ASSIST S.p.A.

RISK ASSESSMENT
INFORMATION TECHNOLOGY

Premessa

Il presente *risk assessment and gap analysis* viene redatto nell'ambito del progetto di revisione del Modello di organizzazione, gestione e controllo ex d.lgs. 231/2001 (d'ora in poi anche soltanto "MOG") di ASSIST S.p.A. (o "la Società"). Oltre all'analisi di tutta la documentazione fornita, sono state svolte specifiche "interviste" al fine di ricostruire il perimetro di attuale attività della Società e di individuare i possibili profili di rischio rilevante ai sensi del d.lgs. 231/2001 (d'ora in poi anche soltanto "il Decreto"), i presidi di controllo già esistenti ovvero gli eventuali *gap* organizzativi.

L'Attività di ASSIST S.p.A.

Assist S.p.A. nasce nel 2006 allo scopo di fornire servizi informatici per la Riscossione Coattiva dei crediti comunali attraverso l'utilizzo del sistema denominato ASSIST.WEB. In particolare l'attività di Assist riguarda i seguenti ambiti : "*riscuotere crediti di qualsiasi natura per conto di soggetti terzi sia in via giudiziale (avvalendosi di legali appositamente nominati) che stragiudiziale; riscuotere quote associative, tributi, contributi, locazioni, canoni, sanzioni ed i relativi interessi; effettuare solleciti e gestire il contenzioso e gli incassi fin dal loro originarsi, sviluppando, se richiesta, l'analisi della partite creditorie della clientela e prospettando la pianificazione delle migliori soluzioni in merito all'ottimizzazione della gestione dei crediti aziendali; rilasciare dichiarazioni attestanti l'inesigibilità dei crediti che, esperiti tutti i tentativi previsti nel relativo mandato, non si sono potuti riscuotere; rilasciare informazioni di natura commerciale relative ad enti, società o privati, mediante recepimento di notizie contenute in banche dati di pubblico dominio o cui la stessa ha comunque accesso in forza dell'attività sviluppata, raccogliendo altresì notizie mediante i propri operatori; realizzare applicazioni software ed erogare servizi informatici per la pubblica amministrazione locale e centrale nonché per le imprese private nei settori della riscossione ordinaria e coattiva e nei servizi alla persona, al patrimonio ed al territorio; pubblicare servizi in ambito pubblico e privato su internet, intranet, ASP (Application Service Provider) nei settori della riscossione ordinaria e coattiva e nei servizi alla pubblica amministrazione ed all'industria; realizzare prodotti e servizi per la gestione e la movimentazione di banche dati e di enti pubblici e privati; " gestire le attività di liquidazione e di accertamento dei tributi e quelle di riscossione dei tributi e di altre entrate e delle attività connesse o complementari indirizzate al supporto delle attività di gestione tributaria e patrimoniale, con esclusione di qualsiasi attività di commercializzazione della pubblicità, di società i cui soci non esercitino direttamente o indirettamente influenza dominante, ai sensi dell'articolo 2359 del codice civile, nei confronti di altri soggetti iscritti nell'albo o che effettuino attività di commercializzazione della pubblicità, ne' abbiano soci che siano imprenditori individuali che svolgono tale attività o siano controllate da società i cui soci siano imprenditori individuali che svolgono tale attività; fornire servizi per la consultazione di banche dati generiche o specifiche finalizzate alla riscossione ordinaria e coattiva*".

Inquadramento attività svolte dalla Funzione IT in ASSIST S.p.A .

La Funzione IT svolge tutte le attività tipiche rientranti nella gestione delle risorse informatiche: gestione degli accessi ai dati e ai sistemi; utilizzo di software e/o di banche dati per lo svolgimento di attività lavorative; gestione del processo di backup; gestione della sicurezza della Rete.

