MODELLO DI ORGANIZZAZIONE GESTIONE E CONTROLLO

DI

SANITASERVICE ASL BR s.r.l.
Società Unipersonale della ASL di Brindisi

Società soggetta a direzione e coordinamento da partedell'ASL BR ai sensi dell'art. 2497 e ss. Codice Civile

PARTE SPECIALE C

DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

(aggiornato al decreto legislativo n. 7 del 15 gennaio 2016, modificato dalla Legge n. 238/2021 e dalla legge 90/2024)

1 DELITTI INFORMATICI E TRATTAMENTO ILLECITO DI DATI

La legge 18 marzo 2008, n. 48 recante "*ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno*" ha introdotto nel d.lgs. 231/2001 l'art. 24-*bis* che estende l'ambito di applicazione del decreto ai delitti informatici e trattamento illecito di dati (di seguito, "**Delitti Informatici**"). Le disposizioni sono state integrate dal d. lgs. n. 7 del 15 gennaio 2016. L'azienda è ottemperante a tutto quanto previsto dal Regolamento generale per la protezione dei dati personali 2016/679.

Di recente con la **legge 28 giugno 2024, n. 90** recante «*Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici*» sono state introdotti un inasprimento delle sanzioni previste dal D.lgs. 231/2001, apportando all'articolo 24-bis D.lgs. 231/2001 (Delitti informatici e trattamento illecito di dati) le seguenti modifiche:

- al comma 1, le parole: «da cento a cinquecento quote» sono sostituite dalle seguenti: «da duecento a settecento quote»;

- al comma 2, la parola: «615 -quinquies» è sostituita dalla seguente: «635 -quater .1» e le parole: «sino a trecento quote» sono sostituite dalle seguenti: «sino a quattrocento quote».

La legge 90/2024 introduce anche un ipotesi aggravata dell'art. 629 c.p. (estorsione) di un'ipotesi aggravata di estorsione realizzata mediante lecondotte di cui agli articoli 615-ter, 617-quater, 617-sexies, 635-bis, 635-quater e 635-quinquies c.p.(reati informatici) ovvero con la minaccia di compierle.

Tale fattispecie è altresì inserita nel Catalogo dei Reati Presupposto della Responsabilità amministrativa degliEnti ex D.lgs. 231/2001 all'art. 24 bis (Delitti informatici e trattamento illecito di dati).

La commissione di tale reato presupposto comporta:

- l'applicazione all'ente della sanzione pecuniaria da trecento a ottocento quote;

- l'applicazione all'Ente delle sanzioni interdittive previste dall'articolo 9, comma 2, per una durata non inferiore a due anni.

1.1 I reati di cui all'art. 24-*bis* del Decreto

Si riporta di seguito una sintetica descrizione dei Delitti Informatici.

Ai sensi dell'art. 26 del Decreto, la Società potrebbe essere considerata responsabile anche qualora le fattispecie fossero integrate nella forma del tentativo.

1.1.1 Falsità riguardanti documenti informatici (art. 491-*bis* c.p.)

La norma, attraverso un rinvio alle disposizioni sulle falsità concernenti atti pubblici e scritture private, previste dal codice penale, ne dispone l'applicazione anche alle ipotesi in cui le rispettive previsioni riguardino un "documento informatico"[1].

[1] Si precisa che il Legislatore parla di "documento informatico" nelle due disposizioni di seguito citate che risultano particolarmente significative ai fini della ricostruzione della nozione del termine:

1. art. 491-*bis* c.p., in commento: "*se alcuna delle falsità previste dal presente capo 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*";

In particolare, le norme del codice penale cui l'articolo in commento fa rinvio sono quelle contenute nel Capo III, Titolo VII, Libro II. Tra queste si segnalano:

- art. 476 c.p. ("falsità materiale commessa dal pubblico ufficiale in atti pubblici");
- art. 477 c.p. ("falsità materiale commessa dal pubblico ufficiale in certificati o autorizzazioni amministrative");
- art. 478 c.p. ("falsità materiale commessa dal pubblico ufficiale in copie autentiche di atti pubblici o privati e in attestati del contenuto di atti");
- art. 479 c.p. ("falsità ideologica commessa dal pubblico ufficiale in atti pubblici");
- art. 480 c.p. ("falsità ideologica commessa dal pubblico ufficiale in certificati o in autorizzazioni amministrative");
- art. 482 c.p. ("falsità materiale commessa dal privato");
- art. 483 c.p. ("falsità ideologica commessa dal privato in atto pubblico");
- art. 484 c.p. ("falsità in registri e notificazioni");
- art. 487 c.p. ("falsità in foglio firmato in bianco. Atto pubblico");
- art. 488 c.p. ("altre falsità in foglio firmato in bianco. Applicabilità delle disposizioni sulle falsità materiali");
- art. 489 c.p. ("uso di atto falso");
- art. 490 c.p. ("soppressione, distruzione e occultamento di atti veri").

