SERVICE CNDCEC S.R.L.

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO AI SENSI DEL DECRETO LEGISLATIVO N. 231/2001

PARTE SPECIALE “B” – DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

1. Le fattispecie di reato di cui all'art. 24-bis d.lgs. 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" (modificato dal d.lgs. n. 7 e 8/2016) ha ampliato le fattispecie di reato che possono generare la responsabilità dell'ente, introducendo, nel corpo del D.Lgs. 231/2001 (di seguito anche 'Decreto'), l'art. 24-bis "*Delitti informatici e trattamento illecito di dati*"**.** Preliminarmente, deve essere osservato che il Legislatore ha previsto due tipologie di reati rilevanti ai fini del Decreto:

A) i reati propriamente informatici;

B) i reati di falso commessi mediante l'utilizzo di (o su) documenti/dati informatici.

A) Con riferimento alla prima categoria di reati (reati propriamente informatici) si rintraccia una serie di elementi comuni, vale a dire:

i) elemento oggettivo: seppure le condotte possono essere materialmente diverse, si tratta di illeciti penali in cui il computer o il sistema informatico o telematico costituisce il fulcro della condotta. Ed infatti il computer o il sistema informatico o telematico rappresentano o il mezzo/ modalità di realizzazione della condotta (condotte realizzate mediante l'uso del computer), o la natura dell'oggetto materiale (condotte realizzate contro il computer - sistema informatico o telematico). Per 'sistema informatico/telematico' si intende *«una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche* (Cass. Sez. VI Pen. 4 ottobre - 14 dicembre 1999, n. 3067). Queste ultime, come si è rilevato in dottrina, sono caratterizzate dalla registrazione (o "memorizzazione") per mezzo di impulsi elettronici, su supporti adeguati di dati, cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit) numerici ("codice"), in combinazioni diverse: tali "dati", elaborati automaticamente dalla macchina, generano le informazioni costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di attribuire un particolare significato per l'utente;

ii) elemento soggettivo: sono tutti reati puniti a titolo di dolo (coscienza e volontà di commettere il reato), anche se per alcuni di essi è necessario anche il dolo specifico (vale a

dire un'intenzione ulteriore che l'agente deve avere di mira nel compiere la condotta delittuosa: es. fine di trarre profitto).

Si riporta, di seguito, la descrizione delle fattispecie incriminatrici richiamate e afferenti la categoria *sub* 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.

Il reato potrebbe configurarsi, a titolo di esempio, qualora un dipendente della Società che si occupa della gestione dei sistemi informativi per conto degli enti soci utilizzi il sistema ed i dati in esso contenuti per finalità diverse rispetto a quelle consentite.
Tale reato è altresì configurabile qualora un dipendente della Società acceda, utilizzando password indebitamente carpite, al sistema informatico altrui (ad esempio competitor, ecc.) al fine di acquisire informazioni relative alle strategie aziendali ecc.

Art. 615 quater del codice penale (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici)

Chiunque, al fine di procurare a sè o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna 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 ad un anno e con la multa sino a euro 5.164. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'art. 617 quater.

Il reato potrebbe configurarsi, ad esempio, nel caso in cui un dipendente della Società effettui un attacco di social engineering, di forza bruta al fine di individuare le credenziali di accesso ad un sistema di un competitor.
Sotto un diverso profilo il dipendente potrebbe, una volta procuratesi le credenziali, riprodurre, diffondere, comunicare o consegnare a terzi i codici, parole chiave o altri mezzi necessari all'accesso al sistema informatico. Queste ultime condotte possono essere integrate anche qualora i codici, le parole chiave o gli altri mezzi siano procurati da un soggetto terzo.

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 sei mesi a quattro 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 uno a cinque 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.

A titolo di esempio, il reato potrebbe realizzarsi qualora un dipendente effettui un attacco di c.d. sniffing mediante l'utilizzo di sistemi atti ad intercettare comunicazioni informatiche/telematiche di un competitor per finalità di spionaggio industriale e/o conseguente diffusione.

