EUROPAM S.p.A. MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 231/01

Parte speciale 8 - gestione dei sistemi informativi aziendali e del sito internet

EUROPAM S.p.a.

SEDE LEGALE
Via Sardorella, 45T · 16162 Genova (Ge) - Italia
Capitale sociale 50.000.000,00 · Cod. Fisc./P.IVA 10848200969
Società soggetta ad attività di direzione e coordinamento di Black Oils S.p.A.
Tel. 010 72271 · Fax 010 7493407
euroenergypec@pec.it

1. I reati relativi alla gestione dei sistemi informativi aziendali e del sito internet

La presente Parte Speciale si riferisce ad alcuni reati, inseriti all'interno del D. Lgs. 231/2001, accomunati dal loro impatto sulla gestione dei sistemi informativi aziendali (sia software che hardware) e sul sito internet della società Europam S.p.A.

Nell'analisi delle fattispecie rilevanti il rischio di commissione di illeciti riconducibili alle famiglie di reato di cui alle seguenti disposizioni del D.lgs. 231/2001 è di seguito rappresentato:

- Art. 24: ("*Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione Europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture");*
- Art. 24 *bis* ("*Delitti informatici e trattamento illecito di dati");*
- Art. 25 *bis* ("*Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento");*
- Art. 25 *bis 1* ("*Delitti contro l'industria e il commercio");*
- Art. 25 ter *("Reati societari",* inclusa la corruzione tra privati*);*
- Art. 25 *octies* 1 ("*Delitti in materia di strumenti di pagamento diversi dai contanti");*
- Art. 25 *novies* ("*Delitti in materia di violazione del diritto d'autore").*

2.Le attività sensibili

Nell'ambito delle analisi condotte all'interno del *risk assessment* Europam S.p.A. ha indentificato le attività sensibili. I principi di controllo successivamente menzionati si applicato a tutti i Destinatari del Modello, in particolar modo nelle situazioni in cui si trovano, per esigenze di servizio, a dover gestire i sistemi informativi interni e il sito internet:

- Gestione e monitoraggio delle licenze software utilizzate nell'ambito dei processi aziendali;
- Attività di change management;
- Utilizzo e gestione dell'infrastruttura tecnologica e dei sistemi informativi e telematici aziendali;
- Implementazione e gestione del sito internet della Società.

All'interno del medesimo documento di *risk assessment*, base del presente Modello, sono state individuate in dettaglio le associazioni logiche tra singola attività sensibile e reati presupposto, i presidi di controllo esistenti e quelli aggiunti o integrati a seguito della riflessione effettuata appunto ai fini del d. lgs. 231/2001.

I rischi specifici relativi ai reati sopra menzionati sono anche mappati all'interno delle seguenti parti speciali: Rapporti con la PA, Vendite.

Nei paragrafi seguenti si illustreranno i principi generali che devono ispirare il comportamento dei Destinatari, ed in seguito i principali presidi volti alla specifica prevenzione dei reati a rischio nelle singole Attività Sensibili, mediante descrizione o rinvio alle procedure facenti parte del sistema normativo della Società.

3.Principi generali di comportamento

I Destinatari, a qualsiasi titolo coinvolti nelle attività connesse agli adempimenti aventi ad oggetto la gestione dei sistemi informativi interni e del sito internet della società sono tenuti a osservare le disposizioni di legge esistenti in materia, le previsioni contenute nel Codice Etico e nella presente Parte Speciale del Modello.

In generale, ai Destinatari è fatto divieto di porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino o possano integrare, direttamente o indirettamente, le fattispecie di reato previste agli artt. 24 ("*Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione Europea o per il conseguimento di erogazioni pubbliche, frode*

EUROPAM S.p.a.
SEDE LEGALE
Via Sardorella, 45T · 16162 Genova (Ge) - Italia
Capitale sociale 50.000.000,00 · Cod. Fisc./P.IVA 10848200969
Società soggetta ad attività di direzione e coordinamento di Black Oils S.p.A.
Tel. 010 72271 · Fax 010 7493407
euroenergypec@pec.it

informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture"), 24 *bis* ("*Delitti informatici e trattamento illecito di dati*"), 25 *bis* ("*Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento*"), 25 *bis 1* ("*Delitti contro l'industria e il commercio"),* 25 ter *("Reati societari",* inclusa la corruzione tra privati);25 *octies* 1 ("*Delitti in materia di strumenti di pagamento diversi dai contanti*"), 25 *novies* ("*Delitti in materia di violazione del diritto d'autore*").

