PARTE SPECIALE D

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

AGGIORNATO DAL CONSIGLIO DI AMMINISTRAZIONE IN DATA 23 MARZO 2023

INDICE

1. I reati di cui all'art. 24 *bis* del D. Lgs. n. 231/2001

La legge 18 marzo 2008, n. 48, recante "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica (Budapest 23 novembre 2001) e norme di adeguamento dell'ordinamento interno" ha ampliato le fattispecie di reato che possono generare la responsabilità dell'ente, introducendo, nel corpo del D. Lgs. n. 231/2001 (di seguito anche "Decreto"), l'art. **24-bis "Delitti informatici e trattamento illecito di dati"** il cui testo – modificato da ultimo con D.L. 21 settembre 2019, n. 105 – stabilisce:

1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.

2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.

3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, e dei delitti di cui all'articolo 1, comma 11, del decreto legge 21 settembre 2019, n. 105 si applica all'ente la sanzione pecuniaria sino a quattrocento quote.

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

a) Art. 615 ter del codice penale (Accesso abusivo ad un sistema informatico o telematico)

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

La pena è della reclusione da uno a cinque anni:

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

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

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

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

b) Art. 617 quater del codice penale (Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche)

Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno e sei mesi a cinque anni.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da tre a otto anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

3) da chi esercita anche abusivamente la professione di investigatore privato.

c) Art. 617 quinquies del codice penale (Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche)

Chiunque, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'art. 617-quater.

d) Art. 635 bis del codice penale (Danneggiamento di informazioni, dati e programmi informatici)

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

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

e) Art. 635 ter del codice penale (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità)

Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

f) Art. 635 quater del codice penale (Danneggiamento di sistemi informatici o telematici)

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

g) Art. 635 quinquies del codice penale (Danneggiamento di sistemi informatici o telematici di pubblica utilità)

Se il fatto di cui all'articolo 635-quater è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad

ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata.

h) Art. 615 quater del codice penale (Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici)

Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino a due anni e con la multa sino a euro 5.164.

La pena è della reclusione da uno a tre anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui al quarto comma dell'articolo 617-quater ’.

i) Art. 615 quinquies del codice penale (Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)

Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l’interruzione, totale o parziale, o l’alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica,

consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329..

l) Art. 491 bis del codice penale (Documenti informatici)

Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici.

La norma sopra citata estende le disposizioni in tema di falso in atto alle falsità riguardanti un documento informatico; i reati richiamati sono i seguenti:

- **Articolo 476 codice penale** (Falsità materiale commessa dal pubblico ufficiale in atti pubblici)

Il pubblico ufficiale, che, nell'esercizio delle sue funzioni,forma, in tutto o in parte, un atto falso o altera un atto vero, è punito con la reclusione da uno a sei anni.

Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a dieci anni.

- **Articolo 477 codice penale** (Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative)

Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, contraffà o altera certificati o autorizzazioni amministrative, ovvero, mediante contraffazione o alterazione, fa apparire adempiute le condizioni richieste per la loro validità, è punito con la reclusione da sei mesi a tre anni.

- **Articolo 478 codice penale** (Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti)

Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, supponendo esistente un atto pubblico o privato, ne simula una copia e la rilascia in forma legale, ovvero rilascia

una copia di un atto pubblico o privato diversa dall'originale, è punito con la reclusione da uno a quattro anni.

Se la falsità concerne un atto o parte di un atto, che faccia fede fino a querela di falso, la reclusione è da tre a otto anni.

Se la falsità è commessa dal pubblico ufficiale in un attestato sul contenuto di atti, pubblici o privati, la pena è della reclusione da uno a tre anni.

- **Articolo 479 codice penale** (Falsità ideologica commessa dal pubblico ufficiale in atti pubblici)

Il pubblico ufficiale, che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente che un fatto è stato da lui compiuto o è avvenuto alla sua presenza, o attesta come da lui ricevute dichiarazioni a lui non rese, ovvero omette o altera dichiarazioni da lui ricevute, o comunque attesta falsamente fatti dei quali l'atto è destinato a provare la verità, soggiace alle pene stabilite nell'articolo 476.

- **Articolo 480 codice penale** (Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative)

Il pubblico ufficiale, che, nell'esercizio delle sue funzioni, attesta falsamente, in certificati o autorizzazioni amministrative, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione da tre mesi a due anni.

Con riferimento alle fattispecie sopra indicate, deve, preliminarmente, ricordarsi che in considerazione della particolare natura della Società (concessionaria di un pubblico servizio), non si può escludere che venga riconosciuta ai dipendenti/rappresentanti della Società, nello svolgimento di alcune attività, la qualifica di Pubblico Ufficiale o Incaricato di Pubblico Servizio e che, quindi, i reati in questione possano essere commessi anche dai dipendenti stessi.

In ogni caso, qualora non fosse riconosciuta loro la qualifica di Pubblico Ufficiale o Incaricato di Pubblico Servizio, i reati di falso in precedenza indicati, sono comunque

astrattamente configurabili ai fini di cui al Decreto nell'ipotesi in cui il dipendente/soggetto riferibile alla Società sia imputato di concorso esterno nei reati eventualmente commessi da coloro i quali dispongono della qualifica soggettiva prima detta. Alla luce di quanto sopra specificato, dunque, i reati possono configurarsi in tutti i casi il dipendente/soggetto riferibile alla Società contribuisca fattualmente o moralmente con atti e/o omissioni l'alterazione / modificazione / contraffazione / formazione / simulazione dei documenti informatici rilevanti ai fini dei precedenti articoli.