Art. 617 quinquies del codice penale (Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche)

Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte 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.

A titolo esemplificativo, il reato si configura mediante l'installazione di dispositivi tecnologici (es., sniffer e scanner di onde elettromagnetiche) volti ad intercettare le comunicazioni telefoniche, o informatiche wired e wireless.

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 ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635[1] ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.

Il reato potrebbe configurarsi, ad esempio, qualora un dipendente della Società alteri dati particolarmente rilevanti detenuti dalla Società stessa o da parte degli enti soci per conto dei quali SERVICE gestisce i sistemi informatici.

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

[1] Art. 635 Cod. Pen. (Danneggiamento):
Chiunque distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili altrui è punito, a querela della persona offesa con la reclusione fino a un anno o con la multa fino a lire seicentomila.
La pena è della reclusione da sei mesi a tre anni e si procede d'ufficio, se il fatto è commesso:
1) con violenza alla persona o con minaccia;
2) da datori di lavoro in occasione di serrate, o da lavoratori in occasione di sciopero, ovvero in occasione di alcuno dei delitti preveduti dagli artt. 330, 331 e 333;
3) su edifici pubblici o destinati a uso pubblico all'esercizio di un culto, o su altre delle cose indicate nel n. 7 dell'articolo 625;
4) sopra opere destinate all'irrigazione;
5) sopra piante di viti, di alberi o arbusti fruttiferi, o su boschi, selve o foreste, ovvero su vivai forestali destinati al rimboschimento.

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 ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

A titolo esemplificativo tale fattispecie potrebbe, astrattamente, realizzarsi nell'ipotesi in cui un dipendente della Società sfruttasse l'accesso consentito ai sistemi informatici degli enti soci per finalità di esecuzione delle prestazioni contrattuali, per danneggiare informazioni, dati e programmi in esso contenuti.

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 ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Vale l'esempio fatto sopra per il reato di cui all'art. 635 bis.

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 ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Vale l'esempio fatto sopra per il reato di cui all'art. 635 ter.

*****

B) Con riferimento alla categoria di reati precedentemente indicata sub b) - i reati di falso commessi mediante l'utilizzo di (o su) documenti/dati informatici - parimenti possono individuarsi una serie di elementi comuni:

i) definizione di 'documento informatico': qualunque supporto informatico contenente dati e informazioni aventi efficacia probatoria (quindi il documento informatico viene equiparato all'atto pubblico o alla scrittura privata avente efficacia probatoria);

ii) bene giuridico tutelato: il bene tutelato dalle norme è la "fede pubblica", vale a dire l'interesse a che i mezzi probatori siano genuini e veridici e alla certezza dei rapporti economici e giuridici;

iii) elemento oggettivo: questa tipologia di reati si concretizza nella condotta di alterare/ manomettere il documento nella sua essenza materiale, ovvero nella sua genuinità (cd 'falsità materiale'), o ancora in condotte che tendono ad incidere sul contenuto dello stesso, vale a dire sulla verità dei fatti in esso espressi (c.d. falsità ideologica);

iv) elemento soggettivo: i reati *de quo* di sono puniti solo a titolo di dolo (è esclusa quindi la punibilità per colpa: negligenza, imperizia, imprudenza inosservanza di leggi).

Art. 491-bis. del codice penale (Documenti informatici)[2]

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

La norma sopra citata estende le disposizioni in tema di **falso** in atto pubblico alle falsità riguardanti un documento informatico; i **reati** richiamati sono, pertanto, 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)**

[2] Si segnala che l'art. 491-bis c.p. è stato modificato dal D.lgs. 15 gennaio 2016, n. 7, il quale ha eliminato il riferimento ai documenti informatici privati. Di conseguenza, in sede di revisione della presente parte speciale, sono stati eliminati i riferimenti alle ipotesi di falsità relative agli atti privati.

