MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 231/01[1]

di

Alitalia – Società Aerea Italiana S.p.A. in amministrazione straordinaria

PARTE SPECIALE H

REATI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

[1] Approvato il 20 gennaio 2025

ALITALIA - SOCIETÀ AEREA ITALIANA S.p.A. in a.s.
SEDE LEGALE:
Piazza Almerico da Schio n.3
Pal. Bravo
00054 Fiumicino (RM)
Italia
Tel. [+39] 06 6563 1

Cap. Soc. € 103.105.126,99 i.v.
Numero di Iscrizione al Registro delle Imprese di Roma,
Codice Fiscale e Partita IVA 13029381004
R.E.A. di Roma n.1418603

INDICE

1. FINALITÁ

La Parte Speciale ha la finalità di definire linee, regole e principi di comportamento che tutti i Destinatari del Modello dovranno seguire al fine di prevenire, nell'ambito delle specifiche Attività Sensibili svolte in Alitalia - Società Aerea Italiana S.p.a. in a.s. (di seguito la "Società" ovvero "Alitalia in A.S."), la commissione dei reati previsti dal D.Lgs. 231/01 (di seguito "Decreto") e di assicurare condizioni di correttezza e trasparenza nella conduzione delle attività aziendali.

Tutte le linee guida, procedure, prassi e principi di comportamento che i Destinatari del Modello dovranno seguire e che sono contenute nella presente Parte Speciale devono essere interpretate e adottate considerando le modificazioni avvenute a seguito e per effetto dell'ammissione della Società alla procedura di amministrazione straordinaria.

Nello specifico, la Parte Speciale del Modello ha lo scopo di:

- indicare le modalità che gli esponenti dei vertici aziendali (i c.d. soggetti in "posizione apicale" o semplicemente "apicali") sono chiamati ad osservare ai fini della corretta applicazione del Modello;
- fornire all'Organismo di Vigilanza e alle altre funzioni di controllo gli strumenti per esercitare le attività di monitoraggio, controllo e verifica.

In linea generale, tutti gli esponenti aziendali dovranno adottare, ciascuno per gli aspetti di propria competenza, comportamenti conformi al contenuto dei seguenti documenti:

- Modello;
- Codice Etico;
- Procedure e disposizioni;
- Procure e deleghe;
- Ordini di servizio e Comunicazioni Organizzative;
- Ogni altro documento che regoli attività rientranti nell'ambito di applicazione del Decreto.

È inoltre espressamente vietato adottare comportamenti contrari a quanto previsto dalle vigenti norme di Legge.

Sono oggetto di analisi della presente Parte Speciale i reati contemplati nell'art. 24-*bis* del Decreto per il dettaglio si rimanda all'Allegato 1 della Parte Generale del Modello ("Elenco reati").

2. LE ATTIVITÁ SENSIBILI AI FINI DEL D. LGS. 231/2001

L'art. 6, comma 2, lett. a) del Decreto indica, tra gli elementi essenziali dei modelli di organizzazione, gestione e controllo, l'individuazione delle cosiddette attività "sensibili", ossia di quelle attività della Società nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto stesso.

2.1 Attività sensibili e modalità esemplificative di reato

Attraverso l'analisi dei processi della Società è stata individuata l'attività "sensibile" riportata in appresso, nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato previste dall'art. 24-*bis* del D. Lgs. 231/2001 (delitti informatici e trattamento illecito di dati).

L'attività sensibile nella quale potrebbe presentarsi il rischio di commissione dei reati di cui alla presente parte speciale è la **Gestione dei sistemi informativi**. Si tratta delle attività di gestione dei sistemi informatici, dal processo di autenticazione e gestione dei profili utente, alla protezione delle reti, della postazione di lavoro e degli accessi da e verso l'esterno, nonché alla sicurezza fisica dell'architettura informatica e alla gestione dei documenti elettronici con valore probatorio e degli output di sistema e dei dispositivi di memorizzazione. Tale attività include anche le *operations* IT e lo sviluppo dell'infrastruttura hardware, software e delle reti informatiche.

