PARTE SPECIALE

- Q –

# DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

Versione approvata dal Consiglio di Amministrazione in data 14 settembre 2022

## PARTE SPECIALE "Q" - DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI

### Q.1 Le tipologie dei delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-octies. 1 del Decreto)

L'art. 3 del d.lgs.184/2021 ha esteso la responsabilità amministrativa degli enti ai delitti in materia di strumenti di pagamento diversi dai contanti, introducendo nel Decreto l'art. 25-octies 1, la cui numerazione vuole sottolineare lo stretto collegamento con i reati di riciclaggio previsti all'art. 25 octies. Il predetto decreto costituisce infatti l'atto di recepimento della Direttiva 2019/713/UE del Parlamento europeo e del Consiglio del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, che rappresentano una minaccia alla sicurezza in quanto possono essere fonti di entrate per la criminalità organizzata e quindi rendono possibili altre attività criminali come il terrorismo, il traffico di droga e la tratta di esseri umani.

La definizione di *strumenti di pagamento diversi dal contante* è rinvenibile nell'art. 1 del d.lgs. 184/2021, il quale definisce come tale «*un dispositivo, oggetto o record protetto immateriale o materiale, o una loro combinazione, diverso dalla moneta a corso legale, che, da solo o unitamente a una procedura o a una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali»,* chiarendo ulteriormente che:

i) per «*dispositivo, oggetto o record protetto»* si intende un dispositivo, oggetto o record protetto contro le imitazioni o l'utilizzazione fraudolenta (per esempio mediante disegno, codice o firma);
ii) la locuzione «*mezzo di scambio digitale»* indica «*qualsiasi moneta elettronica definita all'art. 1, comma 2, lett.* h ter), *d.lgs. 385/1993, e la valuta virtuale»,* intendendosi quest'ultima come una «*rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è legata necessariamente a una valuta legalmente istituita e non possiede lo* status *giuridico di valuta o denaro, ma è accettata da persone fisiche o giuridiche come mezzo di scambio, e che può essere trasferita, memorizzata e scambiata elettronicamente».*

Tali definizioni riprendono sostanzialmente quelle proposte nella Direttiva (UE) 2019/71.

In virtù del primo comma del art. 25-octies.1, la condanna dell'ente può discendere, oltre che dai delitti ex artt. 493-ter c.p. (indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti) e 493-quater c.p. (detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti), anche dalla commissione di frode informatica (art. 640-ter c.p.), nella nuova ipotesi aggravata quando il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale.

Il comma 2 dell'art. 25-octies.1 prevede, inoltre, un'ipotesi residuale di responsabilità dell'ente, in quanto la norma dispone la sanzionabilità di ogni altro delitto contro la fede pubblica (Titolo VII c.p.), contro il patrimonio o che comunque offende il patrimonio (Titolo XIII c.p.) previsto dal codice penale, quando ha ad oggetto strumenti di pagamento diversi dai contanti, salvo che il

fatto integri altro illecito amministrativo sanzionato più gravemente. Tale disposto intende evidentemente responsabilizzare l'ente per tutti gli altri reati riguardanti gli «*strumenti di pagamento diversi dai contanti*» previsti dalla direttiva europea che a sua volta fa espresso riferimento al «*furto o altra illecita appropriazione*» degli strumenti materiali e all'«*ottenimento illecito*» di quelli immateriali; ipotesi queste che vanno sanzionate in quanto «*preparano il terreno all'effettiva utilizzazione fraudolenta dei mezzi di pagamento diversi dal contante*».

Nel seguito si riporta una breve descrizione dei reati ivi contemplati, suddivisi tra:

→ reati potenzialmente realizzabili;

→ reati la cui commissione è considerata remota;

| REATO | RIFERIMENTO | REALIZZABILITÀ |
|---|---|---|
| Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti | art. 493-ter c.p. | remota |
| Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti | art. 493-quater c.p. | remota |
| Frode informatica | art. 640-ter c.p. | possibile |

### Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.)[1]

*Chiunque al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi,* ***o comunque ogni altro strumento di pagamento diverso dai contanti*** *è punito con la reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera* ***gli strumenti o i documenti di cui al primo periodo****, ovvero possiede, cede o acquisisce* ***tali strumenti*** *o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.*

*In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è ordinata la confisca delle cose*

[1] L'art. 2, comma 1, lett. a) del d.lgs. 184/2021 ha disposto la modifica dell'art. 493-ter, rubrica e comma 1.

*che servirono o furono destinate a commettere il reato, nonché del profitto o del prodotto, salvo che appartengano a persona estranea al reato, ovvero quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto.*
*Gli strumenti sequestrati ai fini della confisca di cui al secondo comma, nel corso delle operazioni di polizia giudiziaria, sono affidati dall'autorità giudiziaria agli organi di polizia che ne facciano richiesta.*

L'articolo individua tre diverse tipologie di condotte:

1. la prima consiste nella indebita utilizzazione, cioè nel concreto uso illegittimo delle carte di credito o delle carte di pagamento – lecita o illecita che sia la loro provenienza – da parte del non titolare al fine di realizzare un profitto per sé o per altri;
2. la seconda categoria di condotte include quelle di falsificazione e alterazione dei medesimi strumenti di pagamento;
3. infine, viene punito chi possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi. Si tratta in questi ultimi casi di un'azione che sotto il profilo logico e temporale è distinta dalla prima perché la precede e ne costituisce il presupposto fattuale.

