PARTE SPECIALE – DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI I DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI

Sommario

1. I DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI RICHIAMATI DALL'ARTICOLO 24 BIS DEL D.LGS. 231/2001

La conoscenza della struttura e delle modalità realizzative dei reati, alla cui commissione da parte dei soggetti qualificati ex art. 5 del d.lgs. 231/2001 è collegato il regime di responsabilità a carico dell'ente, è funzionale alla prevenzione dei reati stessi e quindi all'intero sistema di controllo previsto dal decreto.

A tal fine, si riporta di seguito una descrizione dei reati richiamati dall'art. 24-bis del d.lgs. 231/2001.

1.2 DOCUMENTI INFORMATICI (ART. 491 BIS DEL CODICE PENALE)

Questo reato si realizza nel caso di compimento di una condotta illecita di falso relativamente a documenti informatici pubblici o privati aventi efficacia probatoria. In particolare, le falsità concernenti documenti e atti informatici rilevano ai fini del d. lgs. 231/2001, se riferite alle disposizioni indicate dal capo stesso e riferite agli atti pubblici e alle scritture private, che per semplicità, si riportano di seguito.

- ART. 476 C.P. - FALSITÀ MATERIALE COMMESSA DAL PUBBLICO UFFICIALE IN ATTI PUBBLICI: vi incorre 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.

- ART. 477 C.P. - FALSITÀ MATERIALE COMMESSA DAL PUBBLICO UFFICIALE IN CERTIFICATI O AUTORIZZAZIONI AMMINISTRATIVE: vi incorre 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.

- 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: vi incorre 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.

- ART. 479 C.P. - FALSITÀ IDEOLOGICA COMMESSA DAL PUBBLICO UFFICIALE IN ATTI PUBBLICI: vi incorre 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.

- ART. 480 C.P. - FALSITÀ IDEOLOGICA COMMESSA DAL PUBBLICO UFFICIALE IN CERTIFICATI O IN AUTORIZZAZIONI AMMINISTRATIVE: vi incorre 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.

- ART. 481 C.P. - FALSITÀ IDEOLOGICA IN CERTIFICATI COMMESSA DA PERSONE ESERCENTI UN SERVIZIO DI PUBBLICA NECESSITÀ: vi incorre 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 Euro 51,00 a Euro 516,00. Tali pene si applicano congiuntamente se il fatto è commesso a scopo di lucro.

- ART. 482 C.P. - 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.

- ART. 483 C.P. - FALSITÀ IDEOLOGICA COMMESSA DAL PRIVATO IN ATTO PUBBLICO: vi incorre 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.

- ART. 484 C.P. - FALSITÀ IN REGISTRI E NOTIFICAZIONI: vi incorre 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 Euro 309,00.

- ART. 485 C.P. - FALSITÀ IN SCRITTURA PRIVATA: vi incorre chiunque, al fine di

procurare a sé o ad altri un vantaggio o di recare ad altri un danno, forma, in tutto o in parte, una scrittura privata falsa, o altera una scrittura privata vera, è punito, qualora ne faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considerano alterazioni anche le aggiunte falsamente apposte a una scrittura vera, dopo che questa fu definitivamente formata.

- ART. 486 C.P. - FALSITÀ IN FOGLIO FIRMATO IN BIANCO. ATTO PRIVATO: vi incorre chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, abusando di un foglio firmato in bianco, del quale abbia il possesso per un titolo che importi l'obbligo o la facoltà di riempirlo, vi scrive o fa scrivere un atto privato produttivo di effetti giuridici, diverso da quello a cui era obbligato o autorizzato, è punito, se del foglio faccia uso o lasci che altri ne faccia uso, con la reclusione da sei mesi a tre anni. Si considera firmato in bianco il foglio in cui il sottoscrittore abbia lasciato bianco un qualsiasi spazio destinato a essere riempito.

- ART. 487 C.P. - FALSITÀ IN FOGLIO FIRMATO IN BIANCO. ATTO PUBBLICO: vi incorre 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.

- ART. 488 C.P. - 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.

- ART. 489 C.P. - USO DI ATTO FALSO: vi incorre 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.

- ART. 490 C.P. - SOPPRESSIONE, DISTRUZIONE E OCCULTAMENTO DI ATTI VERI: vi

incorre 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.

- ART. 492 C.P. - 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.

- ART. 493 C.P. - 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.