Di seguito sono sintetizzate le condotte illecite e i relativi riferimenti normativi, nell'ambito della presente parte speciale, "Reati informatici e trattamento illecito di dati" (art. 24-bis, D. Lgs. 231/01) [Articolo aggiunto dalla L. 18 marzo 2008 n. 48, art. 7, modificato dal D.Lgs. n. 7 e 8/2016, dal D.L. n. 105/2019 e dalla L. 90/2024]:

- falsità in un documento informatico pubblico avente efficacia probatoria (art. 491-bis c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.);
- detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.);
- detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.);

- estorsione informatica (art. 629, comma 3, c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici pubblici o di interesse pubblico (art. 635-ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.);
- detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 635-quater.1 c.p.);
- danneggiamento di sistemi informatici o telematici di pubblico interesse (art. 635-quinquies c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.);
- violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105).

3. IL SISTEMA DEI CONTROLLI

Nello svolgimento delle Attività Sensibili la Società si ispira ai seguenti *standard* di controllo:

- principi generali di comportamento;
- *standard* di controllo generali, applicabili a tutte le Attività Sensibili prese in considerazione;
- *standard* di controllo specifici, applicabili a ciascuna delle Attività Sensibili per la quale sono individuati.

3.1 Principi generali di comportamento

La presente Parte Speciale prevede l'espresso divieto - a carico dei suddetti Destinatari - di porre in essere comportamenti:

- tali da integrare le fattispecie di reato sopra considerate (art. 24-bis del Decreto);
- che, sebbene risultino tali da non costituire di per sé fattispecie di reato, rientranti tra quelle sopra considerate, possano potenzialmente diventarlo;
- non conformi alle procedure aziendali o, comunque, non in linea con i principi espressi dal presente Modello e dal Codice Etico.

Nell'ambito dei suddetti comportamenti **è fatto divieto di**:

- utilizzare le risorse informatiche (es. personal computer fissi o portatili) assegnate per finalità confliggenti con quelle lavorative;
- porre in essere condotte, anche con l'ausilio di soggetti terzi, miranti all'accesso a sistemi informativi altrui con l'obiettivo di:
  - acquisire abusivamente informazioni contenute nei suddetti sistemi informativi;
  - danneggiare, distruggere dati contenuti nei suddetti sistemi informativi;
  - utilizzare abusivamente codici d'accesso a sistemi informatici e telematici nonché procedere alla diffusione degli stessi;
- distruggere o alterare documenti informatici archiviati sulle directory di rete o sugli applicativi aziendali se non espressamente autorizzati, e in particolare i documenti che potrebbero avere rilevanza probatoria in ambito giudiziario;
- utilizzare o installare programmi diversi da quelli autorizzati;
- accedere ad aree riservate (quali server rooms, locali tecnici, ecc.) senza idonea autorizzazione, temporanea o permanente;
- aggirare o tentare di aggirare i meccanismi di sicurezza aziendali (antivirus, firewall, proxy server, ecc.);
- lasciare il proprio personal computer sbloccato e incustodito;
- rivelare ad alcuno le proprie credenziali di autenticazione (nome utente e password) alla rete aziendale o anche ad altri siti/sistemi;
- detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici di terzi o di enti pubblici;
- intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- utilizzare in modo improprio gli strumenti di firma digitale assegnati;

- alterare in qualsiasi modo il funzionamento di un sistema informatico o telematico della Pubblica Amministrazione, o intervenire senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico della Pubblica Amministrazione, al fine di procurare un vantaggio per la Società;
- entrare nella rete aziendale e nei programmi con un codice d'identificazione utente diverso da quello assegnato;
- installare, duplicare o diffondere a terzi programmi (software) senza essere in possesso di idonea licenza o in supero dei diritti consentiti dalla licenza acquistata (es. numero massimo di installazioni o di utenze);
- procurarsi abusivamente, detenere, produrre, riprodurre, importare, diffondere, comunicare, consegnare o, comunque, mettere in altro modo a disposizione di altri o installare apparecchiature, dispositivi o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero 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, nell'interesse della Società;
- costringere taluno a fare o ad omettere qualche cosa, procurando a sé o ad altri (in particolare, alla Società), un ingiusto profitto con altrui danno, mediante le richiamate condotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies c.p. ovvero con la minaccia di compierle.

3.2 Standard di controllo generali

Gli *standard* di controllo generali relativi alle Attività Sensibili sono indicati nella Parte generale del Modello.

3.3 Standard di controllo specifici

A completezza di informazione si rappresenta che, in seguito alle cessioni dei rami d'azienda, gran parte dei servizi in ambito Sistemi Informativi è fornita da Accenture S.p.A. per il tramite di ITA Airways e, per il resto dei sistemi gestiti da Alitalia, attraverso i servizi del fornitore NTT DATA Italia S.p.a.