Presupposto di queste tipologie di condotta è, infatti, la illecita provenienza della carta o degli altri documenti indicati dalla norma; ciò perché da sole tali condotte non sono caratterizzate da alcuna illiceità a differenza dell'utilizzo indebito o della falsificazione. Nel caso in cui le carte siano contraffatte o alterate l'illecita provenienza deriva direttamente dalla contraffazione o dalla alterazione. Per quanto riguarda le persone giuridiche, tale reato potrebbe astrattamente configurarsi nel caso in cui il dipendente della società cui è affidata la gestione della carta di credito aziendale, ma non ne è il titolare qualificato, la utilizzi indebitamente per un profitto personale arrecando un danno all'ente; laddove invece l'uso indebito fosse ascrivibile al titolare della carta di credito, si potrà configurare il reato di appropriazione indebita ex art. 646 c.p. e non quello di indebito utilizzo di carta di credito.
Diverso invece è il caso in cui l'uso indebito – o addirittura la falsificazione – vengano effettuati nell'interesse e a vantaggio dell'ente di appartenenza, ipotesi che, sebbene in linea teorica non si possa escludere del tutto, appare effettivamente remota.

## Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.)[2]

[2] Il D. lgs. n. 184 del 8 novembre 2021 ha disposto (con l'art. 2, comma 1, lettera b)) l'introduzione dell'art. 493-quater.

*Salvo che il fatto costituisca più grave reato, chiunque, alfine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o a altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo, è punito con la reclusione sino a due anni e la multa sino a 1000 euro.*

*In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è sempre ordinata la confisca delle apparecchiature, dei dispositivi o dei programmi informatici predetti, nonché la confisca del profitto o del prodotto del reato ovvero, quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto.*

Tale fattispecie richiama in parte alcuni reati informatici che sono già inclusi nel catalogo dei reati presupposto: si pensi ai delitti di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici e di diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (artt. 615 quater e 615 quinquies c.p., richiamati nell'art. 24 bis, d.lgs. 231/2001). Tuttavia, considerando il dettato della norma in esame, sebbene in linea teorica non si possa escludere del tutto, appare effettivamente remota la possibilità che tale tipologia di reato possa essere commesso nell'interesse e a vantaggio dell'ente di appartenenza.

### Frode informatica (art. 640-ter c.p.)[3]

*"Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.*

*La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto* ***produce un trasferimento di denaro, di valore monetario o di valuta virtuale o*** *è commesso con abuso della qualità di operatore del sistema.*

*La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.*

*Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o taluna delle circostanze previste dall'articolo 61, primo comma, numero 5, limitatamente all'aver approfittato di circostanze di persona, anche in riferimento all'età, e numero 7."*

[3] Il D. lgs. n. 184 del 8 novembre 2021 ha disposto (con l'art. 2, comma 1, lettera c)) la modifica dell'art. 640-ter, comma 2.

Come sopra accennato, con il d.lgs. 184/2021 viene inserita tra i reati presupposto anche la frode informatica aggravata dal fatto che dalla condotta derivi un trasferimento di denaro, di valore monetario o di valuta virtuale.

## Q.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.
Come anticipato, l'allocazione della nuova disposizione di cui all'art. 25 octies-1 in contiguità con l'art. 25 octies è tutt'altro che involontaria: infatti il legislatore ha voluto rivolgersi a quelle aree organizzative dell'ente che si occupano di gestire, controllare e monitorare i flussi patrimoniali e finanziari, in quanto la gestione illecita - diretta o indiretta - degli strumenti di pagamento (in entrata o in uscita) e dei movimenti monetari, potrebbe rappresentare fonti di entrate per la criminalità organizzata.

Le aree di attività ritenute più specificamente a rischio ai fini della presente Parte speciale "Q" sono dunque indicate nel seguito, richiamando per quanto di interesse quanto riportato nella Parte Speciale E - Reati di ricettazione, riciclaggio e impiego di denaro, beni e utilità di provenienza illecita.

| Rif. Rischio | Attività a rischio reato | Descrizione rischio | Reati |
|---|---|---|---|
| R_95 | Gestione pagamenti fatture | Gestione impropria dei pagamenti anche al fine di avvantaggiare la società o terzi:<br>– es. pagamento di importi maggiori o importi non dovuti<br>– ricezione denaro proveniente da attività illecite - impiego denaro in modo da far perdere le tracce di denaro di origine illecita<br>– utilizzando strumenti di pagamento non intestati alla Società | – *Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti (art. 493-ter c.p.)*<br>– *Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.)*<br>– *Frode informatica (art. 640-ter c.p.)* |
| R_191 | Accesso sistemi informativi interni | Accesso illegittimo ai sistemi informativi aziendali al fine di:<br>– estrarre dati / informazioni / documenti riservati da utilizzare/ diffondere a terzi | – *Frode informatica (art. 640-ter c.p.)* |

| Rif. Rischio | Attività a rischio reato | Descrizione rischio | Reati |
|---|---|---|---|
| | | – danneggiare/alterare i dati ivi contenuti o il sistema (es per coprire inefficienze o comportamenti illeciti nell'autorizzazione degli acquisti interni)<br>– effettuare un trasferimento illecito di denaro, di valore monetario o di valuta virtuale<br>per avvantaggiare un dipendente o la Società | |
| R_193 | Controllo accessi sistemi informativi interni/gestiti dalla società | Mancato controllo sugli accessi al sistema da parte degli amministratori di sistema e mancata tracciabilità degli stessi | – *Frode informatica (art. 640-ter c.p.)* |
| R_195 | Gestione / acquisto banche dati e software aziendali | Abusivo utilizzo/detenzione di banche dati/software con lo scopo di commettere attività illecite. | – *Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.)*<br>– *Frode informatica (art. 640-ter c.p.)* |
| R_196 | Gestione, sviluppo Sistemi informativi interni | Non corretta gestione / sviluppo / danneggiamento di sistemi informativi interni anche al fine di avvantaggiare terzi o la Società (es. danneggiare il sistema accessi per impedirne la consultazione o sviluppare un software per commettere attività illecite) | – *Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti (art. 493-quater c.p.)*<br>– *Frode informatica (art. 640-ter c.p.)* |

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

- ✓ ***Anagrafica evento rischio***: (i) attività a rischio e descrizione; (ii) Risk owner, contributor; (iii) Macro processo, Processo e Fase; (iv) Area e Sotto Area;
- ✓ ***Dettaglio rischio***: (v) Fattori abilitanti; (vi) Conseguenze; (vii) Riferimenti normativa esterna ed interna; (viii) Anomalie significative; (ix) Indicatori di rischio;
- ✓ ***Controlli***: (x) Sintesi misure di controllo; (xi) Misure generali; (xii) Misure specifiche;
- ✓ ***Piani di azione***: sintesi degli interventi correttivi da implementare, monitorati dal RPCT.