1.3 ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO (ART.615 TER CODICE PENALE) PARTE SPECIALE DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI pag. 163

Questo reato si realizza tramite la condotta di un soggetto che si introduce abusivamente 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.

Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- per la fattispecie sopraccitata, la pena è generalmente della reclusione fino a tre anni e il delitto si punisce a querela della persona offesa;
- la pena è, invece, della reclusione da uno a cinque anni e si procede d'ufficio:

1) se il fatto e' 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 e' 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;

- la pena è della reclusione da uno a cinque anni e da tre a otto anni, nonché si procede d'ufficio, se, rispettivamente, l'introduzione abusiva o il mantenimento contro la volontà dell'avente diritto, 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.

1.4 DETENZIONE E DIFFUSIONE ABUSIVA DI CODICI DI ACCESSO A SISTEMI INFORMATICI O TELEMATICI (ART. 615 QUATER CODICE PENALE)

La fattispecie si concretizza allorquando un soggetto, al fine di procurare a sé 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.

Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- la pena è della reclusione sino ad un anno e della multa sino a 5.164 euro, aumentata se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617 quater.

1.5 DIFFUSIONE DI APPARECCHIATURE, DISPOSITIVI O PROGRAMMI INFORMATICI DIRETTI A DANNEGGIARE O INTERROMPERE UN SISTEMA INFORMATICO O TELEMATICO (ART. 615 QUINQUIES DEL CODICE PENALE)

Il reato consiste nella condotta messa in atto da soggetto che, 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, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.

Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- la pena è della reclusione sino a due anni e della multa sino a euro 10.329 euro.

1.6 INTERCETTAZIONE, IMPEDIMENTO O INTERRUZIONE ILLECITA DI COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617 QUATER DEL CODICE PENALE)

Tale reato consiste nell'intercettazione, nell'impedimento o nell'interruzione fraudolenta di comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi.

Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- la pena è della 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 sopraccitate comunicazioni;

- i delitti sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena e' 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.

1.7 INSTALLAZIONE DI APPARECCHIATURE ATTE AD INTERCETTARE, IMPEDIRE OD INTERROMPERE COMUNICAZIONI INFORMATICHE O TELEMATICHE (ART. 617QUINQUIES DEL CODICE PENALE)

Questo reato condanna la condotta di quei soggetti che, fuori dai casi consentiti dalla legge, installano apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;

- la pena è della reclusione da uno a quattro anni; mentre della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617 quater.

1.8 DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (ART. 635 BIS DEL CODICE PENALE)

Il reato condanna la condotta dei soggetti che distruggono, deteriorano, cancellano, alterano o sopprimono informazioni, dati o programmi informatici altrui.

Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- salvo che il fatto costituisca più grave reato, la pena è della reclusione da sei mesi a tre anni e si procede a querela della persona offesa;
- se ricorre una o più delle circostanze di cui al numero 1) del secondo comma dell'articolo 635, ovvero se il fatto e' commesso con abuso della qualità di operatore del sistema, la pena e' della reclusione da uno a quattro anni e si procede d'ufficio.

1.9 DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI UTILIZZATI DALLO STATO O DA ALTRO ENTE PUBBLICO O COMUNQUE DI PUBBLICA UTILITÀ (ART. 635 TER DEL CODICE PENALE)

Tale condotta criminosa consiste nella commissione di 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.

Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- la pena è della 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.

1.10 DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI (ART. 635 QUATER DEL CODICE PENALE)

Tale delitto punisce la condotta del soggetto che, mediante le condotte di cui all'art. 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.

Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- salvo che il fatto costituisca più grave reato, la pena è della 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.

1.11 DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI DI PUBBLICA UTILITÀ (ART. 635 QUINQUIES DEL CODICE PENALE)

Strutturalmente questa ipotesi criminosa è simile a quella trattata al punto precedente, ad eccezione del fatto che le sopraccitate condotte sono dirette a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

Si precisa che:

- si tratta di reato comune, la cui condotta può essere realizzata da chiunque;
- 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.

1.12 FRODE INFORMATICA DEL SOGGETTO CHE PRESTA SERVIZI DI CERTIFICAZIONE DI FIRMA ELETTRONICA (ART. 640 QUINQUIES DEL CODICE PENALE)

Il reato si concretizza qualora 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.

Si precisa che la pena è della reclusione fino a tre anni e della multa da 51 a 1.032 euro.