Gli standard di controllo specifici, coerenti con le migliori *best practices* di controllo interno, definiti per l'Attività Sensibile individuata, sono di seguito descritti.

Definizione del programma operativo per l'IT
La pianificazione operativa dell'IT effettuata è necessaria per gestire tutte le risorse IT coerentemente con le priorità aziendali determinate dall'attuale scenario. Il piano operativo permette ai principali soggetti interessati di comprendere le opportunità e i limiti dell'IT, valutare la performance attuale, identificare i requisiti tecnici e le risorse umane, chiarire il livello degli investimenti necessari.

Definire l'architettura delle informazioni
I Sistemi Informativi hanno definito un modello di gestione delle informazioni aziendali e individuato i sistemi più appropriati per ottimizzare l'uso di queste informazioni. Questo comporta lo sviluppo di un sistema orientato alla classificazione dei dati e dei livelli di sicurezza. Questo processo migliora la qualità delle decisioni garantendo l'affidabilità e la sicurezza delle informazioni fornite e permette la razionalizzazione delle risorse dei sistemi informativi rispetto alle strategie aziendali.

Definire i processi, l'organizzazione e le relazioni dell'IT
La definizione di una struttura IT deve essere effettuata tenendo in debita considerazione i requisiti relativi a: risorse umane, competenze, funzioni, responsabilità, autorità, ruoli e compiti, controllo. Tale organizzazione, con particolare riferimento alla componente operativa, deve essere inquadrata in una struttura dei processi IT che assicuri non solo trasparenza e controllo ma anche il coinvolgimento dell'alta direzione e del management non IT dell'azienda.

Gestione degli investimenti IT
Seppur influenzato dell'attuale situazione economica aziendale in amministrazione straordinaria, viene definito e mantenuto un quadro di riferimento strutturato per gestire i programmi degli investimenti in IT che comprende i seguenti aspetti: costi, benefici, definizione delle priorità, una procedura formale per la redazione e gestione delle previsioni economiche. I soggetti interessati sono consultati per identificare e controllare i costi e i benefici complessivi nell'ambito delle attività IT e promuovere azioni correttive ove necessario. Questo processo promuove la collaborazione dei vari soggetti interessati all'IT e la funzione IT, rende possibile un uso efficace ed efficiente delle risorse IT, permette una gestione trasparente e responsabile dei costi complessivi dell'infrastruttura, dei benefici ottenuti per l'azienda, del ritorno degli investimenti per i quali l'IT è stato fattore abilitante.

Valutazione gestione dei rischi informatici
Sono identificati, analizzati e valutati tutti gli impatti sugli obiettivi aziendali che potrebbero essere determinati da eventi imprevisti. Sono adottate strategie di contenimento dei rischi informatici per ridurre il rischio residuo ad un livello accettato.
Alitalia in a.s., per effetto della cessazione della propria attività operativa e della cessione dei rami di azienda di cui si è detto nella Parte Generale del presente Modello, non possiede più i requisiti di società di interesse nazionale e non è più tenuta al rispetto dei requisiti NIS in materia di *cybersecurity*.
Ciononostante, la componente operativa dei sistemi e delle infrastrutture continua a presidiare gli eventi informatici che rappresentano un potenziale rischio di sicurezza.

Acquisizione e manutenzione del software applicativo

Le applicazioni sono rese disponibili come previsto dai requisiti di business. Questo processo comprende la progettazione delle applicazioni, un'adeguata considerazione dei controlli applicativi e dei requisiti di sicurezza, lo sviluppo e configurazione delle soluzioni nel rispetto degli standard e controlli definiti a livello applicativo. Questo approccio consente alle organizzazioni di supportare in modo appropriato l'operatività aziendale attraverso applicazioni informatiche adatte.

Acquisizione e manutenzione dell'infrastruttura tecnologica
L'azienda ha dei processi per gestire l'acquisizione (anche attraverso la dotazione di servizi in cloud), l'implementazione e l'aggiornamento dell'infrastruttura tecnologica. Questo richiede un approccio basato su dei piani per l'acquisizione, la manutenzione e la protezione dell'infrastruttura coerente con le strategie tecnologiche concordate, oltre alla disponibilità di ambienti di sviluppo e test. Questo approccio garantisce che ci sia un supporto tecnologico continuo per le applicazioni aziendali. In considerazione dell'attuale situazione economica aziendale in amministrazione straordinaria, rimane un subset di applicazioni che non dispongono degli ambienti di sviluppo e test per mancato investimento.