## Q.3 Principi di comportamento

I Destinatari del Modello, competenti per le attività oggetto di regolamentazione della presente Parte speciale, sono dunque tenuti ad osservare i seguenti ulteriori principi:

- rispettare le norme in tema di trasparenza, nel rispetto di quanto indicato nel PTPC;
- 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;

con particolare riguardo alle attività di gestione dei pagamenti

- tenere un comportamento corretto, trasparente e collaborativo, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività finalizzate alla gestione dell'anagrafica fornitori, anche stranieri (attraverso l'amministrazione, l'aggiornamento e il monitoraggio del relativo elenco storico);
- non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi di denaro di rilevante entità;
- assicurare, in caso di pagamenti a favore di soggetti terzi tramite bonifico bancario, il rispetto di tutti i passaggi autorizzativi relativi alla predisposizione, validazione ed emissione del mandato di pagamento, nonché della registrazione a sistema della relativa distinta;
- operare nel rispetto delle rispettive procedure per quanto concerne i pagamenti con Carta di Credito e la gestione del fondo economale, oltre che nel rispetto dei limiti delle deleghe e delle procure conferite in tale ambito;
- in caso di pagamento a carico della Società a mezzo di carta di credito, impiegare esclusivamente la carta di credito aziendale o altro strumento comunque intestato alla Società o a persona fisica in sua rappresentanza;
- assicurare che tutti i pagamenti riferiti ad acquisti realizzati dalla Società vengano effettuati a fronte dell'inserimento a sistema della fattura corrispondente dal personale dell'Area Contabilità Generale e Bilancio a ciò debitamente autorizzato, previa verifica della relativa regolarità formale e della congruità del pagamento con il contratto/ordine d'acquisto corrispondente;
- assicurare un adeguato sistema di segregazione dei poteri autorizzativi, di controllo ed esecutivi in relazione alla gestione dei pagamenti delle fatture e alle modalità di predisposizione ed approvazione delle relative distinte di pagamento;

- operare nel rispetto degli obblighi di legge e ad assicurare la corretta attuazione delle politiche di gestione del rischio di riciclaggio e di finanziamento del terrorismo;
- segnalare tempestivamente ai soggetti competenti ogni circostanza per la quale si conosca, si sospetti, o si abbiano ragionevoli motivi per sospettare che siano state compiute, tentate o siano in corso operazioni di frode e/o falsificazione di mezzi di pagamento diversi dai contanti, riciclaggio, di finanziamento del terrorismo o che i fondi, indipendentemente dalla loro entità, provengano da un'attività criminosa;
- non intrattenere rapporti commerciali con soggetti (fisici o giuridici) dei quali sia conosciuta o sospettata l'appartenenza ad organizzazioni criminali o comunque operanti al di fuori della liceità (i.e. a titolo esemplificativo ma non esaustivo, persone legate all'ambiente del riciclaggio, al traffico di droga, all'usura);

con riguardo all'utilizzo delle apparecchiature informatiche/software

- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente nell'ambito dell'attività svolta dalla Società e per le specifiche finalità assegnate;
- non prestare o cedere a terzi qualsiasi apparecchiatura informatica, senza la preventiva autorizzazione del responsabile della funzione competente alla gestione dei relativi sistemi informatici;
- in caso di smarrimento o furto di qualsiasi apparecchiatura informatica della Società o delle Pubbliche Amministrazioni coinvolte, informare tempestivamente il responsabile della funzione competente alla gestione dei relativi sistemi/dispositivi informatici e attenersi alla Procedura gestione delle violazioni dei dati personali (*data breach notification*);
- utilizzare la connessione internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che rendono necessario il collegamento;
- rispettare le procedure e gli standard previsti in materia di utilizzazione delle risorse informatiche, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali di queste ultime;
- impiegare sulle apparecchiature di Consip soltanto prodotti ufficialmente acquisiti dalla Società;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni di Consip.;
- in ogni caso osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.

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 dagli articoli 25-octies 1 del 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:

- usare in modo illegittimo carte di credito o carte di pagamento – lecita o illecita che sia la loro provenienza –al fine di realizzare un profitto;
- possedere, cedere o acquisire tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi;

- produrre, importare, esportare, vendere, trasportare, distribuire apparecchiature, dispositivi o programmi informatici per la commissione di reati riguardanti strumenti di pagamento diversi dai contanti;

## Q.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.

## Q.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.95

| ANAGRAFICA EVENTO RISCHIO | | | | | |
|---|---|---|---|---|---|
| **Codice rischio** | **95** | **Attività** | **Gestione pagamenti fatture** | **Descrizione Rischio** | Gestione impropria dei pagamenti anche al fine di avvantaggiare la società o terzi:<br>- es. pagamento di importi maggiori o importi non dovuti<br>- es. ricezione denaro proveniente da attività illecite - impiego denaro in modo da far perdere le tracce di denaro di origine illecita<br>- utilizzo di strumenti di pagamento non intestati alla Società |

| | | | | | |
|---|---|---|---|---|---|
| **Risk-owner** | → DDE che autorizzano il pagamento<br>→ DAFC - Contabilità generale e bilancio<br>→ DAL e DRC per firma congiunta pagamenti in assenza resp. DAFC | **Contributor** | // | **Macro-Processo** | Servizi di funzionamento |
| | | | | **Processo** | Amministrazione e Finanza |
| | | | | **Fase** | Gestione fatturazione passiva |
| **Area** | Generale<br>Gestione delle entrate, delle spese e del patrimonio | | **Sotto Area** | Specifico<br>Flussi monetari e finanziari | |

