Modello di Organizzazione Gestione e Controllo ai sensi del D.lgs. 8 giugno 2001, n. 231

PARTE SPECIALE – SEZ. B
Delitti informatici e trattamento illecito di dati (art. 24 bis)

Documento approvato con delibera dell'Amministratore Unico di Aster S.r.l. del 12/04/2021

ELENCO DELLE REVISIONI			
Revisione	**Data**	**Natura delle modifiche**	**Approvazione**
00	12/04/2021	Stesura e prima edizione	Dott. Michele Chiodarelli

INDICE

1. Descrizione fattispecie di reato

La presente sezione si riferisce ai reati informatici - art. 24 bis del D.lgs. 231/2001.
Le fattispecie di reato previste dall'art. 24 bis sono:

- Falsità in un documento informatico pubblico o avente efficacia probatoria (Art. 491-bis c.p.)
- Accesso abusivo ad un sistema informatico o telematico (Art. 615-ter c.p.)
- Detenzione, diffusione abusiva di codici di accesso a sistemi informatici/telematici (Art. 615-quater c.p.)
- Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (Art. 615-quinquies cp)
- Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (Art. 617-quater c.p.)
- Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (Art. 617-quinquies cp)
- Danneggiamento di informazioni, dati e programmi informatici (Art. 635-bis c.p.)
- Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (Art. 635-ter c.p.)
- Danneggiamento di sistemi informatici o telematici (Art. 635-quater c.p.)
- Danneggiamento di sistemi informatici o telematici di pubblica utilità (Art. 635-quinquies c.p.)
- Frode informatica del certificatore di firma elettronica (Art. 640-quinquies)
- Perimetro di sicurezza cibernetico (Art. 1 co 11 bis D.L. 105/2019)

Per la descrizione dettagliata delle fattispecie di reato elencate vedi Mod.231_Parte generale edizione in vigore.

2. Processi e attività sensibili

I reati previsti **dall'art. 24 bis del D.lgs. 231/2001** possono verificarsi tramite comportamenti posti in essere dai seguenti Soggetti (di seguito Esponenti Aziendali) di Aster S.r.l.: amministratori, direzione, responsabili di area o funzione, operatori dei servizi dipendenti e in generale tutti i soggetti coinvolti nei processi di seguito identificati. In termini di configurabilità nel contesto di Aster S.r.l., va segnalato che l'organizzazione gestisce un sistema informativo di interesse pubblico e le proprie attività sono in buona parte gestite da procedure informatiche. In linea generale quindi i reati in questione attraversano l'intera organizzazione aziendale. Tuttavia l'attenzione è stata indirizzata ai casi in cui si possa configurare un interesse o un vantaggio per l'ente, riducendo in parte i potenziali casi applicativi.
È da considerarsi, inoltre, che nell'espletamento delle proprie funzioni, una parte del personale dispone di credenziali per l'accesso a banche dati esterne di proprietà di soggetti pubblici (ad es. Sintel, MePA, …).

N.B.: Il reato di "Frode informatica del soggetto che presta servizi di certificazione di firma elettronica" (art. 640-quinquies c.p.), non sembra configurabile all'interno del contesto aziendale, mancando la qualifica soggettiva presupposto del reato, in quanto l'Ente non svolge il servizio di certificazione di firma elettronica.
Le attività a rischio, considerate tali in base all'analisi effettuata su tutti i processi dell'azienda, sono:

Processo/fasi	Attività sensibili
GESTIONE PROCESSO CONTABILE AMMINISTRATIVO - PROCESSO DI GESTIONE DEI FLUSSI FINANZIARI E TESORERIA:	Operazioni di accesso a sistemi informatici e/o telematici senza autorizzazioni al fine di alterare dati e informazioni; utilizzo improprio di codici ID e PW non attribuiti formalmente, danneggiamento di informazioni e programmi atti a distruggere dati e informazioni (es. contabili, anche utilizzati da PA). (*Reati: accesso abusivo ad un sistema informatico o telematico; detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici. Danneggiamento di informazioni, dati e programmi informatici; danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità; danneggiamento di sistemi informatici o telematici; danneggiamento di sistemi informatici o telematici di pubblica utilità).* Nelle attività di: Adempimenti contabili, fiscali, tributari: invio dati tramite accesso a portali che richiedono identificativo e PW.