Installazioni e certificazioni di soluzioni e modifiche
I nuovi sistemi devono essere resi operativi quando lo sviluppo è completato. Questo richiede un test appropriato in un ambiente dedicato con dei dati di test significativi, la definizione del rilascio e delle istruzioni per la migrazione, la pianificazione dei rilasci e dell'effettivo passaggio in produzione, la revisione post implementazione. Questo garantisce che i sistemi applicativi siano allineati con le aspettative e i risultati concordati.

Definizione e gestione dei livelli di servizio
Una comunicazione efficace tra la Direzione Sistemi Informativi e le strutture interne, relativamente ai servizi richiesti, è resa possibile attraverso un accordo sui servizi IT e sui livelli di servizio attesi. Questo processo facilita l'allineamento tra i servizi IT e i relativi requisiti aziendali.

Gestione dei servizi di terze parti
La necessità di assicurare che i servizi forniti da terze parti (fornitori, rivenditori, partner) siano conformi ai requisiti aziendali ha comportato l'istituzione di uno strutturato processo di gestione delle terze parti. Questo processo è attuato sia attraverso l'inserimento negli accordi con le terze parti di una chiara definizione dei ruoli, delle responsabilità e delle aspettative, sia attraverso la revisione e il monitoraggio di tali accordi per garantirne l'efficacia e la conformità. Un'efficace gestione dei servizi di terze parti minimizza i rischi aziendali associati a mancate o parziali prestazioni dei fornitori.

Assicurare la continuità del servizio
La necessità di assicurare la continuità dei servizi IT ha richiesto l'utilizzo di sistemi di archiviazione dei dati per il ripristino del sistema. Un efficace processo di continuità del servizio minimizza la probabilità e l'impatto di una grave interruzione del servizio IT per processi e funzioni aziendali chiave. La continuità del servizio viene assicurata dai fornitori terzi con i quali sono stipulati contratti di servizio.

Garantire la sicurezza dei sistemi
Una gestione efficace della sicurezza protegge tutte le risorse IT al fine di minimizzare gli impatti aziendali derivanti da vulnerabilità e da incidenti. La necessità di mantenere l'integrità delle informazioni e la protezione delle risorse IT richiede un processo di gestione della sicurezza. In considerazione dell'attuale situazione economica aziendale in amministrazione straordinaria, non si dispone ad oggi di un documento che rappresenti il processo e ne mantenga l'aggiornamento. In ogni caso viene garantito il presidio operativo per la gestione delle vulnerabilità derivanti da notifiche o da potenziali incidenti.

Gestione delle configurazioni
Si rappresenta che, in seguito al processo di separazione dei servizi IT da ITA Airways, il repository delle configurazioni che veniva precedentemente utilizzato non è più in uso. Al completamento della separazione, saranno definite le nuove modalità di gestione delle configurazioni hardware e software.

Gestione dell'operatività IT
Una corretta elaborazione dei dati ha richiesto un'efficace gestione dell'elaborazione dei dati. Questo processo include la definizione di politiche e procedure operative per un'efficace gestione delle elaborazioni schedulate, la protezione di output con informazioni sensibili e il monitoraggio delle prestazioni infrastrutturali. Una gestione efficace delle operazioni aiuta a mantenere l'integrità dei dati e riduce i costi operativi dell'IT.

Assicurare la conformità a leggi e normative esterne
L'attività viene svolta su sollecitazione delle aree aziendali che supervisionano le evoluzioni normative con potenziali impatti sui sistemi a supporto. IT nel programma di attività recepisce le attività in base alle priorità per dar seguito ai programmi evolutivi previsti.

4. FLUSSI VERSO L'ORGANISMO DI VIGILANZA

L'obbligo di un flusso informativo strutturato è concepito quale strumento per garantire l'attività di vigilanza sull'efficacia ed effettività del Modello e per l'eventuale accertamento delle cause che hanno reso possibile il verificarsi dei reati in esame.

Per i dettagli inerenti il responsabile dell'invio, la periodicità di trasmissione del flusso e il suo contenuto si rinvia all'Allegato 2 alla Parte Generale.