| DETTAGLIO RISCHIO | | | |
|---|---|---|---|
| **Fattori abilitanti** | ✓ Scarsa procedimentalizzazione del processo<br>✓ Esercizio prolungato ed esclusivo di responsabilità di una fase da parte di uno o pochi soggetti<br>✓ Errore operativo<br>✓ Accordi illeciti<br>✓ Eccesso di discrezionalità da parte di un singolo soggetto<br>✓ Mancato rispetto delle regole procedurali interne<br>✓ Mancato/ errato recepimento della normativa di settore<br>✓ Assenza controlli | **Conseguenze** | ✓ perdita economica<br>✓ danno erariale<br>✓ sanzioni<br>✓ inefficienza<br>✓ contenzioso<br>✓ danno reputazionale |

| | | | |
|---|---|---|---|
| **Riferimenti normativa esterna** | • L. n. 190/2012<br>• D.Lgs. n. 33/2013<br>• D.Lgs. n. 231/2001<br>• D.Lgs. n. 231/2002<br>• L. 262/2005 | **Riferimenti normativa interna** | o Modalità operative relative alla fase istruttoria degli acquisti interni Consip<br>o Procedura ciclo passivo acquisto beni e servizi<br>o Modalità operative gestione amministrativo-contabile tesoreria<br>o Linee Guida DDE (compiti ed attività) |

| | | | | | |
|---|---|---|---|---|---|
| **Anomalie significative** | // | **KRI** | // | **Indicatori di rischio** | // |

| CONTROLLI |
|---|
| **Sintesi misure di controllo** |

- ✓ Politiche di gestione del rischio (MOG/PTPC/CE)
- ✓ Politiche di gestione del rischio privacy
- ✓ Politiche gestione rischio antiriciclaggio
- ✓ Politiche di gestione del rischio ex L 262/05
- ✓ Trasparenza
- ✓ Segregazione compiti/funzioni
- ✓ Controlli gerarchici
- ✓ Audit/ Controlli
- ✓ Sistema deleghe/procure
- ✓ Archiviazione documentazione rilevante
- ✓ Tracciabilità del processo
- ✓ Reporting
- ✓ Rotazione
- ✓ Flussi informativi
- ✓ Informatizzazione processo
- ✓ Formazione
- ✓ Whistleblowing
- ✓ Certificazioni
- ✓ Sistema disciplinare
- ✓ Sistema procedurale interno
- ✓ Accesso civico

| Misure generali | Misure specifiche |
|---|---|
| La Società si è dotata:<br>- PTPC, Codice etico e Modello ex D.Lgs. 231/2001<br>- 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<br>- Specifiche regole a garanzia della riservatezza delle informazioni<br>- 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<br>- Regolamento per la gestione dell'accesso civico semplice e generalizzato<br>- Piano Integrato dei Controlli<br>- Sistema di whistleblowing<br>- Flussi informativi vs organi di controllo sia periodici che ad evento<br>- Piano integrato di Formazione (d.lgs 231/2001, L. 190/12, d.lgs. 231/07 e GDPR)<br>- Piano Pluriennale di rotazione | - La società si è dotata di procedure interne che disciplinano il ciclo passivo per gli acquisti di beni e servizi e la gestione della tesoreria, elaborate 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<br>- Per quanto riguarda i beni: la DRC (Ufficio Posta) al ricevimento del bene verifica la presenza a sistema (SIACC) di un ordine relativo allo stesso e la corrispondenza tra documento di trasporto e ordine<br>- Per quanto riguarda la fatturazione di beni e servizi sono previste contrattualmente verifiche di conformità del DDE e validazione sul siacc, propedeutiche al pagamento.<br>- Sono previsti controlli specifici effettuati dall'area CGB sul rispetto delle prescrizioni in termini di tracciabilità dei flussi finanziari e sulla corretta registrazione delle fatture ai fini fiscali<br>- Per la gestione del ciclo passivo è utilizzato un sistema contabile integrato con il SIACC che consente la tracciatura delle operazioni e non consente di duplicare la contabilizzazione di una fattura<br>- Le fatture elettroniche sono gestite attraverso il sistema di fatturazione elettronica e transitano sullo SDI<br>- Al momento della registrazione della fattura passiva il sistema contabile in automatico calcola la data di pagamento e la propone al pagamento. La registrazione contabile può essere effettuata solo da personale autorizzato (Area CGB)<br>- Le distinte di pagamento, contenenti i codici CIG e CUP (ove presenti), sono predisposte dagli addetti al Ciclo Passivo, inserite nel sistema home banking dall'addetto di tesoreria, approvate in base ai poteri di firma ed inviate alla banca.<br>- Sono previsti controlli specifici da parte del Dirigente preposto ex L. 262/2005 sul corretto inserimento delle fatture nel sistema contabile; (ii) sulla regolarità formale della fattura e (iii) sulla congruità tra quanto fatturato e quanto validato nel SIACC; (iv) in tema di tracciabilità dei flussi finanziari; (v) sulla corretta registrazione delle fatture ai fini fiscali. Le risultanze dei predetti controlli sono contenute nel reporting periodico da questo sottoposto a CdA/CS/OdV/RPCT.<br>- Verifiche specifiche svolte trimestralmente dalla società di revisione<br>- Il resp. della DAFC è dotato di specifiche procure in tema di pagamenti con limite d'importo oltre il quale firma AD; in assenza di entrambi i pagamenti possono essere autorizzati con firma congiunta dei resp. DAL/DRC sempre nei limiti d'importo consentiti<br>- Trasparenza: Pubblicazione dei dati su Pagamenti Beni e Servizi, Indicatore di tempestività pagamenti, Debiti e numero Creditori e Rendicontazione finanziaria dei singoli contratti in Società Trasparente ex dlgs 50/16 e dlgs 33/13<br>- Il processo è certificato: Certificazione ISO 9001:2015 |
| **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 | 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 | | | | | | | MOLTO ALTO | ADEGUATO | MEDIO BASSO | MOLTO ALTO | ADEGUATO | MEDIO BASSO |