Profili di rischio *ex* d.lgs. 231/2001 connessi alle attività svolte dalla funzione '*Information Technology*"

Le fattispecie di reato di cui al d.lgs. 231/2001 che, a livello assolutamente generale ed astratto, potrebbero essere realizzate nel corso delle attività sopra descritta e pertanto rilevanti nell'attività di mappatura sono le seguenti: **Falsità in un documento informatico pubblico avente efficacia probatoria (artt. 491-bis cod. pen.); Accesso abusivo ad un sistema informatico o telematico (art. 615-ter cod. pen.)/Detenzione o diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater cod. pen.)/Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies cod. pen.)/Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche e telematiche (art. 617 – quater cod. pen.)/ Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis cod. pen.)/ Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter cod. pen.); Danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.); Danneggiamento di sistemi informatici o telematici di pubblica utilità di pubblica utilità (art. 635 quinquies c.p.); nonché, con riferimento alle fattispecie previste all'art. 25-novies del D. Lgs. 231/01, quella di Abusiva duplicazione o riproduzione di programmi per elaboratori e banche dati (art. 171-bis Legge n. 633/1941).**

Le suindicate ipotesi criminose potranno essere integrate, a titolo di esempio, nel caso in cui il sistema informativo aziendale sia utilizzato per l'accesso ad un sistema informativo o telematico, protetto, di terzi (provati o Pubblica Amministrazione) per l'acquisizione di dati riservati nell'interesse o a vantaggio della Società. Così è idonea a configurare un reato la comunicazione di codici di accesso a sistemi informatici della Società - protetti da misure di sicurezza – al fine di procurarsi un vantaggio economico derivante dal risparmio dell'acquisto delle licenze. Particolare rilevanza assume l'utilizzo di programmi informatici (es. virus) per la distruzione di dati di soggetti concorrenti o (es. spyware) per l'intercettazione di comunicazioni di soggetti terzi, nell'interesse o a vantaggio della Società nonché l'utilizzo di dispositivi per il danneggiamento di sistemi informatici di pubblica utilità o di terzi.

***

Attività	Soggetti	Profilo di rischio-reato							Potenziale profilo di rischio (modalità / occasione)	Presidi di controllo esistenti	Gap Analysis (Raccomandazioni / Piano d'azione)
		Reati vs P.A.	Reati Societari	Delitti Informatici	Criminalità organizzata	Industria e Commercio	Ricettaz. e riciclaggio	Altri reati			
Gestione delle risorse informatiche: gestione degli accessi ai dati e ai sistemi; utilizzo di software e/o di banche dati per lo svolgimento di attività lavorative; gestione del processo di backup; gestione della sicurezza della Rete.	**Amministratore Delegato (Marco Giletta)**	Sì	Sì	Sì	No	sì	No	No	<u>Falsità in un documento informatico pubblico avente efficacia probatoria.</u> La modalità di commissione di tale fattispecie potrebbe consistere nella cancellazione o alterazione di informazioni a valenza probatoria presenti sui propri sistemi, allo scopo di eliminare le prove di un altro reato. <u>Accesso abusivo ad un sistema informatico o telematico.</u> La modalità di commissione di tale fattispecie potrebbero essere le seguenti: - l'utilizzo del sistema informatico aziendale e/o per-	<u>Sistema di gestione della sicurezza delle informazioni.</u> Si segnala che la Società, che nel mese di dicembre ha ottenuto certificazione 27001: svolge azioni di monitoraggio anche della sicurezza informatica. La Società: è in possesso di software che consente analisi dei *log*; utilizza un *firewall* che produce report giornaliero; dispone di sistema che prevede tracciabilità di intervento sui files. Tale software traccia tutti i tentativi di accesso e le risultanze non sono soggette a possibili modifiche. E' in uso presso la Società il software	Stante la presenza della maggioranza di server fisici per il *backup* dei dati presso la sola sede di Beinasco, si raccomanda di adottare (nell'ambito del *disaster recovery*) misure logico-organizzative che consistano il posizionamento di server presso una sede diversa e più lontana (es. sede di Novara). Si raccomanda l'inserimento di procedura che preveda la distruzione fisica dei dischi a fronte della dismissione di macchine obsolete. Si suggerisce