2. FUNZIONE DELLA PARTE SPECIALE – DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI -

La presente Parte Speciale si riferisce a comportamenti posti in essere dagli Organi Sociali, dai Dipendenti, nonché dai Consulenti, come meglio definiti nella parte generale, coinvolti nelle Fattispecie di attività sensibili.

Obiettivo della presente parte speciale è garantire che i soggetti sopra individuati mantengano condotte conformi ai principi di riferimento di seguito enunciati, al fine di prevenire la commissione dei reati indicati nel paragrafo precedente.

Nella parte generale sono stati richiamati i principi ispiratori della normativa e i presidi principali per l'attuazione delle vigenti disposizioni in materia.

In questa parte speciale sono individuati i principi di riferimento per la costruzione del Modello, specificamente previsti in relazione alle Fattispecie di attività sensibili individuate al fine di prevenire la commissione dei delitti informatici e di trattamento illecito di dati.

3. PRINCIPI DI RIFERIMENTO GENERALI

3.1 IL SISTEMA ORGANIZZATIVO IN GENERALE

Nell'espletamento di tutte le operazioni attinenti alla gestione e all'utilizzo dei sistemi informativi aziendali, i Dipendenti e gli Organi Sociali devono adottare e rispettare:

1. il sistema di controllo interno, e quindi le procedure aziendali, la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale aziendale e organizzativa;

2. le norme inerenti la gestione e l'utilizzo dei sistemi informativi di Energeko Gas Italia;

3. il sistema disciplinare;

4. in generale, la normativa applicabile.

Si precisa che Energeko Gas Italia ha delegato ad un provider terzo la gestione dei sistemi informativi aziendali, l'implementazione, il monitoraggio e la corretta applicazione delle relative procedure di controllo, disciplinando compiutamente gli aspetti relativi a condizioni e modalità di erogazione del servizio all'interno di uno specifico contratto di service (si veda al riguardo anche quanto espressamente previsto dal successivo paragrafo).

In virtù degli accordi contrattuali in essere tra le parti, al fine di presidiare l'attività sensibile in oggetto, il service provider, su indicazioni specifiche di Energeko Gas Italia, adotta tutte le misure di cui al successivo paragrafo, garantendo piena conformità dei servizi erogati rispetto ai criteri stabiliti all'interno dei contratti ed essendo pertanto responsabile di eventuali inadempienze.

3.2 PRINCIPI GENERALI DI COMPORTAMENTO

La presente parte speciale prevede l'espresso divieto a carico degli Organi Sociali (in via diretta) e dei lavoratori dipendenti e dei consulenti di Energeko Gas Italia (limitatamente rispettivamente agli obblighi contemplati nelle specifiche procedure e agli obblighi contemplati nelle specifiche clausole contrattuali) 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 previste nella presente parte speciale.

La presente Parte Speciale comporta, conseguentemente, l'obbligo a carico dei soggetti sopra indicati di rispettare scrupolosamente tutte le leggi vigenti ed in particolare di:

1. impegnarsi a non rendere pubbliche tutte le informazioni loro assegnate per l'utilizzo delle risorse informatiche e l'accesso a dati e sistemi (avuto particolare riguardo allo username ed alla password, anche se superata, necessaria per l'accesso ai sistemi dell'Azienda);

2. attivare ogni misura ritenuta necessaria per la protezione del sistema, evitando che terzi possano avere accesso allo stesso in caso di allontanamento dalla postazione (uscita dal sistema o blocco dell'accesso tramite password);

3. accedere ai sistemi informativi unicamente a mezzo dei codici identificativi assegnati al singolo soggetto e provvedere, entro le scadenze indicate dal Responsabile ICT Governance, alla modifica periodica della password;

4. astenersi dal porre in essere qualsivoglia comportamento che possa mettere a rischio la riservatezza e/o l'integrità dei dati aziendali;

5. assicurare la veridicità delle informazioni contenute in qualsivoglia atto e/o documento informatico.