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

# R.191

| ANAGRAFICA EVENTO RISCHIO | | | | | |
|---|---|---|---|---|---|
| **Codice rischio** | **191** | **Attività** | **Accesso sistemi informativi interni** | **Descrizione Rischio** | Accesso illegittimo ai sistemi informativi aziendali al fine di:<br>- estrarre dati / informazioni / documenti riservati da utilizzare/ diffondere a terzi<br>- danneggiare/alterare i dati ivi contenuti o il sistema (es per coprire inefficienze o comportamenti illeciti nell'autorizzazione degli acquisti interni)<br>- effettuare un trasferimento illecito di denaro, di valore monetario o di valuta virtuale<br>per avvantaggiare un dipendente o la Società |

| | | | | | |
|---|---|---|---|---|---|
| **Risk-owner** | → DEPSI – Sviluppo Gestione e supporto<br>→ DEPSI - Data Management e Sistemi Informativi Interni<br>→ DEPSI - Infrastrutture e Cybersecurity<br>→ Amministratori sistema<br>→ Responsabile sicurezza | **Contributor** | // | **Macro-Processo** | Servizi di funzionamento |
| | | | | **Processo** | Sicurezza |
| | | | | **Fase** | Modello sicurezza logica |

| | | | |
|---|---|---|---|
| **Area** | Specifico<br>Gestione Sistemi Informativi | **Sotto Area** | Specifico<br>Protezione dei sistemi informativi |

| DETTAGLIO RISCHIO | | | |
|---|---|---|---|
| **Fattori abilitanti** | ✓ Scarsa procedimentalizzazione del processo<br>✓ Esercizio prolungato ed esclusivo di responsabilità di una fase da parte di uno o pochi soggetti<br>✓ Errore operativo<br>✓ Accordi illeciti<br>✓ Eccesso di discrezionalità da parte di un singolo soggetto<br>✓ Mancato rispetto delle regole procedurali interne<br>✓ Mancato/ errato recepimento della normativa di settore<br>✓ Assenza controlli | **Conseguenze** | ✓ perdita economica<br>✓ danno erariale<br>✓ sanzioni<br>✓ inefficienza<br>✓ contenzioso<br>✓ danno reputazionale |

| | | | |
|---|---|---|---|
| **Riferimenti normativa esterna** | • L. n. 190/2012<br>• D.Lgs. n. 231/2001<br>• Regolamento UE 2016/679<br>• D.Lgs. 196/2003 e s.m.i. come modif. dal D.Lgs. 101/2018<br>• DL 144/2005<br>• Provvedimento Garante privacy su Amministratori di sistema | **Riferimenti normativa interna** | o Modello organizzativo Privacy<br>o Istruzioni Operative per le persone autorizzate al Trattamento dei dati personali<br>o Istruzioni Operative per i Referenti Interni del trattamento dei dati personali<br>o Procedura gestione delle violazioni dei dati personali (data breach notification) |

| | | | | | |
|---|---|---|---|---|---|
| **Anomalie significative** | Accesso o tentativo di accesso fraudolento ai sistemi interni/gestiti | **KRI** | 0 / 22 | **Indicatori di rischio** | 0) Segnalazioni pervenute<br>22) Accesso o tentativo di accesso fraudolento ai sistemi interni/gestiti |

| CONTROLLI | |
|---|---|
| **Sintesi misure di controllo** | |
| ✓ Politiche di gestione del rischio (MOG/PTPC/CE)<br>✓ Politiche di gestione del rischio privacy<br>✓ Trasparenza<br>✓ Segregazione compiti/funzioni<br>✓ Controlli gerarchici<br>✓ Audit/ Controlli<br>✓ Sistema deleghe/procure<br>✓ Tracciabilità del processo<br>✓ Archiviazione documentazione rilevante | ✓ Rotazione<br>✓ Reporting<br>✓ Flussi informativi<br>✓ Informatizzazione del processo<br>✓ Formazione<br>✓ Whistleblowing<br>✓ Certificazioni<br>✓ Sistema disciplinare<br>✓ Sistema procedurale interno<br>✓ Accesso civico |
| **Misure generali** | **Misure specifiche** |
| La Società si è dotata:<br>- PTPC, Codice etico e Modello ex D.Lgs. 231/2001<br>- 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<br>- Specifiche regole a garanzia della riservatezza delle informazioni<br>- 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<br>- Regolamento per la gestione dell'accesso civico semplice e generalizzato<br>- Piano Integrato dei Controlli<br>- Flussi informativi vs organi di controllo sia periodici che ad evento<br>- Sistema di whistleblowing<br>- Piano integrato di Formazione (d.lgs 231/2001, L. 190/12, d.lgs. 231/07 e GDPR)<br>- Piano pluriennale di rotazione | - La Società si è dotata di procedure interne per la gestione di specifici adempimenti privacy (es. DPIA); nello specifico, adottata Procedura interna per la gestione delle violazioni dei dati personali (data breach notification) che prevede:<br>o Rilevazione dell'Incidente di sicurezza con individuazione dei soggetti che possono rilevare incidenti di sicurezza<br>o Valutazione dell'Incidente di sicurezza, a tal fine, il DPO con il supporto della DCS e della DEPSI, raccoglie le informazioni e la documentazione ritenute necessarie per la valutazione; all'esito della valutazione del data breach, il DPO sottopone all'AD, per approvazione, la proposta di archiviazione dell'evento o di procedere con la notifica al Garante<br>- Tracciabilità delle operazioni effettuate (attualmente non copre tutti i sistemi)<br>- Strumenti di crittografia<br>- Sistema di data loss prevention<br>- Sistema di classificazione dei documenti<br>- Sistema di tracciabilità degli accessi da parte degli Amministratori di Sistema<br>- Flusso vs OdV/RPTC/DPO in merito alla segnalazione di tutti i casi in cui riscontrino anomalie dei sistemi informatici (dalle quali possano evincersi accessi o tentativi di accessi abusivi, danneggiamenti, violazione delle procedure interne IT, cancellazione dei dati, ecc.) e/o incidenti informatici, ivi incluse le comunicazioni di chiusura degli stessi<br>- Reporting AD o Organi di controllo a CdA/CS su criticità<br>- Adozione Registro data breach<br>- Adozione policy interne per la sicurezza/riservatezza delle informazioni nell'intero ciclo di vita |
| **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 |
| MOLTO ALTO | ADEGUATO | MEDIO BASSO | ALTO | ADEGUATO | BASSO | | | | | | | MOLTO ALTO | ADEGUATO | MEDIO 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 |
| | | | MOLTO ALTO | ADEGUATO | MEDIO BASSO | ALTO | ADEGUATO | BASSO | | | | | | |

