DAIKIN APPLIED EUROPE S.p.A.

Documento di Sintesi

relativo al

Modello di Organizzazione e Gestione
Decreto Legislativo n. 231/2001

“Modello Organizzativo”

Parte Speciale L

Delitti informatici e trattamento illecito dei dati.

INDICE

1. DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

1.1 Premessa

I reati di cui alla presente Parte Speciale sono richiamati all'art. 24*bis* del D. Lgs. 231/2001, introdotto dalla Legge 48/2008 di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica.
Le condotte rilevanti che possono dare origine alla responsabilità amministrativa diretta per la Società, nel cui interesse o vantaggio è stato compiuto l'illecito, hanno per oggetto i reati di cui si fornisce la descrizione nel successivo paragrafo.

1.2 La tipologia dei reati

1.2.1 Accesso abusivo ad un sistema informatico o telematico

Tale reato, previsto e punito dall'art. 615*ter* cod. pen., riguarda la condotta di colui che 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. La fattispecie è aggravata (i) 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; (ii) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; (iii) 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 suddetti fatti 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 fattispecie è ulteriormente aggravata.

1.2.2 Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Tale reato, previsto e punito dall'art. 615*quater* cod. pen., riguarda la condotta di colui che, 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.

1.2.3 Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

Tale reato, previsto e punito dall'art. 615*quinquies* cod. pen., riguarda la condotta di colui 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.

1.2.4 Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

Tale reato, previsto e punito dall'art. 617*quater* cod. pen., riguarda la condotta di colui che fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe. Salvo che il fatto costituisca più grave reato, la medesima fattispecie di illecito si realizza qualora sia rivelato, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle predette comunicazioni.

1.2.5 Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

Tale reato, previsto e punito dall'art. 617*quinquies* cod. pen., riguarda la condotta di colui che, 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.

1.2.6 Danneggiamento di informazioni, dati e programmi informatici

Tale reato, previsto e punito dall'art. 635*bis* cod. pen., riguarda la condotta di colui che, fatto salvo il caso in cui il fatto costituisca più grave reato, distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

1.2.7 Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità

Tale reato, previsto e punito dall'art. 635*ter* cod. pen., riguarda la condotta di colui che, fatto salvo il caso in cui il fatto costituisca più grave reato, 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.
La fattispecie è aggravata se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.

1.2.8 Danneggiamento di sistemi informatici o telematici

Tale reato, previsto e punito dall'art. 635*quater* cod. pen., riguarda la condotta di colui che, fatto salvo il caso in cui il fatto costituisca più grave reato, mediante le condotte di cui all'articolo 635/bis cod. pen. (sopra citato), 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.

1.2.9 Danneggiamento di sistemi informatici o telematici di pubblica utilità

Tale reato, previsto e punito dall'art. 635*quinquies* cod. pen., prevede una fattispecie aggravata della condotta di cui all'articolo 635/quater cod. pen. (sopra citato) che si realizza qualora la medesima condotta è diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

1.2.10 Falsità in un documento informatico pubblico o avente efficacia probatoria

Tale reato, ai sensi dell'art. 491/bis cod. pen., prevede che se alcuna delle falsità riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private.

1.2.11 Frode informatica del soggetto che presta servizi di certificazione di firma elettronica

Tale reato, ai sensi dell'art. 640*quinquies* cod. pen., prevede che commette il delitto in questione 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.

1.3 I reati astrattamente configurabili in Daikin Applied Europe

OMISSIS

1.4 Attività sensibili

OMISSIS

1.5 Gli impegni della società in materia di prevenzione delle fattispecie illecite analizzate.

Daikin Applied Europe si impegna ad improntare la propria attività secondo criteri di massima trasparenza e correttezza, nel rispetto della normativa applicabile e di ogni altra disposizione pertinente. A tal fine, gli impegni assunti dalla Società sono i seguenti:

- il coinvolgimento e la sensibilizzazione di tutta la struttura direttiva, dell'insieme dei dipendenti e di coloro che lavorano per conto dell'organizzazione verso una cultura di responsabilità e di attenzione alle tematiche della corretta gestione del sistema informatico e telematico aziendale;
- garantire che tutte le attività vengano condotte nel pieno rispetto delle prescrizioni legali applicabili, nonché di tutte le regole aziendali finalizzate a prevenire la possibile commissione dei reati di cui al D.Lgs. 231/01, con la consapevolezza da parte del personale, coinvolto nei processi ritenuti sensibili, dei rischi potenziali di reato di cui al medesimo D.Lgs. 231/01, art. 24*bis*;
- la realizzazione di idonei interventi formativi per il personale aziendale rispetto ai rischi potenziali di reato di cui al D.Lgs. 231/01, art. 24*bis*;
- la previsione di un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel Modello Organizzativo al fine di prevenire i reati ai sensi dell'art. 24*bis* del D.Lgs. 231/01;
- la previsione di idonei flussi informativi da parte del personale dipendente verso l'Organismo di Vigilanza della Società in merito ad ogni criticità capace di determinare il rischio di commissione dei reati di cui all'art. 24*bis,* D. Lgs. 231/2001.

Daikin Applied Europe, inoltre, assicura:

- l'esistenza di disposizioni e/o di procedure aziendali standardizzate idonee a fornire principi di comportamento, modalità operative per lo svolgimento delle attività sensibili, nonché idonee modalità di archiviazione della documentazione rilevante;
- la tracciabilità di ogni operazione afferente alle attività sensibili, con particolare riguardo a: ***i)*** la registrazione di ogni operazione; ***ii)*** la verificabilità ex post, eventualmente tramite adeguati supporti documentali, del processo decisionale, con riferimento altresì alla motivazione di ciascuna scelta operativa, a garanzia della massima trasparenza; ***iii)*** una disciplina dettagliata in ordine alla possibilità di cancellare o distruggere le registrazioni effettuate;
- un'adeguata segregazione di compiti, per quanto possibile, eventualmente anche attraverso un idoneo sistema di deleghe e procure, con separazione delle attività tra chi autorizza, chi esegue e chi controlla e con individuazione di un Responsabile delle attività sensibili;
- lo svolgimento periodico, da parte del Responsabile delle attività sensibili, di attività di monitoraggio, nonché, ove richiesto, di stesura della relativa reportistica e di trasmissione della stessa all'Organismo di Vigilanza, fermo restando l'obbligo generalizzato di segnalazione

all'Organismo di Vigilanza della Società di eventuali manomissioni o atti illegali compiuti sui mezzi informatici o telematici aziendali;