Nell'ambito dei suddetti comportamenti, è fatto divieto, in particolare, di:

a) intraprendere azioni atte a superare le protezioni applicate ai sistemi informativi aziendali;

b) installare alcun programma, anche se attinente all'attività aziendale, senza aver prima interpellato il Responsabile ICT Governance;

c) accedere alla rete aziendale, attraverso una connessione alternativa rispetto a quella messa a disposizione da parte dell'Azienda, al fine di eludere il sistema di accesso protetto implementato;

d) accedere in maniera non autorizzata ai sistemi informativi di terzi, né alterarne in alcun modo il loro funzionamento, al fine di ottenere e/o modificare, senza diritto, dati, programmi o informazioni;

Infine, nei confronti di terze parti contraenti (es.: collaboratori, consulenti, partner, fornitori, ecc.), identificate anche in funzione di specifici criteri di importo e significatività della fornitura e coinvolte nello svolgimento di attività a rischio rispetto ai

delitti informatici e trattamento illecito di dati e che operano per conto o nell'interesse di Energeko Gas Italia, i relativi contratti, secondo precisi criteri di selezione definiti nel presente Modello, devono:

- essere definiti per iscritto, in tutte loro condizioni e termini;

- contenere clausole standard al fine del rispetto del D. Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti dal Decreto);

- contenere apposita dichiarazione dei medesimi con cui si affermi di essere a conoscenza della normativa di cui al D. Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti dal Decreto) e di impegnarsi a tenere comportamenti conformi al dettato della norma;

- contenere apposita clausola che regoli le conseguenze della violazione da parte degli stessi delle norme di cui al D. Lgs. 231/2001 (ovvero, se si tratta di soggetto straniero o operante all'estero, al rispetto della normativa internazionale e locale relativa, in particolare, a comportamenti configuranti ipotesi corrispondenti ai delitti informatici e trattamento illecito di dati previsti dal Decreto) (es. clausole risolutive espresse, penali).

4. LE "ATTIVITÀ SENSIBILI RELATIVE AI DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI" AI FINI DEL D.LGS. 231/2001

Le attività sensibili individuate, in riferimento ai Delitti informatici e di trattamento illecito di dati richiamati dall'art. 24-bis del d.lgs. 231/2001, sono le seguenti:

- Utilizzo di risorse e informazioni di natura informatica o telematica, ovvero di qualsiasi altra opera dell'ingegno protetta da diritto d'autore (con particolare riferimento alle occasioni di reato "Gestione delle informazioni relative all'accesso alle risorse informatiche, ai dati ed ai sistemi info-telematici" e "Invio telematico di atti, documenti e scritture").

5. PRINCIPI GENERALI DI CONTROLLO

I Principi generali di controllo posti a base degli strumenti e delle metodologie utilizzate per strutturare i presidi specifici di controllo possono essere sintetizzati come segue:

- SEGREGAZIONE DELLE ATTIVITÀ: si richiede l'applicazione del principio di separazione delle attività tra chi autorizza, chi esegue e chi controlla;

- ESISTENZA DI PROCEDURE/NORME/CIRCOLARI: devono esistere disposizioni aziendali e procedure formalizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili nonché modalità di archiviazione della documentazione rilevante;

- POTERI AUTORIZZATIVI E DI FIRMA: i poteri autorizzativi e di firma devono: i) essere coerenti con le responsabilità organizzative e gestionali assegnate, prevedendo, ove richiesto, l'indicazione delle soglie di approvazione delle spese; ii) essere chiaramente definiti e conosciuti all'interno della Società;

- TRACCIABILITÀ: ogni operazione relativa all'attività sensibile deve essere adeguatamente registrata. Il processo di decisione, autorizzazione e svolgimento dell'attività sensibile deve essere verificabile ex post, anche tramite appositi supporti documentali e, in ogni caso, devono essere disciplinati in dettaglio i casi e le modalità dell'eventuale possibilità di cancellazione o distruzione delle registrazioni effettuate.

6. PRINCIPI DI RIFERIMENTO SPECIFICI RELATIVI ALLE REGOLAMENTAZIONE DELLE SINGOLE ATTIVITÀ SENSIBILI

Ai fini dell'attuazione delle regole elencate al precedente capitolo 3, oltre che dei principi generali contenuti nella parte generale del presente Modello e dei principi generali di controllo di cui al capitolo 5, nel disciplinare le Fattispecie di attività sensibili di seguito descritta, dovranno essere osservati anche i seguenti principi di riferimento.