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

# R.193

| ANAGRAFICA EVENTO RISCHIO | | | | | | |
|---|---|---|---|---|---|---|
| **Codice rischio** | **193** | **Attività** | **Controllo accessi sistemi informativi interni/gestiti dalla società** | **Descrizione Rischio** | Mancato controllo sugli accessi al sistema da parte degli amministratori di sistema e mancata tracciabilità degli stessi | |
| **Risk-owner** | → Amministratori di sistema<br>→ DEPSI – Sviluppo Gestione e supporto<br>→ DEPSI - Data Management e Sistemi Informativi Interni<br>→ DEPSI - Infrastrutture e Cybersecurity | | **Contributor** | // | **Macro-Processo** | Servizi di funzionamento |
| | | | | | **Processo** | Sicurezza |
| | | | | | **Fase** | Modello sicurezza logica |
| **Area** | Specifico<br>Gestione Sistemi Informativi | | | **Sotto Area** | Specifico<br>Protezione dei sistemi informativi | |

| DETTAGLIO RISCHIO | | | |
|---|---|---|---|
| **Fattori abilitanti** | ✓ Scarsa procedimentalizzazione del processo<br>✓ Esercizio prolungato ed esclusivo di responsabilità di una fase da parte di uno o pochi soggetti<br>✓ Errore operativo<br>✓ Accordi illeciti<br>✓ Eccesso di discrezionalità da parte di un singolo soggetto<br>✓ Mancato rispetto delle regole procedurali interne<br>✓ Mancato/ errato recepimento della normativa di settore<br>✓ Assenza controlli | **Conseguenze** | ✓ perdita economica<br>✓ danno erariale<br>✓ sanzioni<br>✓ inefficienza<br>✓ contenzioso<br>✓ danno reputazionale |
| **Riferimenti normativa esterna** | • L. n. 190/2012<br>• D.Lgs. n. 231/2001<br>• Regolamento UE 2016/679<br>• D.Lgs. 196/2003 e s.m.i.<br>• D.Lgs. 101/2018<br>• DL 144/2005<br>• Provvedimento Garante privacy su Amministratori di sistema | **Riferimenti normativa interna** | o Modello organizzativo Privacy<br>o Azioni di Contingency per le procedure di gara sul sistema informativo di e-Procurement<br>o Modalità operative per la gestione unica degli accessi logici al Sistema di e-Procurement<br>o Procedura gestione delle violazioni dei dati personali (data breach notification)<br>o Istruzioni Operative per le persone autorizzate al Trattamento dei dati personali<br>o Istruzioni Operative per i Referenti Interni del trattamento dei dati personali |

| | | | | | |
|---|---|---|---|---|---|
| **Anomalie significative** | Accesso o tentativo di accesso fraudolento ai sistemi interni/gestiti | **KRI** | 0 / 22 | **Indicatori di rischio** | 0) Segnalazioni pervenute<br>22) Accesso o tentativo di accesso fraudolento ai sistemi interni/gestiti |

## CONTROLLI

### Sintesi misure di controllo

- ✓ Politiche di gestione del rischio (MOG/PTPC/CE)
- ✓ Politiche di gestione del rischio privacy
- ✓ Trasparenza
- ✓ Segregazione compiti/funzioni
- ✓ Controlli gerarchici
- ✓ Audit/ Controlli
- ✓ Sistema deleghe/procure
- ✓ Tracciabilità del processo
- ✓ Archiviazione documentazione rilevante
- ✓ Rotazione
- ✓ Reporting
- ✓ Flussi informativi
- ✓ Informatizzazione del processo
- ✓ Formazione
- ✓ Whistleblowing
- ✓ Certificazioni
- ✓ Sistema disciplinare
- ✓ Sistema procedurale interno
- ✓ Accesso civico

### Misure generali

La Società si è dotata:

- 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
- Specifiche regole a garanzia della riservatezza delle informazioni
- 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
- Flussi informativi vs organi di controllo sia periodici che ad evento
- Sistema di whistleblowing
- Piano integrato di Formazione (d.lgs 231/2001, L. 190/12, d.lgs. 231/07 e GDPR)
- Piano pluriennale di rotazione