In particolare, è fatto divieto di:

- utilizzare le risorse informatiche (es. *personal computer* fissi o portatili, smartphone e altri device mobili) assegnate dalla Società per finalità diverse da quelle lavorative;
- alterare o intervenire abusivamente sui registri informatici della Pubblica Amministrazione al fine di assicurare un qualsiasi vantaggio alla Società;
- condividere, scambiare, utilizzare, musiche, immagini o altri contenuti in violazione della normativa del diritto d'autore;
- riprodurre abusivamente, imitare o alterare, anche attraverso l'imitazione fraudolenta, marchi o segni distintivi altrui, anche in concorso con il cliente;
- introdursi abusivamente in un sistema informatico protetto altrui (ad es. del cliente, di un partner commerciale);
- acquisire i mezzi (codici, password, etc.) necessari per accedere ad un sistema informatico altrui (per es. del cliente o del partner commerciale) protetto da misure di sicurezza, ovvero procurare tali mezzi a terzi o, ancora, fornire indicazioni o istruzioni indispensabili per l'accesso al sistema;
- produrre, riprodurre, diffondere, comunicare, consegnare abusivamente apparecchiature o dispositivi diretti a danneggiare o alterare il sistema informativo di terzi;
- intercettare ovvero captare fraudolentemente, anche tramite l'accesso ad *account* di sistemi informatici di terzi (ad es. di clienti o di partner commerciali), comunicazioni (ad es. *mail*) o, ancora, interrompere o impedire le comunicazioni medesime;
- alterare un sistema informatico di terzi ovvero intervenire senza diritto su dati, informazioni o programmi in esso contenuti, con danno del terzo (ad esempio, nel caso della gestione dell'area riservata del sito);
- impedire o turbare l'esercizio dell'attività industriale o commerciale di un terzo (es. di un cliente o di un competitor) mediante intervento sui relativi sistemi informatici.

Inoltre, i Destinatari sono tenuti ad uniformarsi ai seguenti obblighi:

- l'accesso alle informazioni che risiedono sui *server* e sulle banche dati aziendali, ivi inclusi i *client*, è limitato da strumenti di autenticazione;
- gli amministratori di sistema possono accedere a dati e sistemi aziendali solo per l'espletamento delle proprie mansioni;
- il personale dipendente è munito di univoche credenziali di autenticazione per l'accesso ai *client*;
- tutti i *server* e i *laptop* aziendali sono aggiornati periodicamente sulla base delle specifiche necessità e attraverso procedure formalmente definite;
- la rete di trasmissione dati aziendale è protetta da adeguati strumenti di limitazione degli accessi;
- i *server* sono collocati in aree dedicate e protette al fine di renderli accessibili al solo personale autorizzato; le autorizzazioni sono monitorate e aggiornate periodicamente per garantire che l'accesso ai *server* e ai locali che li ospitano siano mantenuti coerenti con le mansioni svolte dal personale;
- il personale svolge la propria attività lavorativa, presso i locali aziendali ovvero da remoto, avvalendosi dei soli strumenti *hardware* e *software* forniti e/o autorizzati dalla Società; nel caso in cui l'attività lavorativa sia svolta da remoto, il personale viene dotato di strumentazione idonea a garantire il rispetto dei principi di sicurezza degli asset aziendali, incluse le reti e le informazioni;
- il personale deve astenersi dal diffondere le informazioni ricevute dalla Società per l'uso dei mezzi informatici aziendali e l'accesso a dati, sistemi e applicazioni aziendali;
- il personale deve attuare i comportamenti richiesti dalla Società e necessari per proteggere il sistema informativo e la relativa sicurezza, diretti ad evitare che terzi possano accedervi in caso di allontanamento dalla postazione di lavoro;