	Gestione pagamenti e gestione rapporti con istituti di credito: accesso e utilizzo homebanking. Rendicontazione progetti verso la PA Gestione pratiche amministrative verso EE.PP. funzionali all'avvio o gestione ordinaria dei servizi. Ricorso a finanza agevolata *(contributi da EE.PP., bandi regionali, ministeriali, finanziamenti pubblici)*
Servizi: GESTIONE SERVIZI ABITATIVI: Programmazione Generale - Erogazione Dei Servizi Abitativi- Gestione Amministrativa Servizi Abitativi	Ricezione incarico da Comune di Mantova di programmazione offerta servizi abitativi (quantificazione alloggi assegnabili) Supporto al caricamento dati nel sistema di gestione regionale Compilazione anagrafe utenza, calcolo canone, predisposizione contratto con inquilino, registrazione contratto con pagamento oneri per conto del Comune
Gestione Condominio in Proprietà Mista	Ricezione prospetto spese condominiali e verifica congruità, pagamento rate alle scadenze prestabilite (quota Comune), verifica eventuale morosità inquilini segnalata da amministratore di condominio
Progettazione Interventi Straordinari (nella gestione dei S.A.)	Fase istruttoria, e. presentazione istanza a enti preposti per realizzazione opere, ricezione atto autorizzativo, incarico realizzazione lavori a ditta esterna, esecuzione lavori, collaudo e relazione finale per consegna lavori *(Aster come appaltatore lavori tramite gara su portale MePA)*
Servizi: GESTIONE WELFARE ABITATIVO E SAT (Alloggi temporanei di emergenza)	Ricezione da Servizi sociali segnalazione di assegnazione ad utente di appartamento temporaneo Contatto con utente per sopralluogo appartamento, invio esito sopralluogo a servizi sociali, predisposizione contratto e convocazione utente per la firma unitamente al regolamento, invio contratto alla firma del dirigente comunale e registrazione. (*Falsità in documenti informatici, accesso abusivo a sistema informatico/telematico, detenzione e diffusione abusiva di codici di accesso, diffusione, danneggiamento di info, dati, programmi utilizzati da ente pubblico, di sistemi informatici o telematici, abusiva duplicazione di programmi per PC*) questi reati si possono configurare ad esempio in fase di caricamento dati e documenti contrattuali.
Servizi: GESTIONE SERVIZI PASS E ABBONAMENTI – (emissione del titolo, rinnovi, controlli, informazione a utente su sanzioni ricevute)	Acquisizione contratto di servizio dal Comune di MN e successiva pianificazione del servizio Richiesta pass da utente/individuazione tipologia pass da parte di ASTER, Verifica doc compilata e doc allegata a corredo (es. contratto di proprietà affitto stallo in ZTL), rilascio pass o ev. modifica pass esistente, rinnovo Controllo periodico pass: ricezione mensile elenco agg.to da polizia locale, verifica requisiti, invio raccomandata a utente o eredi per la riconsegna del pass entro 30 gg, ev. blocco del pass anno successivo in caso di mancata consegna e comunicazione a polizia locale per scollegare le targhe abbinate. Verifica sanzione emessa, ev. azioni correttive all'errore (lettera Aster, post sanatoria) o pagamento sanzione da parte dell'utente *(questi reati si possono configurare in fase di accesso alle piattaforme operative per il caricamento dei dati afferenti alla gestione del servizio PASS/AB).*
Servizi: GESTIONE SERVIZIO EROGAZIONE E CONTROLLO TITOLI DI SOSTA A PAGAMENTO IN SUPERFICIE E GARAGE (S. Giorgio, Parcheggio Mondadori)	Gestione aree di sosta in superficie e strumenti di erogazione titoli (parcometri, altri strumenti elettronici), controllo titoli di sosta e gestione verbali preavvisi di accertamento, rendicontazione incassi a contabilità d'ufficio con consegna scontrino di macchina.
Servizi: GESTIONE SERVIZI ICT per conto del Comune di Mantova (contratto di servizio): servizi PMT (Project Management Tecnico), servizi controllo Qualità delle attività di ICT.	Acquisizione contratti di servizio per l'avvio dell'erogazione dei servizi ICT Gestione dei seguenti servizi divisi per macro aree: 1. Area di governo e coordinamento, 2. Area di innovazione, 3. Area di esercizio, 4. Implementazione e gestione portale WEB comunale. ***N.B:*** *ai fini dei Delitti informatici e trattamento illecito dei dati si considera anche la gestione ICT interna all'azienda ASTER e non solo il servizio di erogazione a cliente.* Nello specifico, a titolo di esempio:

Gestione ordinaria del Sistema Informativo Comunale: servizi di gestione dell'Area di Esercizio (operativa, sistemistica, continuità operativa, sicurezza logistica e fisica) Gestione dei Sistemi informativi e della Privacy propri dell'Ente (sede principale e sede distaccata di Mantova-via S. Giorgio)	Sicurezza e protezione dati Gestione PW di accesso alle postazioni Utilizzo internet e posta elettronica Gestione accessi a sistemi telematici della PA Gestione licenze e copyright programmi (reato in caso di utilizzo di software senza licenza d'uso)

3. Principi di comportamento

I principi di comportamento e le disposizioni della Parte Speciale si applicano a tutti gli amministratori, dirigenti, responsabili di funzione, di processo – anche delegati o incaricati, dipendenti, collaboratori/consulenti esterni, fornitori/partner di Aster S.r.l. che intervengono e sono coinvolti nei processi aziendali sopra identificati.

Scopo della Sezione:

- Indicare procedure, protocolli o regole di condotta, conformi a quanto prescritto dalla parte speciale stessa, da osservare per la corretta applicazione del Modello e al fine di prevenire ed impedire il verificarsi di delitti informatici o il trattamento illecito di dati in possesso dell'ente a causa delle attività svolte – con particolare attenzione nella gestione dei dati relativi alla privacy;
- Fornire ai soggetti indicati l'elenco dei flussi informativi da trasmettere all'OdV incaricato di svolgere le attività di verifica e controllo.

Ai **soggetti** sopra indicati (agli **esterni** attraverso apposite clausole) è fatto **obbligo** di:

- osservare regole e principi del Codice Etico adottato da Aster;
- osservare tutte le leggi, regolamenti e procedure che disciplinano l'attività aziendale, con particolare riferimento alle attività che comportano la gestione dei sistemi informatici e telematici interni ed esterni;
- osservare scrupolosamente tutte le norme volte al mantenimento dell'integrità dei sistemi informatici e agire sempre rispettando le procedure interne;
- Osservare la disciplina in materia di privacy e trattamento dei dati (Reg. UE 679/2016 e s.m.i.).

