lgs. 231/07 e GDPR) - Piano Pluriennale di rotazione 	<ul style="list-style-type: none"> - I contenuti del sito internet della Società sono gestiti dalla DRC- nello specifico sul sito vengono effettuate 2 tipi di pubblicazioni: (i) obbligatorie in base alle norme di legge, le cui modalità (owner - contenuti - tempistiche) sono disciplinati del PTPC; (ii) prodotti elaborati dalla DRC, per i quali vi è la supervisione del resp. gerarchico Non vengono generalmente utilizzati contenuti di terzi: laddove ve ne fosse la necessità, viene effettuato un controllo con la DAL - La Intranet aziendale è gestita in modo analogo al sito internet ma non è soggetta ai medesimi adempimenti normativi dovuti all'elaborazione di comunicazioni esterne
PIANI D'AZIONE SUGGERITI	
//	

SCORING PER FAMIGLIA DI RISCHIO														
190/12			231/ 01			50/16			Trasparenza			Privacy		
Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo
MEDIO ALTO	ADEGUATO	MOLTO BASSO	MEDIO ALTO	ADEGUATO	MOLTO BASSO	MEDIO ALTO	ADEGUATO	MOLTO BASSO	ALTO	ADEGUATO	BASSO	ALTO	ADEGUATO	BASSO

SCORING PER FAMIGLIA DI RISCHIO														
262/ 05			Sicurezza informazioni			Sicurezza fisica			AML			Rischio operativo		
Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo
												ALTO	ADEGUATO	BASSO

SCORING COMPLESSIVO					
Scoring Inerente complessivo			Scoring Residuo complessivo		
Minimo	Medio	Massimo	Minimo	Medio	Massimo
MEDIO ALTO	ALTO	ALTO	MOLTO BASSO	BASSO	BASSO

ANAGRAFICA EVENTO RISCHIO											
Codice rischio	194	Attività	Gestione banche dati e software aziendali	Descrizione Rischio	Abusiva duplicazione o detenzione di programmi per elaboratori o illecito utilizzo di banche dati, con lo scopo di: - consentire un risparmio alla Società in termini di costi legati al mancato acquisto di prodotti informatici o banche dati muniti di regolare licenza						
Risk-owner	→ DEPSI – Area Cybersecurity e Infrastrutture/Area Pianificazione e analisi della domanda. → Tutte le risorse		Contributor	//	<table border="1"> <tr> <td>Macro-Processo</td> <td>Servizi di funzionamento</td> </tr> <tr> <td>Processo</td> <td>Sicurezza</td> </tr> <tr> <td>Fase</td> <td>Modello sicurezza logica</td> </tr> </table>	Macro-Processo	Servizi di funzionamento	Processo	Sicurezza	Fase	Modello sicurezza logica
Macro-Processo	Servizi di funzionamento										
Processo	Sicurezza										
Fase	Modello sicurezza logica										
Area	Specifico Gestione Sistemi Informativi		Sotto Area	Specifico Gestione software/ hardware							
DETTAGLIO RISCHIO											
Fattori abilitanti	<ul style="list-style-type: none"> ✓ Scarsa procedimentalizzazione del processo ✓ Esercizio prolungato ed esclusivo di responsabilità di una fase da parte di uno o pochi soggetti ✓ Errore operativo ✓ Accordi illeciti ✓ Eccesso di discrezionalità da parte di un singolo soggetto ✓ Mancato rispetto delle regole procedurali interne ✓ Assenza controlli 			Conseguenze	<ul style="list-style-type: none"> ✓ perdita economica ✓ danno erariale ✓ sanzioni ✓ inefficienza ✓ contenzioso ✓ danno reputazionale 						
Riferimenti normativa esterna	<ul style="list-style-type: none"> • L. n. 190/2012 • D.Lgs. n. 231/2001 • GDPR • D.Lgs. 196/2003 e s.m.i. • D.Lgs. 101/2018 Provvedimento Garante privacy su Amministratori di sistema 		Riferimenti normativa interna	<ul style="list-style-type: none"> ○ Modello organizzativo Privacy ○ Istruzioni Operative per le persone autorizzate al Trattamento dei dati personali ○ Istruzioni Operative per i Referenti Interni del trattamento dei dati personali ○ Gestione delle violazioni dei dati personali (data breach notification) ○ Regole aziendali per l'utilizzo del personal computer, posta elettronica ed internet 							
Anomalie significative	//	KRI	//	Indicatori di rischio	//						
CONTROLLI											
Sintesi misure di controllo											
<ul style="list-style-type: none"> ✓ Politiche di gestione del rischio (MOG/PTPC/CE) ✓ Politiche di gestione del rischio privacy ✓ Segregazione compiti/funzioni ✓ Controlli gerarchici ✓ Audit/ Controlli ✓ Sistema deleghe/procure ✓ Tracciabilità del processo ✓ Archiviazione documentazione rilevante 			<ul style="list-style-type: none"> ✓ Rotazione ✓ Flussi informativi ✓ Informatizzazione processo ✓ Formazione ✓ Whistleblowing ✓ Sistema disciplinare ✓ Sistema procedurale interno ✓ Accesso civico 								