1.1.2 Accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.)

2. art. 1, comma 1, lett. p) d.lgs. 82/2005 (c.d. Codice dell'amministrazione digitale): "*Ai fini del presente codice si intende per: (…) p) documento informatico: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*".

Prima che la legge 48/2008 abrogasse il secondo periodo del primo comma dell'art. 491-*bis* c.p., in esso era possibile leggere che "*a tale fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli*". Attualmente quindi, ai fini dell'applicazione del D.lgs. 231/2001 è documento informatico "*la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti aventi efficacia probatoria*". L'elemento dell'"*efficacia probatoria*" richiesto dall'art. 491-*bis* c.p. è riscontrabile sicuramente nel documento informatico munito di firma elettronica qualificata e di firma digitale (nell'ipotesi di tali "firme forti", l'efficacia probatoria sarà quella *ex* art. 2702 c.c.), ai sensi dell'art. 21, comma 2, D.lgs. 82/2005. Per quanto concerne invece il documento elettronico cui è apposta una firma elettronica semplice (come ad esempio, *password*, codice *pin*) l'efficacia probatoria è liberamente valutabile dal Giudice in giudizio (art. 21, comma 1, D.lgs. 82/2005). Nell'ipotesi invece di documento informatico non sottoscritto, la valenza probatoria sarà quella dell'art. 2712 c.c., a seguito della modifica dello stesso da parte dell'art. 23, comma 1, D.lgs. 82/2005.

1.1.3 L'art. 615-*ter* punisce chiunque abusivamente si introduce in un sistema informatico[2] o telematico[3] protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

Il Legislatore prevede sanzioni più elevate 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;
- il colpevole per commettere il fatto minaccia o usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
- 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, ovvero la sottrazione, anche mediante riproduzione o trasmissione, o l'inaccessibilità al titolare.

È, inoltre, previsto un aggravamento della sanzione qualora i fatti sopra descritti 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 norma non si limita alla tutela della *privacy* informatica e telematica, ovvero alla riservatezza dei dati memorizzati nei sistemi informatici o trasmessi con sistemi telematici, ma offre un'ampia tutela che si concreta nello *ius excludendi alios*.

1.1.4 **Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-*quater* c.p.)**

---

[2] Si rileva che l'art. 1 della Convenzione di Budapest individua come sistema informatico "*qualsiasi apparecchiatura o rete di apparecchiature interconnesse o collegate, una o più delle quali, attraverso l'esecuzione di un programma per l'elaboratore, compiono elaborazione automatica di dati*". "*Rientrano, dunque nella definizione tutti i dispositivi hardware che gestiscono dei dati attraverso uno o più programmi (software): si tratterà degli strumenti elettronici, informatici o telematici, sia che essi lavorino in rete, sia che lavorino in assoluta autonomia (telefoni cellulari, palmari). Peraltro, sul punto era già intervenuta la Suprema Corte, affermando che per sistema informatico «deve intendersi un complesso di apparecchiature destinate a compiere una funzione utile all'uomo, attraverso l'utilizzazione di tecnologie informatiche, che sono caratterizzate dalla registrazione o memorizzazione per mezzo di impulsi elettrici, su supporti adeguati di dati, cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazioni diverse, nonché costituito dalla elaborazione automatica di tali dati, in modo da generare informazioni costituite da un insieme, più o meno vasto, dei dati stessi, organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente»*" (Giordanengo, *I reati informatici: le intrusioni illecite*, in atti del convegno *I reati informatici e la responsabilità amministrativa degli enti*, Milano, 15 e 16 ottobre 2008). Quanto al concetto di "dati informatici", lo stesso è individuato dall'art. 1, lett. b), della medesima Convenzione che lo definisce come "*qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione*". "*Rientrano, dunque in tale definizione tanto i programmi software, quanto i dati personali che mediante gli stessi vengono elaborati*" (Giordanengo, *op. cit.*).