- un sistema di archiviazione della documentazione afferente alle aree sensibili, che garantisca l'impossibilità di modifica (se non con apposita evidenza) dei dati ivi conservati, nonché la possibilità di accesso ai documenti già archiviati solo alle persone autorizzate in base alle norme interne;
- l'adozione di una politica sulla sicurezza informatica previamente redatta, formalmente approvata, aggiornata periodicamente e comunicata a tutto il personale aziendale;
- l'adozione di procedure di *backup* per ciascuna rete di telecomunicazione, nonché la definizione della frequenza dell'attività, delle modalità della stessa e del periodo di conservazione dei relativi dati;
- l'esistenza di procedure per fronteggiare eventuali eventi informatici emergenziali e/o disastrosi, tramite sistemi di *incident tracking/incident handling* finalizzati, anche attraverso la previsione di opportuni canali e modalità di comunicazione per la tempestiva segnalazione di incidenti e situazioni sospette, a tracciare ed archiviare nonché gestire tutte le anomalie e le situazioni sospette che si dovessero palesare nell'utilizzo degli apparati informatici e a garantire un intervento tempestivo per la risoluzione del problema e la prevenzione di ulteriori comportamenti inadeguati;
- l'esistenza di procedure formalizzate, in ordine alla generazione ed alla protezione dei *log* delle attività sui sistemi, quantomeno nel contesto delle attività che coinvolgono dati sensibili;
- l'idoneità rispetto al ruolo ricoperto delle risorse umane (interne ed esterne) impiegate nell'area IT, al fine di ridurre rischi derivanti da azioni che ledano l'integrità, la riservatezza e la fruibilità del patrimonio informativo aziendale, nonché i rischi derivanti da usi non autorizzati del patrimonio informatico ed informativo aziendale. In particolare, a tale scopo, la Società assicura i) la verifica dell'adeguatezza, in termini di affidabilità e sicurezza, delle figure professionali selezionate, ii) l'individuazione delle responsabilità da assegnare a ciascuna risorsa e la determinazione delle condizioni del relativo rapporto di lavoro, collaborazione o consulenza, iii) la contrattualizzazione per iscritto dei rapporti con le risorse selezionate, con specifica evidenza delle clausole relative alla descrizione dei ruoli e delle responsabilità attribuiti, agli impegni di riservatezza ed ai controlli che la Società si riserva di effettuare sul relativo operato;
- la gestione dei rapporti con le controparti secondo principi di trasparenza, correttezza e veridicità;
- la formalizzazione e la documentazione degli incarichi conferiti a collaboratori esterni e consulenti, con evidenza delle motivazioni della scelta del collaboratore e/o del consulente (anche in considerazione del tipo di attività affidata ed il luogo ove la medesima deve essere svolta) e delle considerazioni sul prezzo applicato e sulla sua coerenza e congruità;
- il controllo sull'attività posta in essere, per conto della Società, da collaboratori esterni e consulenti, nonché sulle attività di gestione e conservazione della relativa documentazione.

OMISSIS

1.6 Principi e norme di comportamento per i Destinatari

I Destinatari, individuati alla stregua di quanto specificato nella Parte Generale (punto 3.5), **devono**:

- astenersi dal porre in essere condotte capaci di realizzare i reati di cui al D.lgs. 231/01;

- astenersi dal porre in essere condotte che, sebbene non integrino le ipotesi di cui al D.lgs. 231/01, siano potenzialmente in grado di configurarle;
- agire nel rispetto dei poteri di rappresentanza e di firma, nell'ambito delle deleghe e procure conferite;
- tenere un comportamento corretto e trasparente, nel rispetto delle norme di legge e delle procedure aziendali interne, in tutte le attività;
- utilizzare gli strumenti informatici aziendali e assegnati nel rispetto delle procedure aziendali in vigore ed esclusivamente per l'espletamento della propria attività lavorativa;
- utilizzare la navigazione in internet e la posta elettronica esclusivamente per le attività lavorative;
- custodire accuratamente le proprie credenziali d'accesso ai sistemi informativi utilizzati, evitando che soggetti terzi possano venirne a conoscenza, e aggiornare periodicamente le password;
- custodire accuratamente le risorse informatiche aziendali o di terze parti (es. personal computer fissi o portatili) utilizzate per l'espletamento delle attività lavorative;
- rispettare le policy di sicurezza concordate e definite con le terze parti per l'accesso a sistemi o infrastrutture di queste ultime.

A tutti i Destinatari del presente Modello (individuati a norma del punto 3.5 della Parte Generale), sono rivolti i seguenti divieti, quali principi generali di comportamento:

- divieto 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;
- divieto di violare i principi e le procedure aziendali previste nella presente Parte Speciale;
- divieto di accedere in maniera non autorizzata ai sistemi informativi utilizzati dalla Pubblica Amministrazione o di alterarne, in qualsiasi modo, il funzionamento o di intervenire con qualsiasi modalità cui non si abbia diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico o a questo pertinenti per ottenere e/o modificare informazioni a vantaggio dell'azienda o di terzi, o comunque al fine di procurare un indebito vantaggio all'azienda od a terzi;
- divieto di porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso a sistemi informativi altrui con l'obiettivo di acquisire abusivamente, danneggiare o distruggere informazioni o dati contenuti nei suddetti sistemi informativi;
- divieto di acquisire abusivamente, alterare, danneggiare o distruggere informazioni o dati contenuti nei sistemi informativi aziendali o di terze parti o programmi informatici della Società o della Pubblica Amministrazione, per ottenere vantaggi o condizioni favorevoli per l'azienda;
- divieto di distruggere o alterare documenti informatici archiviati sulle directory di rete o sugli applicativi aziendali e, in particolare, i documenti che potrebbero avere rilevanza probatoria in ambito giudiziario;
- divieto di danneggiare, distruggere gli archivi o i supporti relativi all'esecuzione delle attività di back-up;
- divieto di detenere, diffondere o utilizzare abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- divieto di entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato;