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, segnalarsi che i dipendenti/soggetti riferibili alla Società (es. consulenti tecnici), nell'esercizio di alcune funzioni, potrebbero rivestire la qualifica di pubblico ufficiale o incaricato di pubblico servizio (per la definizione si veda la Parte Speciale A). Di conseguenza i reati di falso in precedenza indicati sono astrattamente configurabili ai fini di cui al Decreto; inoltre, anche per l'esercizio delle funzioni per le quali non rivestono la qualifica di pubblico ufficiale o incaricato di pubblico servizio, i dipendenti/soggetti riferibili alla Società potrebbero essere imputati di concorso esterno nei reati eventualmente commessi da coloro i quali dispongono della qualifica soggettiva prima detta.

- **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.

- **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.

In via esemplificativa, il reato sarebbe configurabile laddove un dipendente della Società alteri le ricevute bancarie telematiche di versamenti tributari.

- **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 e 309,00.

A titolo di esempio, un dipendente della Società potrebbe alterare il dossier da inviare all'AVCP fornendo false informazioni.

- **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.

Per le modalità esemplificative di questi reati (487 e 488) valgano le considerazioni prima espresse con riferimento ai reati commessi dai pubblici ufficiali/incaricati di pubblico servizio.

- **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.
Qualora si tratti di scritture private, chi commette il fatto è punibile soltanto se ha agito al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno.

A titolo di esempio tale fattispecie è astrattamente realizzabile qualora il dipendente della Società utilizzi documenti informatici falsi, senza aver concorso a falsificare il documento, per procurare un vantaggio alla Società.

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

Chiunque, in tutto o in parte, distrugge, sopprime od occulta un atto pubblico o una scrittura privata veri soggiace rispettivamente alle pene stabilite negli articoli 476, 477, 482 e 485, secondo le distinzioni in essi contenute. Si applica la disposizione del capoverso dell'articolo precedente.

A titolo esemplificativo, la fattispecie è astrattamente realizzabile nei casi in cui il dipendente della Società acceda in un sistema informatico altrui e distrugga documenti aventi efficacia probatoria.

- **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.

Queste fattispecie (492 e 493) sono definitorie ai fini della eventuale estensione oggettiva o soggettiva dei reati di falso.

2. Aree aziendali, attività sensibili, funzioni coinvolte, reati ipotizzabili e presidi/procedure di controllo

In occasione dell'implementazione dell'attività di *risk assessment,* funzionale all'aggiornamento del modello di organizzazione, gestione e controllo (di seguito, anche, '**Modello'**), sono state individuate, nell'ambito della struttura organizzativa ed aziendale di SERVICE CNDCEC S.R.L. (di seguito anche la '**SERVICE'** o '**Società'**):

- le **aree aziendali** potenzialmente "sensibili" rispetto alle quali è stato ritenuto astrattamente sussistente il rischio di commissione (direttamente o indirettamente) dei reati sopra indicati;
- le **attività c.d. "sensibili**", all'interno di ciascuna area, al cui espletamento è connesso il rischio di commissione dei reati sopra indicati;
- le **funzioni aziendali coinvolte** nell'esecuzione e gestione di tali attività "sensibili" e che, astrattamente, potrebbero commettere i reati sopra indicati,
- i **reati astrattamente ipotizzabili** con riferimento a ciascuna area aziendale/attività sensibile;
- i **principali presidi di controllo** in relazione a ciascuna area a rischio; in particolare, fermo restando il rispetto delle regole definite nel Modello e nei suoi protocolli (sistema di deleghe e procure, procedure, Codice Etico, ecc.), vengono indicati i principali punti di controllo che i soggetti che svolgono le loro mansioni all'interno delle aree a rischio sotto indicate sono tenuti a rispettare, al fine di prevenire e impedire il verificarsi dei reati sopra indicati.

Di seguito è riepilogato il quadro esposto con riferimento all'area "**GESTIONE SISTEMI INFORMATIVI"**, individuata come "a rischio".