6.1 UTILIZZO DI RISORSE E INFORMAZIONI DI NATURA INFORMATICA O TELEMATICA OVVERO DI QUALSIASI ALTRA OPERA DELL'INGEGNO PROTETTA DA DIRITTO D'AUTORE

La regolamentazione dell'attività deve prevedere:

- l'implementazione di un approccio di governance dei sistemi informativi aziendali improntato al rispetto degli standard di sicurezza attiva e passiva, volti a garantire l'identità degli utenti e la protezione, la confidenzialità, l'integrità e la disponibilità dei dati. In particolare Energeko Gas Italia ha implementato un sistema centralizzato per la gestione delle componenti software, che, pertanto, non possono essere aggiornate o modificate in alcun modo da parte del singolo utente;

- la possibilità di accedere ai sistemi informativi solo previa opportuna identificazione da parte dell'utente, a mezzo username e password assegnati originariamente dall'Azienda. Per i sistemi di identificazione e accesso Energeko Gas Italia ha definito un iter tale per cui ogni utente ha necessità di inserire una password - costituita da un codice alfanumerico con un numero minimo di caratteri - per "loggarsi" e accedere ai sistemi;

- l'obbligo di cambiamento della password, a seguito del primo accesso, e la periodicità di modifica della suddetta password a seconda della frequenza di utilizzo e della criticità dei dati cui si accede per mezzo della stessa. In particolare il sistema informativo di Energeko Gas Italia prevede che ciascun utente modifichi la propria password periodicamente e comunque non oltre 60 giorni dalla registrazione. Qualora l'utente non provveda alla modifica di propria iniziativa, il sistema è strutturato in modo da inviare in automatico alert preliminari alcuni giorni prima che la password scada. Decorso anche questo termine, il sistema obbliga l'utente al cambio password per poter accedere al sistema;il monitoraggio, con frequenza periodica, di tutti gli accessi e le attività svolte sulla rete aziendale nei limiti e con le modalità di cui alla vigente normativa.

Energeko Gas Italia prevede una lista con un elenco dettagliato di siti inaccessibili ai propri utenti;

- la registrazione e la verifica di tutti gli accessi e le attività svolte sulla rete aziendale da remoto, nei limiti e con le modalità di cui alla vigente normativa. In particolare gli utenti autorizzati da Energeko Gas Italia hanno la possibilità di accedere alla rete da remoto

tramite check-point VPN - previa espressa autorizzazione del Responsabile gerarchico, oppure utilizzando esclusivamente la mail, con l'autorizzazione del Responsabile gerarchico e dopo aver seguito un corso sulla sicurezza informatica;

- Inoltre l'Ufficio del Personale comunica tutte le assunzioni e le cessazioni, nonché tutti i passaggi di stato/mansioni che possono impattare sulla gestione delle utenze informatiche, in modo che vengano attivate tutte le utenze necessarie. Si sottolinea che, al fine di abilitare le utenze, è necessaria l'autorizzazione del diretto superiore dell'utente richiedente.

La cessazione dei rapporti lavorativi comportano la disattivazione delle utenze. E' previsto in ogni caso che, decorsi 60 giorni dalla data di ultimo utilizzo, le utenze vengano comunque disattivate;

- l'adeguata formazione di ogni risorsa sui comportamenti da tenere per garantire la sicurezza dei sistemi informativi e sulle possibili conseguenze, anche penali, che possono derivare dalla commissione di un illecito.

7. I CONTROLLI DELL'ORGANISMO DI VIGILANZA

Fermo restando il potere discrezionale di attivarsi con specifici controlli a seguito delle segnalazioni ricevute, l'Organismo di Vigilanza effettua periodicamente controlli a campione sulle attività di Energeko Gas Italia potenzialmente a rischio di compimento dei Delitti informatici e di trattamento illecito di dati che sono state incluse nel piano di lavoro approvato dall'Organismo stesso, in funzione della valutazione del rischio assegnata in sede di predisposizione del Modello e nel corso dei suoi successivi aggiornamenti (si veda al riguardo l'Allegato 1 al presente documento). Tali controlli sono diretti a verificare la conformità dei comportamenti in relazione ai principi espressi nel presente documento e, in particolare, alle procedure interne in essere e a quelle che saranno adottate in attuazione del presente documento.

A tal fine, si ribadisce che all'Organismo di Vigilanza viene garantito libero accesso a tutta la documentazione aziendale rilevante inerente le Fattispecie di attività sensibili.

L'Organismo di Vigilanza riferisce di detti controlli al Organismo di Gestione.