- **Articolo 481 codice penale** (Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità)

Chiunque, nell'esercizio di una professione sanitaria o forense, o di un altro servizio di pubblica necessità, attesta falsamente, in un certificato, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a un anno o con la multa da e 51,00 a e 516,00.

Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro.

Si veda quanto riportato nel punto precedente con la differenza che, in questo caso, il concorso deve accedere ad una condotta posta in essere dall'esercente una professione sanitaria (es. infermiere, medico, ecc.) o forense (es., avvocato).

- **Articolo 482 codice penale** (Falsità materiale commessa dal privato)

Se alcuno dei fatti preveduti dagli articoli 476, 477 e 478 è commesso da un privato, ovvero da un pubblico ufficiale fuori dell'esercizio delle sue funzioni, si applicano rispettivamente le pene stabilite nei detti articoli, ridotte di un terzo.

- **Articolo 483 codice penale** (Falsità ideologica commessa dal privato in atto pubblico)

Chiunque attesta falsamente al pubblico ufficiale, in un atto pubblico, fatti dei quali l'atto è destinato a provare la verità, è punito con la reclusione fino a due anni.

Se si tratta di false attestazioni in atti dello stato civile, la reclusione non può essere inferiore a tre mesi.

- **Articolo 484 codice penale** (Falsità in registri e notificazioni)

Chiunque, essendo per legge obbligato a fare registrazioni soggette all'ispezione dell'Autorità di pubblica sicurezza, o a fare notificazioni all'Autorità stessa circa le proprie operazioni industriali,commerciali o professionali, scrive o lascia scrivere false indicazioni è punito con la reclusione fino a sei mesi o con la multa fino a € 309,00.

- **Articolo 487 codice penale** (Falsità in foglio firmato in bianco. Atto pubblico)

Il pubblico ufficiale, che, abusando di un foglio firmato in bianco, del quale abbia il possesso per ragione del suo ufficio e per un titolo che importa l'obbligo o la facoltà di riempirlo, vi scrive o vi fa scrivere un atto pubblico diverso da quello a cui era obbligato o autorizzato, soggiace alle pene rispettivamente stabilite negli articoli 479 e 480.

- **Articolo 488 codice penale** (Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali)

Ai casi di falsità su un foglio firmato in bianco diversi da quelli preveduti dai due articoli precedenti, si applicano le disposizioni sulle falsità materiali in atti pubblici o in scritture private.

- **Articolo 489 codice penale** (Uso di atto falso)

Chiunque, senza essere concorso nella falsità, fa uso di un atto falso soggiace alle pene stabilite negli articoli precedenti, ridotte di un terzo.

- **Articolo 490 codice penale** (Soppressione, distruzione e occultamento di atti veri)

Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico vero o, al fine di recare a sé o ad altri un vantaggio o di recare ad altri un danno, distrugge, sopprime od occulta un testamento olografo, una cambiale o un altro titolo di credito trasmissibile per girata o al portatore veri, soggiace rispettivamente alle pene stabilite negli articoli 476, 477, 482, secondo le distinzioni in essi contenute.

- **Articolo 492 codice penale** (Copie autentiche che tengono luogo degli originali mancanti)

Agli effetti delle disposizioni precedenti, nella denominazione di «atti pubblici» e di «scritture private» sono compresi gli atti originali e le copie autentiche di essi, quando a norma di legge tengano luogo degli originali mancanti.

- **Articolo 493 codice penale** (Falsità commesse da pubblici impiegati incaricati di un servizio pubblico)

Le disposizioni degli articoli precedenti sulle falsità commesse da pubblici ufficiali si applicano altresì agli impiegati dello Stato, o di un altro ente pubblico, incaricati di un pubblico servizio relativamente agli atti che essi redigono nell'esercizio delle loro attribuzioni.

m) Art. 640 quinquies del codice penale (Frode informatica del soggetto che presta servizi di certificazione di firma elettronica)

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

n) Articolo 1, co. 11, D.L. 105/2019 (perimetro di sicurezza cibernetica)

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

Si segnala che, in virtù dell'attività svolta, tale fattispecie di reato non sembra allo stato applicabile alla Società in quanto non è stata individuata tra i soggetti destinatari di tali obblighi.

2. Le "attività sensibili" relative ai reati informatici

L'art. 6, comma 2, lett. a) del Decreto indica, tra gli elementi essenziali del modello di organizzazione, gestione e controllo (di seguito, il "Modello"), l'individuazione delle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto.

L'analisi dei processi aziendali svolta ha consentito di individuare, nell'ambito della struttura organizzativa ed aziendale di CEM Ambiente S.p.A. ("CEM Ambiente" o la "Società"), un'area a rischio reato denominata "gestione dei sistemi informativi", ovvero un settore e/o processo aziendale rispetto al quale è stato ritenuto astrattamente sussistente il rischio di commissione delle fattispecie di reato richiamate dall'art. 24-bis Decreto.