Misure generali	Misure specifiche
<p>La Società si è dotata:</p> <ul style="list-style-type: none"> - PTPC, Codice etico e Modello ex D.Lgs. 231/2001 - Sistema Privacy Consip, che disciplina le modalità di trattamento dei dati, le figure che operano in tale ambito e gli obblighi cui sono soggetti i destinatari del Sistema stesso - Sistema disciplinare interno finalizzato a sanzionare il mancato rispetto del sistema procedurale interno e dei principi contenuti nel PTPC, del Codice etico e del Modello ex D.Lgs. 231/2001 - Regolamento per la gestione dell'accesso civico semplice e generalizzato - Piano Integrato dei Controlli - Sistema di whistleblowing - Flussi informativi vs organi di controllo sia periodici che ad evento - Piano integrato di Formazione (d.lgs 231/2001, L. 190/12, d.lgs. 231/07 e GDPR) - Programma pluriennale di rotazione 	<ul style="list-style-type: none"> - Nell'ambito del Sistema Privacy, è stato definito un Modello organizzativo nel rispetto della segregazione dei compiti e delle funzioni ed elaborate: <ul style="list-style-type: none"> o Istruzioni Operative per le persone autorizzate al Trattamento dei dati personali o Istruzioni Operative per i Referenti Interni del trattamento dei dati personali o Regole aziendali per l'utilizzo del personal computer, posta elettronica ed internet nell'ambito delle quali sono fornite specifiche regole di comportamento e divieti in ordine all'improprio utilizzo di software/banche dati (es. è vietato installare software, al di fuori di quelli già installati dall'azienda) - L'utilizzo delle licenze è gestito dalla DEPSI, che garantisce: <ul style="list-style-type: none"> o la tracciabilità dell'utilizzo delle risorse / licenze o la gestione degli asset
<p>PIANI D'AZIONE SUGGERITI</p>	
<p> </p>	

SCORING PER FAMIGLIA DI RISCHIO														
190/12			231/ 01			50/16			Trasparenza			Privacy		
Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo
MEDIO ALTO	ADEGUATO	MOLTO BASSO	ALTO	ADEGUATO	BASSO									

SCORING PER FAMIGLIA DI RISCHIO														
262/ 05			Sicurezza informazioni			Sicurezza fisica			AML			Rischio operativo		
Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo
												MEDIO ALTO	ADEGUATO	MOLTO BASSO

SCORING COMPLESSIVO					
Scoring Inerente complessivo			Scoring Residuo complessivo		
Minimo	Medio	Massimo	Minimo	Medio	Massimo
MEDIO ALTO	ALTO	ALTO	MOLTO BASSO	BASSO	BASSO