[3] Per sistema telematico si intende, secondo un primo orientamento espresso in dottrina, ogni forma di telecomunicazione che si giovi dell'apporto informatico per la sua gestione, indipendentemente dal fatto che la comunicazione avvenga via cavo, via etere o con altri sistemi (cfr. Borruso, in AA.VV., *Profili penali dell'informatica*, Milano, 1994, 7 ss.). Altri riducono invece il significato del termine alle forme di comunicazione via cavo, ed essenzialmente alle comunicazioni via linea telefonica tra *computers* (cfr. Buonuomo, in AA.VV., *Profili penali dell'informatica*, Milano, 1994, 148 ss.).

L'art. 615-*quater* sanziona chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, o consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, 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.

Sanzioni più gravi sono previste se il fatto è commesso:

- in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
- 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, ovvero con abuso della qualità di operatore del sistema.

Il bene giuridico tutelato dalla norma in oggetto sarebbe da individuarsi nella riservatezza delle chiavi d'accesso, considerate dal Legislatore alla stregua di qualità personali riservate, in quanto identificatrici della persona. Con questa previsione il Legislatore ha voluto fornire una tutela anticipata dal momento che sanziona tutta una serie di condotte che sono preparatorie rispetto alla condotta descritta dal disposto di cui all'art. 615-*ter* (*Accesso abusivo ad un sistema informatico o telematico*).

La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma.

1.1.5 Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* c.p.)

L'art. 617-*quater* (così come il successivo art. 617-*quinquies*) è una norma volta a tutelare la sicurezza e la genuinità delle comunicazioni informatiche e telematiche.

La fattispecie punisce:

- chiunque fraudolentemente intercetta, impedisce o interrompe comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni informatiche o telematiche intercettate.

Sanzioni più elevate sono previste se il fatto è commesso:

- in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
- in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni o 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, ovvero con abuso della qualità di operatore del sistema;

- da chi esercita anche abusivamente la professione di investigatore privato.

1.1.6 Detenzione, diffusione e Installazione abusiva di apparecchiature e di altri mezzi atti ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* c.p.)

L'art. 617-*quinquies* punisce l'installazione, fuori dai casi consentiti dalla legge, di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

Sanzioni più elevate sono previste se il fatto è commesso:

- in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 2), la pena è della reclusione da due a sei anni.

Quando ricorre taluna delle circostanze di cui all'articolo 617-quater, quarto comma, numero 1), la pena è della reclusione da tre a otto anni»

La norma tutela in forma anticipata il bene giuridico della riservatezza delle informazioni o notizie trasmesse per via telematica o elaborate da singoli sistemi informatici. Il Legislatore ha ritenuto opportuno ricorrere allo schema del reato di pericolo per realizzare la più ampia tutela dell'interesse protetto.

1.1.7 Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* c.p.)

L'art. 640-*quinquies* punisce la condotta posta in essere dal 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.

1.1.8 Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* c.p.)

La fattispecie si realizza quando chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui.

Sanzioni più gravi sono previste se il fatto è commesso con violenza alla persona o minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

L'art. 5 della legge 48/2008 ha operato un complessivo riordino delle fattispecie di danneggiamento, riunendo sotto le norme dall'articolo 635-*bis* al 635-*quinquies* c.p., le varie figure di danneggiamento informatico e abrogando i commi 2 e 3 dell'art. 420 c.p. (*Attentato a impianti di pubblica*

utilità). In particolare, il Legislatore ha disposto lo scorporo tra le fattispecie di danneggiamento di sistemi informatici o telematici e quella di danneggiamento di informazioni, dati o programmi informatici.

Inoltre, è stata introdotta una distinzione tra i casi di danneggiamento di dati o sistemi con rilevanza meramente privatistica e i casi in cui sono poste in essere condotte volte a danneggiare dati o sistemi di pubblica utilità.

1.1.9 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.)

La fattispecie si realizza quando chiunque 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.

Sanzioni più elevate sono previste se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici.