Nell'ambito della suddetta area sono state/i individuate/i:

- le relative **attività c.d. "sensibili"**, ovvero quelle specifiche attività al cui espletamento è connesso il rischio di commissione dei reati in questione;
- **le funzioni/ruoli aziendali coinvolti** nell'esecuzione di tali attività "sensibili" e che, astrattamente, potrebbero commettere i reati informatici sebbene tale individuazione dei ruoli/funzioni non debba considerarsi, in ogni caso, tassativa

atteso che ciascun soggetto individuato nelle procedure potrebbe in linea teorica essere coinvolto a titolo di concorso;

Si sottolinea che, in linea teorica, tali reati possono essere astrattamente commessi da tutte le funzioni aziendali e dall'Amministratore di Sistema.

Di seguito verranno riportate le attività c.d. "sensibili" ricomprese nell'area "**gestione dei sistemi informativi"**, individuata come "a rischio" con riferimento ai reati informatici.

AREA SENSIBILE N. 1 – GESTIONE DEI PROFILI UTENTE E DEL PROCESSO DI AUTORIZZAZIONE	
funzioni aziendali coinvolte	- Direzione Corporate (Sistemi IT) - Potenzialmente tutte le funzioni aziendali
attività sensibili	Si tratta dell'attività svolta dall'amministratore di sistema mediante la quale viene gestito il ciclo di vita degli utenti (creazione, modifica, disattivazione, etc.) e definite le risorse alle quali questi possono accedere. In fase di creazione di un nuovo utente, ad esso viene associato un elemento identificativo univoco denominato user-id ed un profilo di autorizzazione, gestito mediante un processo ed una procedura di autorizzazione. Il profilo di autorizzazione permette di definire le risorse alle quali l'utente può accedere (files, cartelle, programmi applicativi etc.) e la tipologia di accesso consentita (es. sola consultazione, possibilità di modificare il dato etc.).
reati astrattamente ipotizzabili	1. *Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)* 2. *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)*

	3. *Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)* 4. *Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)* 5. *Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)* 6. *Danneggiamento di sistemi informatici o telematici (art. 635 quater c. p.)* 7. *Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)* 8. *Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615 quater c.p.)* 9. *Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)* 10. *Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)*

AREA SENSIBILE N. 2 – GESTIONE DEL PROCESSO DI AUTENTICAZIONE	
funzioni aziendali coinvolte	- Direzione Corporate (Sistemi IT) - Potenzialmente tutte le funzioni aziendali.
attività sensibili	Si tratta dell'attività mediante la quale tutti gli utenti (sia gli utenti finali che gli utenti di tipo "*administrator*") accedono ai programmi applicativi, al sistema operativo nonché alle varie risorse (files, cartelle, stampanti etc.).

	L'autenticazione avviene specificando la user-id associata all'utente finale, e la relativa password. Una volta effettuata con successo l'autenticazione, l'utente può accedere a tutte e sole le risorse che sono state previamente definite in fase di definizione del profilo utente e del profilo di autorizzazione.
reati astrattamente ipotizzabili	1. *Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)* 2. *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)* 3. *Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)* 4. *Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)* 5. *Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)* 6. *Danneggiamento di sistemi informatici o telematici (art. 635 quater c. p.)* 7. *Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)* 8. *Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615 quater c.p.)* 9. *Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)*

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

AREA SENSIBILE N. 3 – GESTIONE DEL PROCESSO DI CREAZIONE, TRATTAMENTO, ARCHIVIAZIONE DI DOCUMENTI ELETTRONICI CON VALORE PROBATORIO	
funzioni aziendali coinvolte	- Direzione Corporate (Sistemi IT) - Potenzialmente tutte le funzioni aziendali
attività sensibili	Si tratta dell'attività volta a gestire la documentazione elettronica aziendale, pubblica o privata, con finalità probatoria in modo che siano monitorati gli stati di utilizzo, modifica ed archiviazione della documentazione.
reati astrattamente ipotizzabili	1. *Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)* 2. *Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)* 3. *Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.)* 4. *Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)* 5. *Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615 quater c.p.)* 6. *Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)* 7. *Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)* 8. *art. 491 bis c.p. e reati di falso correlati:*

	- *art. 476 c.p. (Falsità materiale commessa dal pubblico ufficiale in atti pubblici);* - *art. 477 c.p. (Falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative);* - *art. 478 c.p. (Falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti);* - *art. 479 c.p. (Falsità ideologica commessa dal pubblico ufficiale in atti pubblici);* - *art. 480 c.p. (Falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative);* - *art. 481 c.p. (Falsità ideologica in certificati commessa da persone esercenti un servizio di pubblica necessità);* - *art. 482 c.p. (Falsità materiale commessa dal privato)* - *art. 483 c.p. (Falsità ideologica commessa dal privato in atto pubblico)* - *art. 484 c.p. (Falsità in registri e notificazioni)* - *art. 487 c.p. (Falsità in foglio firmato in bianco. Atto pubblico)* - *art. 488 c.p. (Altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali)* - *art. 489 c.p. (Uso di atto falso)* - *art. 490 c.p. (Soppressione, distruzione e occultamento di atti veri)* - *art. 492 c.p. (Copie autentiche che tengono luogo degli originali mancanti)* - *art. 493 (Falsità commesse da pubblici impiegati incaricati di un servizio pubblico).*