GESTIONE SISTEMI INFORMATIVI	
Soggetti/Funzioni aziendali coinvolte	• Sistemi informativi – gestione sito web
Attività sensibili	a) Gestione dell'attività di manutenzione dei sistemi esistenti e gestione dell'attività di elaborazione dei dati b) Gestione della sicurezza informatica sia a livello fisico che a livello logico c) Attività di back-up dei dati e degli applicativi d) Gestione adempimenti relativi alla trasparenza (D.Lgs. 33/2013) * * * *Documenti informatici (art. 491-bis c.p.) e reati di falso correlati* *Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)* *Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)*
Reati astrattamente ipotizzabili	
Protocolli, presidi di controllo e procedure interne	**Presidi comportamentali** - Codice etico **Presidi procedurali** Per ciò che concerne la gestione dei sistemi informativi e il trattamento dei dati personali, oltre al Codice Etico, occorre fare riferimento ad ulteriori disposizioni di tipo procedurale. • Devono essere definiti sulla base di una specifica e formalizzata disposizione organizzativa ruoli e responsabilità in tema di sicurezza (Responsabile Funzione Sistemi Informativi); • Deve essere garantita la rilevazione e la tempestiva segnalazione degli incidenti sulla sicurezza, con l'indicazione delle azioni preventive da compiere e delle attività di ripristino a seguito di danneggiamento di software (es. virus), al fine di consentire le azioni correttive adeguate tempestivamente e organizzare un archivio storico, utile a fine di prevenzione e di adozione di nuove contromisure. • Devono essere formalizzati i criteri e le modalità di accesso e utilizzo (aziendali e personale) dei sistemi informativi aziendali e le regole necessarie al fine di un corretto utilizzo delle informazioni e dei beni associati alle strutture di elaborazione delle informazioni (cfr. "Disciplinare Aziendale in materia di utilizzo degli strumenti informatici"). Per quanto riguarda l'accesso e utilizzo dei sistemi informatici, l'accesso ai sistemi e agli applicativi deve avvenire sulla base di un'opportuna profilazione degli utenti, attraverso: 1)l'adozione di procedure di validazione delle credenziali di sufficiente complessità, con previsione di modifiche periodiche e previsione di cessazione del diritto di accesso al termine del rapporto di collaborazione con la Società; 2) l'aggiornamento regolare dei sistemi informativi in uso; 3) adeguate procedure di autorizzazione. In caso di esternalizzazione del servizio di gestione dei sistemi informatici o di altri servizi che comportino l'utilizzo di sistemi informatici di soggetti terzi: - qualora sia previsto il coinvolgimento di soggetti terzi nella gestione del processo in esame, gli stessi sono tenuti all'osservanza di protocolli sopra descritti; - i contratti di fornitura del servizio e le lettere di incarico a soggetti terzi per