- divieto di rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale o anche ad altri siti/sistemi;
- divieto di intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- divieto di installare, utilizzare, duplicare o diffondere a terzi programmi (software) senza essere in possesso di idonea licenza o superando i diritti consentiti dalla licenza acquistata (es. numero massimo di installazioni o di utenze);
- divieto di accedere ad aree riservate (quali server rooms, locali tecnici, ecc.) senza idonea autorizzazione, temporanea o permanente;
- divieto di accedere, per qualsivoglia finalità o utilità, senza autorizzazione ed in violazione della legge, a sistemi informatici o telematici altrui, nonché a violare i relativi limiti di accesso al sistema informatico aziendale della Società;
- il divieto, in genere, salvo particolari autorizzazioni determinate da specifiche ragioni di lavoro, anche tramite sistemi di blocco o limitazione automatica, della connessione, consultazione, navigazione, streaming ed estrazione mediante downloading, a siti web che siano considerati illeciti (e quindi, a titolo esemplificativo, siti che presentino contenuti contrari alla morale, alla libertà di culto ed all'ordine pubblico, che consentano la violazione della privacy, che promuovano e/o appoggino movimenti terroristici o sovversivi, riconducibili ad attività di pirateria informatica, ovvero che violino le norma in materia di copyright e diritto d'autore);
- il divieto di modifica delle configurazioni aziendali standard di software ed hardware aziendale e di collegamento degli strumenti informatici o telematici aziendali a rete di connessione pubblica o privata mediante strumenti (linee telefoniche o apparecchiature wireless) di qualsiasi genere;
- divieto di alterare e/o modificare documenti informatici aventi efficacia probatoria;
- divieto di aggirare le regole di sicurezza imposte sugli strumenti informatici o telematici aziendali e sulle reti di collegamento interne.
- divieto di formare falsamente (sia sotto il profilo materiale sia per quanto attiene al contenuto) documenti societari aventi rilevanza esterna;
- divieto di lasciare documenti incustoditi contenenti informazioni riservate o codici di accesso ai sistemi;
- divieto di lasciare incustodito il proprio personal computer sbloccato;
- divieto di utilizzare i sistemi informativi a disposizione per attività non autorizzate nell'ambito dell'espletamento delle attività lavorative;
- divieto di salvare sulle unità di memoria aziendali contenuti o file non autorizzati o in violazione del diritto d'autore.

1.7 Procedure specifiche

OMISSIS

1.8 Verifiche e flusso informativo verso l'Organismo di Vigilanza

L'Organismo di Vigilanza esegue periodici controlli sulle attività a rischio, sopra indicate, al fine di verificarne la coerenza con le prescrizioni contenute nel Modello Organizzativo e, in modo particolare, con le procedure che la Società ha definito per disciplinare lo svolgimento delle attività sensibili.

Tutte le funzioni aziendali, apicali e/o sottoposte all'altrui direzione, nonché i componenti degli organi sociali, hanno l'obbligo di informare prontamente l'O.d.V. a fronte di richieste dallo stesso formulate o al verificarsi di eventi o circostanze tali da far presumere la commissione di un possibile reato di cui al D. Lgs. 231/2001.

L'O.d.V., in particolare, con riferimento ai reati di cui al D. Lgs. 231/2001, è destinatario, anche tramite la procedura di *whistleblowing*, del seguente flusso informativo:

OMISSIS