### Misure specifiche

- La Società si è dotata di procedure interne che descrivono il processo e le modalità operative per la gestione ed il controllo degli accessi logici al Sistema di e-Procurement della Pubblica Amministrazione al fine di proteggere la documentazione e i dati personali da accessi e trattamenti non autorizzati; nello specifico è previsto:
  - o Area Sviluppo Gestione e Supporto effettua periodicamente un monitoraggio sulle utenze volto a verificare che: i) tutti gli utenti (personale interno e esterno) che risultano abilitati sul Sistema abbiano ragione di avere ancora l'utenza; ii) i diritti di accesso siano coerenti rispetto al ruolo ricoperto
  - o "liste di accesso" da sottoporre a revisione con periodicità semestrale per verificare la validità delle autorizzazioni e dei diritti di accesso associati
  - o Ciascun responsabile di Area/Divisione, con cadenza semestrale, verifica e aggiorna il documento pubblicato sull'apposito mini sito Consip contenente, per ciascuna Area gli utenti Consip/i fornitori esterni registrati nel Sistema e i relativi profili
  - o la storia dell'utenza è preservata per sempre
- Adottata una procedura che disciplina le azioni di Contingency per le procedure di gara sul sistema informativo di e-Procurement;
- Adozione policy interne per la gestione di specifici adempimenti privacy: adottata procedura interna per la gestione delle violazioni dei dati personali (data breach notification)
- Tracciabilità delle operazioni effettuate
- Sistema di data loss prevention
- Sistema di tracciabilità degli accessi da parte degli Amministratori di Sistema
- Flusso vs OdV/RPTC/DPO in merito alla segnalazione di tutti i casi in cui riscontrino anomalie dei sistemi informatici (dalle quali possano evincersi accessi o tentativi di accessi abusivi, danneggiamenti, violazione delle procedure interne IT, cancellazione dei dati, ecc.) e/o incidenti informatici, ivi incluse le comunicazioni di chiusura degli stessi
- Reporting AD o Organi di controllo a CdA/CS su criticità
- Policy gestione utenze
- Nomina Responsabile sicurezza del fornitore nell'ambito dei contratti
- Adozione Registro data breach

## 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 |
| MOLTO ALTO | PARZIALMENTE ADEGUATO | MEDIO | MOLTO ALTO | PARZIALMENTE ADEGUATO | MEDIO | | | | | | | MOLTO ALTO | PARZIALMENTE ADEGUATO | MEDIO |

| 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 |
| | | | MOLTO ALTO | ADEGUATO | MEDIO BASSO | ALTO | ADEGUATO | BASSO | | | | | | |

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

# R.195

| ANAGRAFICA EVENTO RISCHIO | | | | | |
|---|---|---|---|---|---|
| **Codice rischio** | **195** | **Attività** | **Gestione/ acquisto banche dati e software aziendali** | **Descrizione Rischio** | Abusivo utilizzo/detenzione di banche dati/software con lo scopo di commettere attività illecite |
| **Risk-owner** | → DEPSI – Sviluppo Gestione e supporto<br>→ DEPSI - Data Management e Sistemi Informativi Interni<br>→ DEPSI - Infrastrutture e Cybersecurity<br>→ Tutte le risorse | | **Contributor** | // | **Macro-Processo**: Servizi di funzionamento<br>**Processo**: Sicurezza<br>**Fase**: Modello sicurezza logica |
| **Area** | Specifico<br>Gestione Sistemi Informativi | | | **Sotto Area** | Specifico<br>Gestione software/ hardware |

| DETTAGLIO RISCHIO | | | |
|---|---|---|---|
| **Fattori abilitanti** | ✓ Scarsa procedimentalizzazione del processo<br>✓ Esercizio prolungato ed esclusivo di responsabilità di una fase da parte di uno o pochi soggetti<br>✓ Errore operativo<br>✓ Accordi illeciti<br>✓ Eccesso di discrezionalità da parte di un singolo soggetto<br>✓ Mancato rispetto delle regole procedurali interne<br>✓ Assenza controlli | **Conseguenze** | ✓ perdita economica<br>✓ danno erariale<br>✓ sanzioni<br>✓ inefficienza<br>✓ contenzioso<br>✓ danno reputazionale |
| **Riferimenti normativa esterna** | • L. n. 190/2012<br>• D.Lgs. n. 231/2001<br>• Regolamento UE 2016/679<br>• D.Lgs. 196/2003 e s.m.i.<br>• D.Lgs. 101/2018<br>• Provvedimento Garante privacy su Amministratori di sistema | **Riferimenti normativa interna** | o Modello organizzativo Privacy<br>o Istruzioni Operative per le persone autorizzate al Trattamento dei dati personali<br>o Istruzioni Operative per i Referenti Interni del trattamento dei dati personali |

| | | | | | |
|---|---|---|---|---|---|
| **Anomalie significative** | | **KRI** | | **Indicatori di rischio** | |

| CONTROLLI | |
|---|---|
| **Sintesi misure di controllo** | |
| ✓ Politiche di gestione del rischio (MOG/PTPC/CE)<br>✓ Politiche di gestione del rischio privacy<br>✓ Trasparenza<br>✓ Segregazione compiti/funzioni<br>✓ Controlli gerarchici<br>✓ Audit/ Controlli<br>✓ Sistema deleghe/procure<br>✓ Tracciabilità del processo<br>✓ Archiviazione documentazione rilevante<br>✓ Rotazione | ✓ Reporting<br>✓ Flussi informativi<br>✓ Informatizzazione del processo<br>✓ Formazione<br>✓ Whistleblowing<br>✓ Certificazioni<br>✓ Sistema disciplinare<br>✓ Sistema procedurale interno<br>✓ Accesso civico |

| Misure generali | Misure specifiche |
|---|---|
| La Società si è dotata:<br>- PTPC, Codice etico e Modello ex D.Lgs. 231/2001<br>- 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<br>- Specifiche regole a garanzia della riservatezza delle informazioni<br>- 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<br>- Regolamento per la gestione dell'accesso civico semplice e generalizzato<br>- Piano Integrato dei Controlli<br>- Flussi informativi vs organi di controllo sia periodici che ad evento<br>- Sistema di whistleblowing<br>- Piano integrato di Formazione (d.lgs 231/2001, L. 190/12, d.lgs. 231/07 e GDPR)<br>- Piano pluriennale di rotazione | - Tracciabilità dell'utilizzo delle risorse / licenze<br>- Gestione degli asset<br>- Istruzioni interne che vietano esplicitamente tali comportamenti |
| **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 |
| MOLTO ALTO | ADEGUATO | MEDIO BASSO | MOLTO ALTO | ADEGUATO | MEDIO 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 |
| | | | MOLTO ALTO | ADEGUATO | MEDIO BASSO | | | | | | | MOLTO ALTO | ADEGUATO | MEDIO BASSO |