	l'espletamento di attività svolte nell'interesse dell'azienda devono prevedere l'introduzione di specifiche clausole di esonero di responsabilità e l'attestazione della osservanza delle politiche e procedure di sicurezza delle informazioni, volte a prevenire i rischi dovuti alle eventuali connessioni esistenti tra il sistema informatico della Società ed i loro sistemi; - In caso di accordo di collaborazione esterna con un soggetto che fornisca i servizi informatici, deve essere previsto nei contratti l'inserimento di clausole che consentano alla Società di monitorare le attività svolte; - I contratti/lettere di incarico di cui sopra devono essere formalizzate e prevedere: 1) clausole di non divulgazione delle informazioni; 2) l'impegno da Parte del consulente affidatario al rispetto del Codice etico e dei protocolli specificamente indicati nel presente Modello, nonché clausole che prevedano l'applicazione di sanzioni nel caso di violazione degli obblighi previsti dal D.Lgs.231/2001. Per ciò che concerne gli adempimenti relativi alla trasparenza, le procedure da seguire sono definite da diverse norme che assumono particolare rilievo per la SERVICE, vale a dire: a) art. 1, comma 15, Legge n. 190/12: la Trasparenza dell'attività amministrativa, in ossequio al dettato costituzionale contenuto nell'art. 117, comma 2, lett. m), è assicurata dalle società a partecipazione pubblica locale mediante la pubblicazione, nei propri siti web istituzionali, delle informazioni relative ai procedimenti amministrativi, secondo criteri di facile accessibilità, completezza e semplicità di consultazione, nel rispetto delle disposizioni in materia di segreto di Stato, di segreto d'ufficio e di protezione dei dati personali. Nei siti web istituzionali delle P.A. e delle società a partecipazione pubblica sono pubblicati anche i relativi bilanci e conti consuntivi, nonché i costi unitari di realizzazione delle opere pubbliche e di produzione dei servizi erogati ai cittadini. Le informazioni sui costi sono pubblicate sulla base di uno schema-tipo redatto dall'Autorità per la vigilanza sui contratti pubblici di lavori, servizi e forniture, che ne cura altresì la raccolta e la pubblicazione nel proprio sito web istituzionale al fine di consentirne un'agevole comparazione; b) art. 1, comma 16, Legge n. 190/12: fermo restando quanto stabilito nell'art. 53 del D.Lgs. n. 165/01, come da ultimo modificato dal comma 42 del presente articolo, nell'art. 54 del "Codice dell'Amministrazione digitale" di cui al D.Lgs. n. 82/05, nell'art. 21 della Legge n. 69/09, e nell'art. 11 del D.Lgs. n. 150/09, le società partecipate assicurano i livelli essenziali (previsti al comma 15) con particolare riferimento ai procedimenti di: • autorizzazione o concessione; • scelta del contraente per l'affidamento di lavori, forniture e servizi, anche con riferimento alla modalità di selezione prescelta ai sensi del "Codice dei Contratti pubblici" relativi a lavori, servizi e forniture, di cui al D.Lgs. 50/2016. Con riferimento al procedimento di scelta del contraente, "Service s.r.l.", nel momento in cui si trova ad affidare all'esterno beni, servizi e lavori di importo superiore alla soglia di cui ai c.d. "acquisti in economia", è in ogni caso tenuta a pubblicare sul proprio siti web: - la struttura proponente; - l'oggetto del bando; - l'elenco degli operatori invitati a presentare offerte; - l'aggiudicatario;

	- l'importo di aggiudicazione; i tempi di completamento dell'opera, servizio o fornitura; - l'importo delle somme liquidate. Entro il 31 gennaio di ogni anno tali informazioni, relativamente all'anno precedente, sono pubblicate in tabelle riassuntive rese liberamente scaricabili in un formato digitale standard aperto che consenta di analizzare e rielaborare, anche a fini statistici, i dati informatici. Le partecipate trasmettono in formato digitale tali informazioni all'Autorità per la vigilanza sui contratti pubblici di lavori, servizi e forniture, che le pubblica nel proprio sito web in una sezione liberamente consultabile da tutti i cittadini, catalogate in base alla tipologia di stazione appaltante e per Regione; c) art. 1, comma 29, Legge n. 190/12: SERVICE, in quanto Società partecipata, rende noto, tramite il proprio sito web istituzionale, almeno un indirizzo di Posta elettronica certificata cui il cittadino possa rivolgersi per trasmettere istanze ai sensi dell'art. 38 del D.P.R. 445/2000 e ricevere informazioni circa i provvedimenti e i procedimenti amministrativi che lo riguardano; d) art. 1, comma 30, Legge n. 190/12: la Società, nel rispetto della disciplina del diritto di accesso ai documenti amministrativi di cui alla L. 241/1990, in materia di procedimento amministrativo, ha l'obbligo di rendere accessibili in ogni momento agli interessati, tramite strumenti di identificazione informatica di cui all'art. 65, comma 1, del CAD (D.Lgs. 82/2005), le informazioni relative ai provvedimenti e ai procedimenti amministrativi che li riguardano, ivi comprese quelle relative allo stato della procedura, ai relativi tempi e allo specifico ufficio competente in ogni singola fase.