Ai medesimi soggetti **è fatto esplicito divieto** di:

- manomettere e/o danneggiare i sistemi informatici attuando comportamenti non corretti dal punto di vista normativo;
- falsificare documenti informatici pubblici o aventi efficacia probatoria;
- accedere abusivamente a sistemi informatici o telematici;
- detenere o diffondere abusivamente codici d'accesso a sistemi informatici protetti;
- diffondere apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere i sistemi informatici;
- interrompere o impedire illecitamente comunicazioni informatiche interne;
- danneggiare dati, informazioni o programmi informatici (sono inclusi anche quei dati necessari nei rapporti Società – Stato, con altri enti pubblici)
- utilizzare in modo illegale password di PC, codici di accesso o informazioni per compiere una delle condotte di cui sopra;
- accedere illegalmente e duplicare banche dati;
- installare programmi non originali, eseguire il download di software dalla rete, senza autorizzazione;
- utilizzare il proprio account aziendale per comunicazioni private e viceversa;

Ai fini dell'attuazione dei comportamenti di cui sopra, Aster si **impegna** a:

- fornire una adeguata informazione e formazione sul corretto utilizzo dei sistemi informativi;
- predisporre procedure in tema di sicurezza informatica (data-breach, hackeraggio, ecc.);

- regolare l'utilizzo e l'accesso a sistemi informatici, tramite gli strumenti in dotazione (PC, cellulari, tablet, ecc..), solo per finalità connesse all'operatività aziendale, riducendo al minimo i rischi;
- proteggere il perimetro aziendale, il controllo degli accessi e le infrastrutture critiche dislocate;
- effettuare, nel rispetto della normativa vigente, controlli periodici sulla rete informatica aziendale;
- predisporre e mantenere strumenti adeguati (hardware e software) a protezione di server e sistemi informativi;
- gestire e monitorare un inventario delle licenze in uso e valutare la necessità di rinnovare o meno i contratti di licenza in base alle esigenze aziendali.

4. Protocolli specifici

Oltre al Codice Etico e ai principi generali sopra indicati, Aster sta adottando protocolli specifici per la mitigazione dei rischi commissione reato individuati. I protocolli possono essere formalizzati integrando procedure già esistenti nel SGQA e nel Sistema Privacy di Aster, adottandone di nuove, o in regolamenti di condotta, policy (es. Policy Privacy), ecc.

Tali protocolli hanno inoltre lo scopo di fornire un maggior grado di dettaglio operativo alle funzioni aziendali che lavorano nei processi e attività a rischio di commissione reati ex D.lgs. 231/01.

I presìdi fisici ad oggi utilizzati dall'ente e in costante miglioramento, consistono in una serie di misure tecniche sul sistema informativo per garantire la sicurezza e la protezione dei dati, prevenire possibili attacchi esterni e garantire un corretto utilizzo da parte del personale.

Vanno infine considerati ad integrazione del MOGC i presìdi previsti dalle misure di sicurezza in materia di protezione dei dati personali previsti dal Piano di Miglioramento a seguito delle analisi svolte e delle azioni individuate (ed eventuali procedure allegate o richiamate dallo stesso).

Tra le misure tecniche adottate da Aster si citano le seguenti:

- Sistemi di autenticazione informatica per l'accesso ai sistemi informatici (accesso al personal computer, accesso ai programmi, accesso alle banche dati esterne). Sistemi di autorizzazione attraverso la profilazione dei singoli utenti (o gruppi di utenti) nell'utilizzo delle risorse informatiche (es. programmi gestionali e contabili), con l'obiettivo di limitare l'accesso ai soli dati di propria competenza, in base alle regole organizzative dell'ente. *Es: il Responsabile dei sistemi informatici predispone e cura l'aggiornamento di una matrice che evidenzia i profili di accesso ai sistemi, in base alle autorizzazioni fornite dai rispettivi responsabili.*
- Altre misure tecniche previste dal Piano di Miglioramento ed attività di audit previste a carico dell'amministratore di sistema.

È evidente che la rapida evoluzione della tecnologia impone frequenti aggiornamenti ed adeguamenti dei protocolli vigenti, per accrescerne la loro efficacia. (Es: a *tale scopo ogni anno, nell'ambito della procedura di stesura del bilancio previsionale, vengono valutati ed esposti i fabbisogni di spesa per aggiornamenti tecnici o formativi).*

QUESTA È L'ULTIMA PAGINA DEL DOCUMENTO