AREA SENSIBILE N. 4 – GESTIONE E PROTEZIONE DELLA POSTAZIONE DI LAVORO	
funzioni aziendali coinvolte	- Direzione Corporate (Sistemi IT) - Potenzialmente tutte le funzioni aziendali
attività sensibili	Si tratta dell'attività volta ad informare l'utente della postazione di lavoro circa le modalità per una corretta gestione dei beni aziendali, della posta elettronica e della sicurezza informatica.
reati astrattamente ipotizzabili	1. *Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)* 2. *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)* 3. *Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)* 4. *Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)* 5. *Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)* 6. *Danneggiamento di sistemi informatici o telematici (art. 635 quater c. p.)* 7. *Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)* 8. *Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615 quater c.p.)* 9. *Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)* 10. *Frode informatica del soggetto che presta servizi di*

	certificazione di firma elettronica (art. 640 quinquies c.p.)

AREA SENSIBILE N. 5 – GESTIONE DEGLI ACCESSI DA E VERSO L'ESTERNO	
funzioni aziendali coinvolte	- Direzione Corporate (Sistemi IT) - Potenzialmente tutte le funzioni aziendali.
attività sensibili	Si tratta dell'attività di gestione degli accessi da e verso l'esterno, non essendo ammesso al personale l'accesso a determinati siti internet. Inoltre, la gestione degli accessi dall'esterno è implementata da standard di sicurezza ben definiti e si basa su adeguati protocolli di protezione.
reati astrattamente ipotizzabili	1. *Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)* 2. *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)* 3. *Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)* 4. *Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)* 5. *Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)* 6. *Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.)* 7. *Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)* 8. *Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.)*

AREA SENSIBILE N. 6 – GESTIONE E PROTEZIONE DELLE RETI	
funzioni aziendali coinvolte	- Direzione Corporate (Sistemi IT) - Potenzialmente tutte le funzioni aziendali.
attività sensibili	Si tratta dell'attività di gestione degli accessi da e verso l'esterno, non essendo ammesso al personale l'accesso a determinati siti internet. Inoltre, la gestione degli accessi dall'esterno è implementata da standard di sicurezza ben definiti e si basa su adeguati protocolli di protezione.
reati astrattamente ipotizzabili	1. *Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)* 2. *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)* 3. *Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)* 4. *Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)* 5. *Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)* 6. *Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.)* 7. *Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)* 8. *Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615 quater c.p.)* 9. *Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici*

	diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.) 10. *Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)*

AREA SENSIBILE N. 7 – GESTIONE DEGLI OUTPUT DI SISTEMA E DEI DISPOSITIVI DI MEMORIZZAZIONE (ES. USB, CD)	
funzioni aziendali coinvolte	- Direzione Corporate (Sistemi IT) - Potenzialmente tutte le funzioni aziendali.
attività sensibili	Si tratta dell'attività di monitoraggio e gestione degli output di sistema e dei dispositivi di memorizzazione come Hard Disk esterni, Hard Disk portatili, Compact Disk ecc..
reati astrattamente ipotizzabili	1. *Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)* 2. *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)* 3. *Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)* 4. *Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)* 5. *Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)* 6. *Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.)* 7. *Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)* 8. *Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a*

	sistemi informatici o telematici (art. 615 quater c.p.) 9. *Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)* 10. *Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)*

AREA SENSIBILE N. 8 – SICUREZZA FISICA	
funzioni aziendali coinvolte	- Direzione Corporate (Sistemi IT) - Potenzialmente tutte le funzioni aziendali.
attività sensibili	Si tratta dell'attività volta a garantire la sicurezza fisica degli ambienti e delle risorse che vi operano.
reati astrattamente ipotizzabili	1. *Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)* 2. *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)* 3. *Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)* 4. *Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)* 5. *Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)* 6. *Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.)* 7. *Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.)* 8. *Detenzione, diffusione e installazione abusiva di*

	apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615 quater c.p.) 9. *Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)* 10. *Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)*

AREA SENSIBILE N. 9 – GESTIONE DEGLI ACQUISTI DI MATERIALE IT	
funzioni aziendali coinvolte	- Direzione Corporate (Sistemi IT) - Potenzialmente tutte le funzioni aziendali.
attività sensibili	Si tratta di un'attività volta a prevedere un processo periodico di pianificazione e controllo del budget IT: ad esempio per la fornitura hardware di apparecchiature informatiche.
reati astrattamente ipotizzabili	1. *Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.)* 2. *Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.)* 3. *Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)* 4. *Danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.)* 5. *Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635 ter c.p.)* 6. *Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.)* 7. *Danneggiamento di sistemi informatici o telematici di*

	pubblica utilità (art. 635-quinquies c.p.) 8. *Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615 quater c.p.)* 9. *Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)* 10. *Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.)*

3. Il sistema dei controlli

La Società ha adottato un complesso ed articolato sistema di controlli, contenuto nelle seguenti procedure e documenti:

- Procedura per la gestione delle violazioni dei dati personali o "data breach";
- Regolamento per l'esercizio del sistema di Videsorveglianza di CEM Ambiente S.p.A.;
- Regolamento per l'esercizio dei sistemi di Videosorveglianza presso le Piattaforme Ecologiche;
- Procedura Gestione del Sistema informatico che regola:
  - le modalità di autenticazione e qualificazione utenze;
  - la gestione delle password;
  - la gestione delle dotazioni;
  - la postazione di lavoro fissa;
  - la postazione di lavoro portatile (laptop);
  - la gestione degli accessi alla rete internet-intranet e i relativi servizi;
  - i servizi di posta elettronica
  - la configurazione di hardware/software;

- l’utilizzo di telefoni fissi, fax e fotocopiatrici;
- l’utilizzo di dispositivi mobili (smartphone/tablet);
- l’utilizzo di strumenti di collaborazione e delle risorse condivise;
- l’accesso alla rete aziendale da parte di terzi;
- la protezione antivirus e autorizzazione all’utilizzo di dispositivi di memorizzazione rimovibili;
- la trasmissione delle informazioni;
- gli auditing di sistema;
- l’accesso ai dati dell’utente e la tutela della privacy;
- i sistemi di controllo graduali;
- la cessazione della disponibilità di servizi informativi e modalità di reso;
- il trattamento di dati protetti dal diritto d’autore;
- la segnalazione di anomalie/incidenti di sicurezza;

- Procedura Operativa per il monitoraggio da remoto dei sistemi di Videosorveglianza territoriale;
- Verbali di verifiche periodiche;
- Varie informative;
- Atti di nomina a Responsabile del trattamento dei dati;
- Atti di nomina ad incaricato del trattamento dei dati;
- Atto di nomina ad Amministratore di Sistema;
- Atti di nomina da parte dei Comuni soci, che designano CEM Ambiente S.p.A. in qualità di Responsabile esterno del trattamento dei dati relativamente alla gestione di TARI / ARERA;
- Atti di nomina da parte dei Comuni soci, che designano CEM Ambiente S.p.A. in qualità di Responsabile esterno del trattamento dei dati relativamente alla

gestione dei sistemi di accesso in Piattaforma Ecologica mediante CNS / CIE / CEM Card e gestione dotazioni ;

- Atto di nomina del Responsabile della protezione dei dati (RPD).

Di seguito, si menzionano i principali controlli in essere in relazione ciascuna delle macroaree sensibili sopra individuate.

a) Gestione dei profili utente e del processo di autorizzazione

Con riferimento alla presente area a rischio la Società ha adottato una serie di punti di controllo volti a prevenire il rischio che vengano integrati le fattispecie di reato sopra indicate.

In via esemplificativa e non esaustiva vengono di seguito menzionati una serie di controlli posti in essere dalla Società, la quale ha:

- attribuito il ruolo di "Amministratore di Sistema" solo ed esclusivamente al Responsabile dei Sistemi Informativi (d'ora innanzi anche solo RSI) di CEM Ambiente; tutti gli altri soggetti, a vario titolo coinvolti nelle operazioni di amministrazione o gestione di sistema, assumono la qualifica di operatori di sistema e devono operare attenendosi alle istruzioni impartite dall'RSI;
- nominato tutti i dipendenti di CEM Ambiente incaricati del trattamento dati ed assegnato ad ogni incaricato, individualmente, una o più credenziali per l'autenticazione;
- fornito istruzioni scritte a responsabili ed incaricati affinché le user – id siano utilizzate in maniera strettamente individuale;
- configurato il sistema informatico in maniera tale che le password siano modificabili autonomamente da parte degli utenti finali e che non siano memorizzate in chiaro ma venga memorizzata solamente l'impronta hash;
- instaurato un processo strutturato e tracciabile che prevede la richiesta di accesso ai dati e l'abilitazione nei necessari profili di autorizzazione, nonché, in caso di dimissioni, licenziamenti, ecc., la disattivazione immediata delle credenziali di autenticazione;

- esplicitamente vietato l'accesso ai computer client agli amministratori di sistema in assenza del dipendente interessato, prevedendo che gli accessi alla postazione client che si rendano necessari per operazioni di amministrazione e gestione di sistema dovranno avvenire alla presenza del dipendente interessato e, in ogni caso, dandone comunicazione anticipata con un termine di almeno 7 giorni.

b) Gestione del processo di autenticazione

Con riferimento alla presente area a rischio la Società ha adottato una serie di punti di controllo volti a prevenire il rischio che vengano integrati le fattispecie di reato sopra indicate.

In via esemplificativa e non esaustiva vengono di seguito menzionati una serie di controlli posti in essere dalla Società, la quale ha:

- nominato tutti i dipendenti di CEM Ambiente incaricati del trattamento dati ed assegnato ad ogni incaricato, individualmente, una o più credenziali per l'autenticazione;
- fornito istruzioni scritte a responsabili ed incaricati affinché le user – id siano utilizzate in maniera strettamente individuale;
- fornito istruzioni scritte a responsabili ed incaricati affinché le password siano mantenute segrete e non siano comunicate ad altri;
- fornito istruzioni scritte a responsabili ed incaricati affinché le password siano lunghe almeno otto caratteri e non contengano riferimenti agevolmente riconducibili al responsabile o all'incaricato.
- configurato il sistema informatico in maniera tale che le password siano modificabili autonomamente da parte degli utenti finali e che non siano memorizzate in chiaro ma venga memorizzata solamente l'impronta hash;
- instaurato un processo strutturato e tracciabile che prevede la richiesta di accesso ai dati e l'abilitazione nei necessari profili di autorizzazione, nonché, in caso di dimissioni, licenziamenti, ecc., la disattivazione immediata delle credenziali di autenticazione.

c) Gestione del processo di creazione, trattamento, archiviazione di documenti elettronici con valore probatorio.