ANAGRAFICA EVENTO RISCHIO					
Codice rischio	207	Attività	Gestione attività testata registrata	Descrizione Rischio	Gestione impropria delle pubblicazioni effettuate in qualità di testata registrata, diffondendo/utilizzando impropriamente opere di ingegno protette (es. con i quaderni Consip)
Risk-owner	→ AD → DRC - Comunicazione	Contributor	- Tutte le Divisioni - DAL	Macro-Processo	Servizi di funzionamento
				Processo	Comunicazione
				Fase	Media relation
Area	Specifico Gestione delle informazioni riservate		Sotto Area		
DETTAGLIO RISCHIO					
Fattori abilitanti	<ul style="list-style-type: none"> ✓ Scarsa proceduralizzazione del processo ✓ Esercizio prolungato ed esclusivo di responsabilità di una fase da parte di uno o pochi soggetti ✓ Errore operativo ✓ Accordi illeciti ✓ Eccesso di discrezionalità da parte di un singolo soggetto ✓ Mancato rispetto delle regole procedurali interne ✓ Assenza controlli 			Conseguenze	<ul style="list-style-type: none"> ✓ perdita economica ✓ danno erariale ✓ sanzioni ✓ inefficienza ✓ contenzioso ✓ danno reputazionale
Riferimenti normativa esterna	<ul style="list-style-type: none"> • L. 633/1941 e s.m.i. • D.Lgs. 82/2005 e s.m.i. (CAD) 	Riferimenti normativa interna	//		
Anomalie significative	//	KRI	//	Indicatori di rischio	//
CONTROLLI					
Sintesi misure di controllo					
<ul style="list-style-type: none"> ✓ Politiche di gestione del rischio (MOG/PTPC/CE) ✓ Segregazione compiti/funzioni ✓ Controlli gerarchici ✓ Audit/Controlli ✓ Sistema deleghe/procure ✓ Tracciabilità del processo ✓ Archiviazione documentazione rilevante 			<ul style="list-style-type: none"> ✓ Rotazione ✓ Flussi informativi ✓ Formazione ✓ Whistleblowing ✓ Sistema disciplinare ✓ Sistema procedurale interno ✓ Accesso civico 		

Misure generali	Misure specifiche
<p>La Società si è dotata:</p> <ul style="list-style-type: none">- PTPC, Codice etico e Modello ex D.Lgs. 231/2001- Sistema disciplinare interno finalizzato a sanzionare il mancato rispetto del sistema procedurale interno e dei principi contenuti nel PTPC, del Codice etico e del Modello ex D.Lgs. 231/2001- Regolamento per la gestione dell'accesso civico semplice e generalizzato- Piano Integrato dei Controlli- Sistema di whistleblowing- Flussi informativi vs organi di controllo sia periodici che ad evento- Piano integrato di Formazione (d.lgs 231/2001, L. 190/12, d.lgs. 231/07 e GDPR)- Programma pluriennale di rotazione	<ul style="list-style-type: none">- Consip, in quanto testata registrata presso il Tribunale Civile di Roma (versione cartacea iscr. n. 11 del 16 gennaio 2009 - versione elettronica iscr. n. 14 del 16 gennaio 2009), pubblica "Quaderni Consip", sotto la supervisione della DRC ed il supporto delle Divisioni di volta in volta interessate, anche con il supporto della DAL, secondo un processo tracciato e documentato, sebbene non procedimentalizzato- I contenuti delle pubblicazioni sono approvati dall'AD
PIANI D'AZIONE SUGGERITI	
//	

SCORING PER FAMIGLIA DI RISCHIO														
190/12			231/ 01			50/16			Trasparenza			Privacy		
Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo
MEDIO ALTO	ADEGUATO	MOLTO BASSO	MEDIO ALTO	ADEGUATO	MOLTO BASSO									

SCORING PER FAMIGLIA DI RISCHIO														
262/ 05			Sicurezza informazioni			Sicurezza fisica			AML			Rischio operativo		
Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo
												ALTO	ADEGUATO	BASSO

SCORING COMPLESSIVO					
Scoring Inerente complessivo			Scoring Residuo complessivo		
Minimo	Medio	Massimo	Minimo	Medio	Massimo
MEDIO ALTO	ALTO	ALTO	MOLTO BASSO	BASSO	BASSO