Attività	Soggetti	Profilo di rischio-reato							Potenziale profilo di rischio (modalità / occasione)	Presidi di controllo esistenti	Gap Analysis (Raccomandazioni / Piano d'azione)
		Reati vs P.A.	Reati Societari	Delitti Informatici	Criminalità organizzata	Industria e Commercio	Ricettaz. e riciclaggio	Altri reati			
									sonale per l'accesso ad un sistema informatico o telematico di terzi (ad es. per entrare in possesso di dati riservati che riguardano concorrenti), nell'interesse o a vantaggio della Società; - l'accesso o permanenza di un tecnico/ amministratore del sistema nel sistema informatico aziendale e/o di Clienti al di fuori dell'ambito lavorativo o di uno specifico incarico o superando i limiti di permanenza nel sistema; - utilizzo del sistema informatico aziendale e/o per-	Microsoft *Data Protection Manager* che procede a backup dei dati sensibili e dei dati su *server*, mediante l'utilizzo di hardware dedicato. La Società ha attualmente in essere misure di protezione dell'accesso alle aree dove hanno sede informazioni e strumenti di gestione delle stesse: la Sala Server, videosorvegliata, è chiusa con chiave nella disponibilità esclusiva di responsabile IT e di Amministratore. In ordine alle misure volte alla riduzione dei rischi correlati ad occasioni di accesso non autorizzato, la Società ha in uso politica di accessi (in	l'implementazione di momenti di formazione IT nonché relativi alle procedure/policy in uso. Nell'ambito della revisione delle politiche di accesso, si raccomanda la suddivisione in reparti e gruppi al fine di limitare il più possibile, compatibilmente con le esigenze operative della Società, l'accesso in capo al singolo di dati e/o informazioni non necessarie per le sue mansioni. Si suggerisce la formalizzazione dei controlli effettuati dalla Funzione IT sulla rete

Attività	Soggetti	Profilo di rischio-reato							Potenziale profilo di rischio (modalità / occasione)	Presidi di controllo esistenti	Gap Analysis (Raccomandazioni / Piano d'azione)
		Reati vs P.A.	Reati Societari	Delitti Informatici	Criminalità organizzata	Industria e Commercio	Ricettaz. e riciclaggio	Altri reati			
									sonale per l'accesso o la permanenza contro la volontà di chi ha il diritto di escluderlo in un sistema informatico o telematico protetto aziendale, nell'interesse o a vantaggio della Società. <u>Detenzione o diffusione abusiva di codici di accesso a sistemi informatici o telematici</u>. La modalità di commissione di tale fattispecie potrebbe consistere nella comunicazione di codici di accesso a sistemi informatici protetti da misure di sicurezza (es. software e/o	fase di revisione). In ordine all'accesso controllato ai propri sistemi informativi, al momento esistono n. 3 server che gestiscono utenti (ciascuno in possesso di autonoma pwd). E' in uso un unico gruppo di utenti che comprende tutti i dipendenti. Esistono gruppi più ristretti anche se le procedure massive risultano prevalenti. Esiste (in fase di sperimentazione) misura di sicurezza sul pc in uso al commerciale (fuori sede): inaccessibilità del disco per dati contenuti in una determinata sezione. In ordine ai controlli sulla rete aziendale, la Funzione IT effettua controlli che non	aziendale e sulle informazioni che vi transitano. Con riferimento all'attività svolta (in virtuale, via VPN) in Albania (società fornitore terzo), si suggerisce la creazione di stabile organizzazione con controllo totale da parte della Società. Con riferimento ai rapporti con terze parti, si raccomanda l'implementazione di adeguati requisiti di sicurezza (es. stampatore).

Attività	Soggetti	Profilo di rischio-reato							Potenziale profilo di rischio (modalità / occasione)	Presidi di controllo esistenti	Gap Analysis (Raccomandazioni / Piano d'azione)
		Reati vs P.A.	Reati Societari	Delitti Informatici	Criminalità organizzata	Industria e Commercio	Ricettaz. e riciclaggio	Altri reati			
									banche dati) in uso alla Società e/o a terzi al fine di procurarsi un vantaggio economico derivante dal risparmio dell'acquisto delle licenze. <u>Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.</u> Le modalità di commissione di tale fattispecie potrebbero essere le seguenti: - utilizzo di programmi informatici (es. virus) per la distruzione di dati / informazio-	sono oggetto di formalizzazione.	