Con riferimento alla presente area a rischio la Società ha adottato una serie di punti di controllo volti a prevenire il rischio che vengano integrati le fattispecie di reato sopra indicate.

In via esemplificativa e non esaustiva vengono di seguito menzionati una serie di controlli posti in essere dalla Società:

- i dati memorizzati sui vari server sono salvati con due volte al giorno, mediante replica su apposito storage server collocato in locale chiuso a chiave;
- alla fine del processo di salvataggio è necessario verificare che in fase di scrittura non si siano realizzate situazioni di errore, anomalia. ecc. e che i dati salvati siano effettivamente ripristinati e leggibili;
- è previsto che almeno una volta al mese venga fatto un full backup di tutti i dati su un supporto esterno di memorizzazione (hard disk esterno) da conservarsi presso altra sede aziendale;
- in caso di distruzione o danneggiamento è possibile ripristinare integralmente gli archivi in tempi compatibili con le esigenze degli incaricati ed in ogni caso non superiori ai sette giorni solari.

d) Gestione e protezione della postazione di lavoro

Con riferimento alla presente area a rischio vengono di seguito menzionati, in via esemplificativa e non esaustiva, una serie di controlli previsti dalla Società:

- blocco automatico della postazione di lavoro o del terminale in caso di prolungata inattività (tempo di inattività superiore a massimo 5 minuti);
- regolare spegnimento del computer alla fine dell'attività lavorativa quotidiana e verifica dell'avvenuto regolare spegnimento del PC da parte del dipendente;

- impostazione di una password che permette di bloccare il PC (mediante screen saver protetto da password) prima di allontanarsi anche temporaneamente dal PC;
- l'Amministratore di sistema effettua delle verifiche periodiche, a sorpresa, sull'utilizzo della postazione di lavoro, redigendo un apposito verbale all'esito della verifica.

e) Gestione degli accessi da e verso l'esterno

Con riferimento alla presente area a rischio la Società ha adottato una serie di punti di controllo, in particolare, in via esemplificativa e non esaustiva la Società:

- ha tassativamente vietato di installare componenti hardware o software senza l'autorizzazione scritta, richiesta e concessa anche tramite mail, dell'RSI;
- ha esplicitamente previsto l'utilizzo del software antivirus installato sul PC;
- esegue periodicamente dei Security Test sui firewall e sul Fortinet per verificare se vi siano vulnerabilità o configurazioni poco sicure;
- valuta periodicamente (ogni 6 mesi) il livello effettivo di protezione perimetrale della rete.

f) Gestione e protezione delle reti

Con riferimento alla presente area a rischio la Società ha adottato una serie di punti di controllo volti a prevenire il rischio che vengano integrati le fattispecie di reato sopra indicate.

In particolare, la Società esegue, periodicamente, uno screening del sistema volto ad individuare e rimuovere le vulnerabilità eventualmente presenti nei server di posta elettronica, server web e più in generale su tutti gli apparati di tipo server e sui principali programmi applicativi.

g) Gestione degli output di sistema e dei dispositivi di memorizzazione (es. USB, CD)

Con riferimento alla presente area a rischio la Società ha adottato i seguenti punti di controllo:

- L'utilizzo di supporti di memorizzazione rimovibili (es. hard disk esterni, CD ROM, DVD, chiavette USB o altri supporti magnetici/elettronici/ottici) è limitato al solo uso lavorativo per finalità di trasferimento e di backup di dati e documenti informatici.
- L'utente deve assicurarne la cancellazione sicura al termine dell'esigenza e, in caso di trattamento di dati personali o aziendali, curare la riservatezza del contenuto mediante l'adozione di idonee misure di protezione in conformità alle procedure aziendali in termini di classificazione e protezione delle informazioni aziendali.
- l supporti rimovibili devono essere comunque custoditi ed utilizzati in modo tale da impedire accessi non autorizzati da parte di terzi ed estrazione non consentita dei dati.
- Possono essere utilizzati esclusivamente supporti di memorizzazione rimovibili che siano stati messi a disposizione dall'Azienda o di cui l'utente ne abbia potuto preventivamente verificare affidabilità e provenienza (ad es. non devono essere utilizzate chiavette USB rinvenute accidentalmente che possono essere veicolo per la trasmissione intenzionale di *malware).*

h) Sicurezza fisica (include sicurezza cablaggi, dispositivi di rete, etc.)