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

# R.196

| ANAGRAFICA EVENTO RISCHIO | | | | | |
|---|---|---|---|---|---|
| **Codice rischio** | **196** | **Attività** | **Gestione, sviluppo Sistemi informativi interni** | **Descrizione Rischio** | Non corretta gestione / sviluppo / danneggiamento di sistemi informativi interni anche al fine di avvantaggiare terzi o la Società (es. danneggiare il sistema accessi per impedirne la consultazione o sviluppare un software per commettere attività illecite) |
| **Risk-owner** | → DEPSI – Sviluppo Gestione e supporto<br>→ DEPSI - Data Management e Sistemi Informativi Interni<br>→ DEPSI - Pianificazione e analisi della domanda<br>→ DEPSI - Infrastrutture e Cybersecurity<br>→ Responsabile sicurezza | | **Contributor** | // | **Macro-Processo**: Servizi di funzionamento<br>**Processo**: Sicurezza<br>**Fase**: Modello sicurezza logica |
| **Area** | Specifico<br>Gestione Sistemi Informativi | | | **Sotto Area** | Specifico<br>Protezione dei sistemi informativi |

| DETTAGLIO RISCHIO | | | |
|---|---|---|---|
| **Fattori abilitanti** | ✓ Scarsa procedimentalizzazione del processo<br>✓ Esercizio prolungato ed esclusivo di responsabilità di una fase da parte di uno o pochi soggetti<br>✓ Errore operativo<br>✓ Accordi illeciti<br>✓ Eccesso di discrezionalità da parte di un singolo soggetto<br>✓ Mancato rispetto delle regole procedurali interne<br>✓ Assenza controlli | **Conseguenze** | ✓ perdita economica<br>✓ danno erariale<br>✓ sanzioni<br>✓ inefficienza<br>✓ contenzioso<br>✓ danno reputazionale |
| **Riferimenti normativa esterna** | • L. n. 190/2012<br>• D.Lgs. n. 231/2001<br>• Regolamento UE 2016/679<br>• D.Lgs. 196/2003 e s.m.i. come modif. dalD.Lgs. 101/2018<br>• Provvedimento Garante privacy su Amministratori di sistema | **Riferimenti normativa interna** | o Modello organizzativo Privacy<br>o Istruzioni Operative per le persone autorizzate al Trattamento dei dati personali<br>o Istruzioni Operative per i Referenti Interni del trattamento dei dati personali<br>o Procedura gestione delle violazioni dei dati personali (data breach notification) |

| | | | | | |
|---|---|---|---|---|---|
| **Anomalie significative** | Accesso o tentativo di accesso fraudolento ai sistemi interni/gestiti | **KRI** | 0 / 22 | **Indicatori di rischio** | 0) Segnalazioni pervenute<br>22) Accesso o tentativo di accesso fraudolento ai sistemi interni/gestiti |

| CONTROLLI | |
|---|---|
| **Sintesi misure di controllo** | |
| ✓ Politiche di gestione del rischio (MOG/PTPC/CE)<br>✓ Politiche di gestione del rischio privacy<br>✓ Trasparenza<br>✓ Segregazione compiti/funzioni<br>✓ Controlli gerarchici<br>✓ Audit/ Controlli<br>✓ Sistema deleghe/procure<br>✓ Tracciabilità del processo<br>✓ Archiviazione documentazione rilevante<br>✓ Rotazione | ✓ Reporting<br>✓ Flussi informativi<br>✓ Informatizzazione del processo<br>✓ Formazione<br>✓ Whistleblowing<br>✓ Certificazioni<br>✓ Sistema disciplinare<br>✓ Sistema procedurale interno<br>✓ Accesso civico |
| **Misure generali** | **Misure specifiche** |
| La Società si è dotata:<br>- PTPC, Codice etico e Modello ex D.Lgs. 231/2001<br>- 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<br>- Specifiche regole a garanzia della riservatezza delle informazioni<br>- 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<br>- Regolamento per la gestione dell'accesso civico semplice e generalizzato<br>- Piano Integrato dei Controlli<br>- Flussi informativi vs organi di controllo sia periodici che ad evento<br>- Sistema di whistleblowing<br>- Piano integrato di Formazione (d.lgs 231/2001, L. 190/12, d.lgs. 231/07 e GDPR)<br>- Piano pluriennale di rotazione | - Adottata procedura interna per la gestione delle violazioni dei dati personali (data breach notification) che prevede:<br>o Rilevazione dell'Incidente di sicurezza con individuazione dei soggetti che possono rilevare incidenti di sicurezza<br>o Valutazione dell'Incidente di sicurezza, a tal fine, il DPO con il supporto della DCS e della DEPSI, raccoglie le informazioni e la documentazione ritenute necessarie per la valutazione; all'esito della valutazione del data breach, il DPO sottopone all'AD, per approvazione, la proposta di archiviazione dell'evento o di procedere con la notifica al Garante<br>- Adozione Registro data breach<br>- Tracciabilità delle operazioni effettuate<br>- Strumenti di crittografia<br>- Sistema di data loss prevention<br>- Sistema di tracciabilità degli accessi da parte degli Amministratori di Sistema<br>- Flusso vs OdV/RPTC/DPO in merito alla segnalazione di tutti i casi in cui riscontrino anomalie dei sistemi informatici (dalle quali possano evincersi accessi o tentativi di accessi abusivi, danneggiamenti, violazione delle procedure interne IT, cancellazione dei dati, ecc.) e/o incidenti informatici, ivi incluse le comunicazioni di chiusura degli stessi<br>- Reporting AD o Organi di controllo a CdA/CS su criticità |
| **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 |
| MOLTO ALTO | ADEGUATO | MEDIO BASSO | MOLTO ALTO | ADEGUATO | MEDIO 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 |
| | | | MOLTO ALTO | ADEGUATO | MEDIO BASSO | | | | | | | MOLTO ALTO | ADEGUATO | MEDIO BASSO |

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