3. Principi generali di controllo e di comportamento

In relazione alle attività sensibili sopraindicate, sono stati adottati una serie di standard di controllo volti a garantire un sistema di gestione della sicurezza informatica. In particolare, in linea con quanto previsto dalle Linee Guida di Confindustria si ravvisa la previsione nel Codice Etico aziendale di direttive su comportamenti etici ai fini della gestione delle informazioni aziendali e dei beni informatici e si adottano i seguenti presidi;

- l'adozione di una serie di controlli volti a garantire un sistema di gestione della sicurezza informatica, tra cui:
- chiara identificazione e segregazione dei ruoli e delle responsabilità delle funzioni aziendali coinvolte nel processo di gestione dei sistemi informativi;
- adozione di specifici dispositivi hardware e software specifici per il salvataggio dei dati;
- definizione formale della frequenza dei back-up, delle modalità e dei tempi di conservazione dei supporti per i dati;
- affidamento della gestione dell'IT, incluse le attività legate alla sicurezza, mediante contratto di outsourcing;
- divieto di lasciare attiva una sessione di lavoro in caso di loro allontanamento dal PC;
- limitazioni nell'utilizzo di dispositivi elettronici che prescrivono che l'accesso ad internet sia consentito per finalità attinenti l'attività lavorativa mentre viene tollerato il moderato utilizzo per fini personali purché lo stesso, direttamente o indirettamente, non costituisca reato;
- adozione di account di posta elettronica certificata (P.E.C.);
- accesso alla rete ai sistemi aziendali soggetto ad autenticazione mediante l'uso di UserID e Password, la quale è soggetta a scadenza e a 'criteri di robustezza';
- protezione dei sistemi informatici con appositi antivirus;
- divieto di installazione di software non autorizzati su PC aziendali e installazione di software protetti, con accesso consentito solo a utenti dotati di un profilo con privilegi di amministratore;
- redazione di file Log per le varie attività dei sistemi informativi.

Tutti le risorse aziendali 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:

1. **integrità:** consistente nella garanzia che ogni dato aziendale sia realmente e completamente rappresentativo, in maniera oggettiva e senza interpretazioni, dei contenuti a cui si riferisce. Tale obiettivo si persegue tramite l'adozione di opportune contromisure che impediscano alterazioni incidentali o intenzionali che ne possono mutare il significato originale o, in alternativa, forniscano la possibilità di rilevare la suddetta alterazione del dato e di recuperare il dato integro;
2. **riservatezza:** consistente nella garanzia che un dato aziendale venga reso disponibile solamente alle applicazioni ed agli utenti incaricati e autorizzati al suo utilizzo;
3. **disponibilità:** consistente nella garanzia di reperibilità dei dati aziendali in funzione delle esigenze di continuità dei processi aziendali e di rispetto delle norme (di legge e non) che impongono la conservazione storica o determinati livelli di servizio.

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 dall'art. 24-bis del Decreto;
- violare i principi previsti dalle procedure aziendali adottate dalla Società.

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

a) alterare documenti informatici, pubblici o privati, aventi efficacia probatoria;

b) accedere/mantenersi abusivamente al sistema informatico o telematico di soggetti pubblici o privati;

c) accedere abusivamente al proprio sistema informatico o telematico al fine di alterare e /o cancellare dati e/o informazioni;

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

e) detenere e utilizzare abusivamente codici, parole chiave o altri mezzi idonei

all'accesso al proprio sistema informatico o telematico al fine di acquisire informazioni riservate;

f) 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;

g) svolgere attività fraudolenta di intercettazione, impedimento o interruzione di comunicazioni;

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

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

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

Pertanto, i soggetti sopra indicati devono:

1. utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
2. 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 e per motivi strettamente lavorativi;
3. evitare di trasferire all'esterno della Società e/o trasmettere files, documenti, o qualsiasi altra documentazione riservata di proprietà della Società stessa, se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni;
4. evitare l'utilizzo di strumenti software e/o hardware atti a intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
5. utilizzare la connessione a Internet per gli scopi e il tempo strettamente necessario allo svolgimento delle attività lavorative;
6. rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse

informatiche;

7. impiegare sulle apparecchiature della Società solo prodotti ufficialmente acquisiti dalla Società stessa;

8. astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;

9. astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;

10. osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società;

11. osservare scrupolosamente quanto previsto dalle politiche di sicurezza aziendali per la protezione e il controllo dei sistemi informatici.