Con riferimento alla presente area a rischio vengono di seguito menzionati, in via esemplificativa e non esaustiva, una serie di controlli previsti dalla Società:

- i server ed i principali apparati di protezione perimetrale e connettività (switch, router, firewall, centralino telefonico etc.) sono custoditi in luogo chiuso con accesso controllato. Al riguardo, CEM Ambiente ha individuato i soggetti responsabili, autorizzati all'accesso con il badge personale, della custodia delle chiavi;

- è stato istituito un registro dove vengono tracciati gli accessi alla sala server da parte di soggetti esterni. il registro contiene i dati identificativi, la data e l'ora d'entrata e di uscita, il motivo, l'indicazione di quali apparati siano stati eventualmente asportati dalla sala server, la firma del soggetto esterno e la firma del dipendente CEM Ambiente che ha compilato il registro.

i) Gestione degli acquisti di materiale IT

Con riferimento alla presente area a rischio la Società ha adottato una serie di punti di controllo volti a prevenire il rischio che vengano integrati le fattispecie di reato sopra indicate.

In particolare, la Società

- si fa rilasciare dai fornitori esterni una dichiarazione scritta di conformità dei nuovi software ai requisiti del disciplinare tecnico del D. lgs. 196/2003 ed al GDPR prima di acquistare i nuovi software;
- procede all'acquisto del materiale IT nel rispetto delle prassi e delle procedure in materia di acquisti.

4. Principi generali di comportamento

I Destinatari del Modello, nell'esecuzione della propria attività lavorativa, nonché della prestazione professionale e/o contrattuale, devono attenersi ai **principi generali di comportamento** di seguito enunciati.

In particolare, i Destinatari hanno l'obbligo di:

- **osservare** tutte le regole e i principi contenuti nel presente Modello, nel Codice Etico, leggi, regolamenti, protocolli e procedure (già adottate o che saranno implementate nelle Aree a Rischio) che disciplinano l'utilizzo dei sistemi informatici;
- **rispettare policy e procedure** adottate dalle Società per il corretto utilizzo dei sistemi informatici, nonché le procedure e misure di sicurezza adottate in materia di Protezione dei dati personali;

- **attenersi a principi di diligenza e correttezza** nell'utilizzo delle risorse informatiche e telematiche aziendali.

Inoltre, tutti i Destinatari e, in particolare, coloro i quali rivestono posizioni rilevanti nell'utilizzo e nell'amministrazione dei sistemi informatici, devono ispirare la loro azione ai seguenti principi di comportamento:

- **Riservatezza:** garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette nel corso dell'intero ciclo di vita dell'informazione, sia in formato elettronico che cartaceo, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla;
- **Integrità**: garanzia che qualunque dato, sia in formato elettronico che cartaceo, sia esatto, affidabile, corretto ed aggiornato. Si deve garantire non solo che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati, ma anche che i soggetti autorizzati non alterino o falsifichino le informazioni, che devono essere sempre corrette, esatte ed affidabili;
- **Disponibilità**: garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

Sulla base di tali principi generali, la presente parte speciale prevede l'espresso divieto a carico di tutti i destinatari del Modello di:

- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, considerati individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato rientranti tra quelle sopra considerate (art. 24-bis del D.Lgs. 231/2001);
- violare i principi e le procedure aziendali di seguito previste.

Nell'ambito delle suddette regole, è fatto divieto, in particolare, di:

a) utilizzare gli strumenti informativi per finalità estranee alle mansioni assegnate, per scopi personali o per scopi illeciti;

b) falsificare, in tutto o in parte, alterare, contraffare, abusivamente redigere, distruggere, sopprimere od occultare documenti informatici di qualsiasi tipologia (es. scritture private, contratti, dichiarazioni certificati o autorizzazioni amministrative) o simularne copia, nonché fare qualsiasi utilizzo di documenti come sopra formati;

c) introdursi abusivamente (con qualsiasi mezzo, anche utilizzando password o codici di autenticazione altrui o illecitamente acquisiti) in un sistema informatico o telematico, di altri Utenti, delle Società o di terzi, ovvero mantenersi all'interno del sistema stesso contro la volontà espressa o tacita di chi ha il diritto esclusivo di accedere allo stesso, ovvero accedere ad aree del sistema per le quali non si ha autorizzazione (ad es. accedendo a banche dati per le quali non si è stati autorizzati);

d) tentare di aggirare i sistemi di sicurezza interni al fine di effettuare operazioni non previste per il profilo di autorizzazione attribuito dal proprio Responsabile di Funzione e/o dal Responsabile Servizi Informatici;

e) divulgare in ambito esterno od interno informazioni relative ai sistemi informativi aziendali ovvero divulgare o comunicare password e codici di accesso a sistemi informatici dell'azienda o di soggetti terzi;

f) copiare o trasferire a terzi dati o software aziendali al fuori di quanto previsto dalle procedure aziendali e dai limiti delle autorizzazioni richieste, alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;

g) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei all'accesso a un sistema informatico o telematico di soggetti concorrenti, pubblici o privati, al fine di acquisire informazioni riservate;

h) svolgere attività di approvvigionamento e/o produzione e/o diffusione di apparecchiature e/o software allo scopo di danneggiare un sistema informatico o telematico, di soggetti, pubblici o privati, le informazioni, i dati o i programmi in

esso contenuti, ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento;

i) svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni relative a un sistema informatico o telematico di soggetti, pubblici o privati, al fine di acquisire informazioni riservate;

j) istallare apparecchiature per l'intercettazione, impedimento o interruzione di comunicazioni di soggetti pubblici o privati;

k) svolgere attività di modifica e/o cancellazione illecita di dati, informazioni o programmi di soggetti privati o soggetti pubblici o comunque di pubblica utilità;

l) svolgere attività di danneggiamento di informazioni, dati e programmi informatici o telematici altrui;

m) distruggere, danneggiare, rendere inservibili sistemi informatici o telematici di pubblica utilità.