EUROPAM S.p.a.
SEDE LEGALE
Via Sardorella, 45T · 16162 Genova (Ge) - Italia
Capitale sociale 50.000.000,00 · Cod. Fisc./P.IVA 10848200969
Società soggetta ad attività di direzione e coordinamento di Black Oils S.p.A.
Tel. 010 72271 · Fax 010 7493407
euroenergypec@pec.it

- il personale deve accedere al sistema informativo aziendale unicamente attraverso i codici di identificazione assegnati, provvedendo alla loro modifica periodica;
- il personale deve astenersi da qualsiasi condotta (anche colposa) che possa compromettere la riservatezza, la disponibilità e l'integrità delle informazioni e dei dati aziendali;
- il personale deve astenersi da qualsiasi condotta diretta a superare o aggirare le protezioni del sistema informativo aziendale o altrui;
- il personale deve utilizzare software e banche dati in conformità alla normativa sul diritto d'autore;
- il personale deve conservare i codici identificativi assegnati, astenendosi dal comunicarli a terzi che in tal modo potrebbero accedere abusivamente a dati aziendali riservati;
- il personale non può installare programmi senza aver preventivamente informato la funzione aziendale preposta alla gestione della sicurezza informatica;
- il personale deve astenersi dal porre in essere condotte finalizzate ad alterare o falsificare documenti informatici;
- il personale deve garantire, anche nelle comunicazioni con i terzi, la coerenza dell'uso di marchi, segni distintivi, diritti di proprietà industriale rispetto alle caratteristiche della soluzione informatica o di customer care (i messaggi non devono, infatti, essere in alcun modo ingannevoli);
- il personale deve rispettare e adeguarsi alle policy e procedure aziendali in vigore.

4.Principi di controllo

Con riferimento alle attività sensibili, come individuate all'interno della presente parte speciale, la Società ritiene necessario che i Destinatari si uniformino, nel rispetto delle regole comportamentali di cui sopra, alle procedure in essere adottate dalla Società, cui in ogni caso si rinvia, nonché ai Principi di controllo di seguito rappresentati:

- la funzione IT fornisce servizi specifici riguardanti il supporto operativo relativo ai personal computer e ai telefoni aziendali nonché a tutti gli asset informatici (ad es. manutenzione del sistema operativo, backup, manutenzione delle piattaforme di controllo ecc.);
- la funzione IT monitora, tramite apposito tool, la scadenza delle licenze dei software in uso presso la Società;
- la funzione IT gestisce le attività legate alla sicurezza informatica esterna e interna verificando, con cadenza periodica, gli accessi svolti tramite i sistemi informatici aziendali ed esaminando eventuali anomalie; provvede inoltre a condividere tempestivamente tali anomalie, secondo quanto indicato all'interno delle procedure aziendali;
- la funzione HR, di concerto con la funzione IT, garantisce adeguata formazione e informazione al personale sulle procedure adottate in materia di utilizzo degli strumenti informatici, con particolare riferimento alle tematiche riguardanti la sicurezza informatica;
- la funzione IT analizza, valuta e implementa le patch rilasciate dai fornitori al fine di correggere le anomalie di funzionamento e le vulnerabilità di sicurezza; essa inoltre tiene traccia, in apposito database, delle patch rilasciate, incluse quelle non implementate, con l'indicazione della motivazione e della valutazione degli impatti sui sistemi;
- ai lavoratori che operano da remoto (es. in regime di c.d. "lavoro agile") è messa a disposizione un'informativa sulle misure da seguire in materia di sicurezza dei sistemi informativi;
- la funzione IT provvede alla rimozione dei diritti di accesso al termine del rapporto di lavoro di ciascun dipendente;
- tutta la documentazione attestante il processo in oggetto deve essere correttamente conservata ad opera della funzione IT, per quanto di competenza, con modalità tali da impedire la modifica successiva, se non con apposita evidenza, al fine di permettere la corretta tracciabilità dell'intero processo e di agevolare eventuali controlli successivi a campione;
- in relazione al contratto di *ousourcing* per la gestione del sito della società, l'Ufficio Legale e Societario provvede a definire, in apposito accordo formalizzato e autorizzato, in forma scritta, dai soggetti aziendali