Attività	Soggetti	Profilo di rischio-reato							Potenziale profilo di rischio (modalità / occasione)	Presidi di controllo esistenti	Gap Analysis (Raccomandazioni / Piano d'azione)
		Reati vs P.A.	Reati Societari	Delitti Informatici	Criminalità organizzata	Industria e Commercio	Ricettaz. e riciclaggio	Altri reati			
									ni di concorrenti, anche mediante l'uso del telefono cellulare aziendale; - Utilizzo di programmi informatici (es. virus) per la distruzione di dati / informazioni della Società (ad es. per sottrarli al controllo di un Ente Pubblico), anche mediante l'uso del telefono cellulare aziendale. <u>Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche.</u> La modalità di commissione di tale fatti-		

Attività	Soggetti	Profilo di rischio-reato							Potenziale profilo di rischio (modalità / occasione)	Presidi di controllo esistenti	Gap Analysis (Raccomandazioni / Piano d'azione)
		Reati vs P.A.	Reati Societari	Delitti Informatici	Criminalità organizzata	Industria e Commercio	Ricettaz. e riciclaggio	Altri reati			
									specie potrebbe consistere nella diffusione di programmi informatici (es. *spyware*) o installazione di apparecchiature per l'intercettazione di comunicazioni ad es. di un concorrente o di un Ente Pubblico. <u>Danneggiamento di informazioni, dati e programmi informatici.</u> La modalità di commissione di tale fattispecie potrebbe consistere nell'utilizzo del sistema informatico aziendale per il danneggiamento di informazioni, dati o programmi di Terzi (es. *outsourcer*), nell'interesse o a		

Attività	Soggetti	Profilo di rischio-reato							Potenziale profilo di rischio (modalità / occasione)	Presidi di controllo esistenti	Gap Analysis (Raccomandazioni / Piano d'azione)
		Reati vs P.A.	Reati Societari	Delitti Informatici	Criminalità organizzata	Industria e Commercio	Ricettaz. e riciclaggio	Altri reati			
									vantaggio della Società. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo stato o da altro ente pubblico o comunque di pubblica utilità. La modalità di commissione di tale fattispecie potrebbe consistere nell'utilizzo del sistema informatico aziendale per l'alterazione / danneggiamento di registri informatici / sistemi informatici della Pubblica Amministrazione o comunque di pubblica utilità (es. per modificare dati relativi alla Società, quali le		

Attività	Soggetti	Profilo di rischio-reato							Potenziale profilo di rischio (modalità / occasione)	Presidi di controllo esistenti	Gap Analysis (Raccomandazioni / Piano d'azione)
		Reati vs P.A.	Reati Societari	Delitti Informatici	Criminalità organizzata	Industria e Commercio	Ricettaz. e riciclaggio	Altri reati			
									dichiarazioni fiscali, o di concorrenti o utilizzati dallo stato / da altro Ente Pubblico). <u>Danneggiamento di sistemi informatici o telematici.</u> La modalità di commissione di tale fattispecie potrebbe consistere nell'utilizzo di dispositivi, anche mediante ricorso a società esterne, per il danneggiamento di sistemi informatici di Terzi. <u>Danneggiamento di sistemi informatici o telematici di pubblica utilità.</u> La modalità di com-		

Attività	Soggetti	Profilo di rischio-reato							Potenziale profilo di rischio (modalità / occasione)	Presidi di controllo esistenti	Gap Analysis (Raccomandazioni / Piano d'azione)
		Reati vs P.A.	Reati Societari	Delitti Informatici	Criminalità organizzata	Industria e Commercio	Ricettaz. e riciclaggio	Altri reati			
									missione di tale fattispecie potrebbe consistere nell'utilizzo di dispositivi, anche mediante ricorso a società esterne, per il danneggiamento di sistemi informatici di pubblica utilità.		