Pertanto, i soggetti sopra indicati devono:

1. in tutte le operazioni di trattamento di dati, sia in formato elettronico che cartaceo, assicurare che i dati siano esatti, corretti, affidabili e, se necessario aggiornati;
2. utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
3. in caso di smarrimento o furto di sistemi, apparati, personal computer, supporti di memorizzazione contenenti dati, dati e archivi in formato elettronico o cartaceo etc., informare tempestivamente la Direzione Amministrazione & Finanze e gli uffici amministrativi e presentare denuncia all'Autorità Giudiziaria preposta;
4. evitare di introdurre e/o conservare in azienda (in forma cartacea, informatica e mediante utilizzo di strumenti aziendali), a qualsiasi titolo e per qualsiasi ragione, documentazione e/o materiale informatico di natura riservata e di proprietà di terzi, salvo acquisiti con il loro espresso consenso nonché

applicazioni/software che non siano state preventivamente approvate dalla Responsabile Servizi Informatici o la cui provenienza sia dubbia;

5. evitare di trasferire all'esterno della Società e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della Società stessa o di altra società del Gruppo, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione della Direzione interessata;
6. evitare di lasciare incustodito e/o accessibile ad altri il proprio PC oppure consentire l'utilizzo dello stesso ad altre persone (famigliari, amici, ex-dipendenti, ex-collaboratori ecc.);
7. evitare l'utilizzo di password di altri utenti aziendali, neanche per l'accesso ad aree protette in nome e per conto dello stesso, salvo espressa autorizzazione del Responsabile Servizi Informatici; qualora l'utente venisse a conoscenza della password di altro utente, è tenuto a darne immediata notizia al Responsabile Servizi Informatici;
8. Astenersi dal comunicare ad altri o diffondere le proprie password;
9. evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
10. utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività che hanno reso necessario il collegamento;
11. rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche o telematiche;
12. impiegare sulle apparecchiature della Società solo prodotti ufficialmente acquisiti dalla Società stessa o con l'autorizzazione della Società stessa;
13. astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;

14. astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
15. osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società;
16. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici;
17. per gli amministratori e gli operatori di sistema, osservare scrupolosamente quanto previsto dal Regolamento per la gestione dei sistemi informativi di CEM Ambiente S.p.A.

4.1 Ulteriori adempimenti

Al fine di evitare il rischio di commissione dei Reati di cui alla presente Parte Speciale, i Destinatari, nello svolgimento degli adempimenti amministrativi che comportino il ricorso a mezzi informatici o telematici per l'invio di dichiarazioni/comunicazioni alla P.A dovranno altresì attenersi ai seguenti principi:

- nello svolgimento degli adempimenti amministrativi che comportino il ricorso a mezzi informatici o telematici devono essere adottate specifiche procedure volte a garantire la correttezza del processo. In particolare le procedure devono:
  a) individuare espressamente il soggetto incaricato di tali adempimenti;
  b) garantire, nel rispetto di quanto previsto dalla normativa in materia di privacy, un controllo sulla correttezza nell'utilizzo dei sistemi informatici;
  c) garantire la segretezza di password e codici identificativi degli eventuali account dedicati.
- le dichiarazioni inviate alla Agenzia delle Entrate, le dichiarazioni doganali, ed ogni altra dichiarazione o comunicazione inviata per via telematica alla Pubblica Amministrazione dovrà essere veritiera ed è fatto divieto di alterazione, in qualsiasi modo, delle stesse.

- deve essere previsto un efficace sistema di segnalazione all'O.d.V. di qualsiasi disfunzione/irregolarità (ad es. connessa al deposito degli atti societari presso il registro delle imprese/all'accesso al Circuito NIS/ all'invio delle dichiarazioni all'agenzia delle Entrate ed alle autorità doganali/ ad ogni altro eventuale adempimento amministrativo da svolgersi per via telematica) che sia tale da far presumere la commissione di uno dei Reati di cui alla presente Sezione;

5. I compiti dell'OdV

Con riguardo ai compiti specifici dell'OdV, pur dovendosi intendere qui richiamati, in generale, i compiti assegnati all'OdV nella Parte Generale del Modello,", l'OdV, tra l'altro, deve:

- monitorare l'adeguatezza e l'effettività delle procedure e dei protocolli interni volti a prevenire il pericolo di commissione dei reati informatici;
- esaminare eventuali segnalazioni provenienti dagli organi di controllo e da qualsiasi dipendente, disponendo gli accertamenti ritenuti necessari;
- curare l'aggiornamento del Modello con riguardo agli aspetti di sicurezza informatica, proponendo agli organi aziendali di volta in volta competenti l'adozione delle misure ritenute necessarie o opportune al fine di preservare l'adeguatezza e/o l'effettività del Modello stesso.

L'OdV deve comunicare i risultati della propria attività di vigilanza e controllo in materia di reati informatici, al Consiglio di Amministrazione ed al Collegio Sindacale, secondo i termini indicati nella Parte Generale.