EUROPAM S.p.a.
SEDE LEGALE
Via Sardorella, 45T · 16162 Genova (Ge) - Italia
Capitale sociale 50.000.000,00 · Cod. Fisc./P.IVA 10848200969
Società soggetta ad attività di direzione e coordinamento di Black Oils S.p.A.
Tel. 010 72271 · Fax 010 7493407
euroenergypec@pec.it

che detengono le apposite procure, i compiti e le responsabilità assegnati all'*outsourcer*, inserendo altresì le clausole necessarie per portare la società terza a conoscenza del Modello 231 di Europam e dei suoi principi; tali prescrizioni si applicano inoltre a soggetti terzi che, in maniera stabile, collaborano con Europam nell'esecuzione di attività operative concernenti i sistemi informativi (es. attività di change management e di implementazione di migliorie funzionali evolutive);

- riguardo agli adempimenti operativi declinati all'interno dei contratti di *outsourcing*, è compito di Europam monitorare sul corretto svolgimento delle attività assegnate al fornitore, nel rispetto degli standard contrattuali definiti e pena l'applicazione delle penali previste;
- la scelta dei fornitori di servizi avviene nel rispetto della procedura Acquisti di beni e servizi generali e dei principi di controllo espressi all'interno della parte speciale n.3 "Acquisto di beni, servizi e incarichi professionali";
- in particolare, con riferimento alla gestione del sito della società, le richieste sono inoltrate dai referenti dei reparti interessati all'*outsourcer* esterno; tutte le implementazioni sono approvate dal referente di reparto prima di essere pubblicate online.

I Destinatari sono tenuti al rispetto dei principi di controllo previsti dal Modello anche laddove si trovino ad operare all'estero (ad es. in concorso con i referenti delle consociate estere); la responsabilità prevista dal Decreto si configura, infatti, anche in relazione ai reati commessi all'estero.

5.Funzioni coinvolte

Le funzioni aziendali e i soggetti coinvolti nella gestione dei sistemi informativi aziendali e del sito internet, nell'ambito delle attività sensibili identificate all'interno della presente Parte Speciale, sono:

- Amministratori della Società;
- Responsabile IT;
- Responsabile Risorse Umane;
- Ufficio Legale e Societario.

6.Flussi nei confronti dell'OdV

L'Organismo di Vigilanza richiede alle singole funzioni aziendali di inviare, su base periodica, i seguenti flussi informativi (che potranno essere integrati e/o modificati dallo stesso Organismo di Vigilanza, anche in considerazione degli esiti delle verifiche di competenza), al fine di effettuare un'attività sistematica e formalizzata di monitoraggio delle anomalie, delle eccezioni e delle deroghe registrate nel periodo di riferimento rispetto all'attuazione della presente Parte Speciale.

Parte speciale di riferimento	Flusso	Funzione responsabile dell'invio	Invio
Parte speciale 8: **Gestione dei sistemi informativi interni e del sito internet della società**	Elenco riepilogativo di tutti i casi in cui si riscontrano anomalie dei sistemi informatici (dalle quali possano evincersi accessi o tentativi di accessi abusivi, danneggiamenti, violazione delle procedure interne IT, cancellazione dei dati, ecc.)	IT	Annuale

EUROPAM S.p.a.
SEDE LEGALE
Via Sardorella, 45T · 16162 Genova (Ge) - Italia
Capitale sociale 50.000.000,00 · Cod. Fisc./P.IVA 10848200969
Società soggetta ad attività di direzione e coordinamento di Black Oils S.p.A.
Tel. 010 72271 · Fax 010 7493407
euroenergypec@pec.it

	Elenco delle licenze *software* in uso e delle relative date di scadenza.	IT	Annuale
	Informativa circa la correttezza delle utenze e della relativa profilazione in termini di accessi ai sistemi informativi	IT	Annuale

EUROPAM S.p.a.

SEDE LEGALE
Via Sardorella, 45T · 16162 Genova (Ge) - Italia
Capitale sociale 50.000.000,00 · Cod. Fisc./P.IVA 10848200969
Società soggetta ad attività di direzione e coordinamento di Black Oils S.p.A.
Tel. 010 72271 · Fax 010 7493407
euroenergypec@pec.it