È, inoltre, previsto un aumento della pena se il fatto è commesso con violenza alla persona o minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

1.1.10 Danneggiamento di sistemi informatici o telematici (art. 635-*quater* c.p.)

L'art. 635-*quater* punisce chiunque, mediante le condotte di cui al sopra citato articolo 635-*bis*, 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.

È previsto un aumento della pena se il fatto è commesso con violenza alla persona o minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

1.1.11 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)

Chiunque, 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, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici è punito con la reclusione fino a due anni e con la multa fino a euro 10.329.

La pena è della reclusione da due a sei anni quando ricorre taluna delle circostanze di cui all'articolo 615-ter, secondo comma, numero 1).

La pena è della reclusione da tre a otto anni quando il fatto riguarda i sistemi informatici o telematici di cui all'articolo 615-ter, terzo comma»;

1.1.12 Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-*quinquies* c.p.)

La norma prevede sanzioni nel caso in cui il fatto previsto dal precedente articolo 635-*quater* è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

Sanzioni più gravi sono previste se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile.

È, inoltre, previsto un aumento della pena se il fatto è commesso con violenza alla persona o minaccia ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.

1.2 Attività Sensibili. Principi di comportamento e protocolli di prevenzione

A seguito dello svolgimento delle attività di *risk mapping* e *risk assessment*, sono state individuate, nell'ambito della struttura organizzativa ed aziendale della Società, le specifiche Attività Sensibili che possono astrattamente comportare il rischio per la Società di commissione dei Delitti Informatici sopra elencati, nonché le relative funzioni aziendali coinvolte.

Successivamente, sono stati individuati i principi di comportamento e i principali protocolli di prevenzione che vengono attuati dalla Società al fine di prevenire la commissione di detti reati.

1.2.1 Attività Sensibili

L'Attività Sensibile principale è quella che concerne l'utilizzazione dell'infrastruttura tecnologica e dei sistemi informativi e telematici ed include le seguenti attività:

- definizione delle regole da adottare in materia di sicurezza del sistema informatico e telematico;
- gestione degli accessi al sistema informatico degli utenti interni ed esterni, dei profili utente e del processo di autenticazione;
- gestione degli aspetti concernenti la sicurezza informatica di documenti elettronici con valore probatorio, della protezione delle reti e delle comunicazioni;
- gestione della sicurezza fisica, ambientale (include sicurezza apparecchiature, cablaggi, dispositivi di rete, informazioni, ecc.) e delle attività di inventariazione dei beni;
- acquisizione e gestione di apparecchiature, di dispositivi (anche di rilevazione) connessi con il sistema o di programmi informatici (ivi inclusi lo sviluppo degli stessi e i servizi di installazione e manutenzione);

- monitoraggio/verifica periodica del sistema informatico e gestione degli incidenti e dei problemi di sicurezza informatica.

(Funzioni coinvolte: Organo Amministrativo (AU), ICT ed in alcune circostanze DPO).

Le Attività Sensibili sopra identificate potranno essere modificate e/o integrate a seguito degli aggiornamenti delle attività di *risk mapping* e *risk assessment* effettuate di volta in volta dall'OdV a seguito del verificarsi di situazioni quali, a titolo esemplificativo, cambiamenti organizzativi, aggiornamenti legislativi in relazione ai Reati, ecc. Tali modifiche e/o integrazioni delle Attività Sensibili dovranno essere successivamente approvate dall'Organo Amministrativo della Società.

1.2.2 Principi generali di comportamento

Tutti i Destinatari del Modello, nell'espletamento delle rispettive attività e funzioni, devono agire nel rispetto, oltre che delle previsioni contenute nel MOG e nel Codice Etico 231, delle procedure aziendali adottate dalla Società in relazione alle Attività Sensibili al fine di prevenire la commissione dei Delitti Informatici.

In generale, per tutte le operazioni che concernono le Attività Sensibili individuate nel precedente paragrafo 1.2.1, la Società stabilisce i seguenti principi:

- il trattamento informatico dei dati viene operato in osservanza di adeguate misure di sicurezza quali quelle contenute nel d.lgs. 196/2003, nel Regolamento generale per la protezione dei dati personali 2016/679 e nelle *best practice* di riferimento;
- la formazione e l'attuazione delle decisioni della Società rispondono ai principi e alle prescrizioni contenute nelle disposizioni di legge, dell'atto costitutivo, del Modello e del Codice Etico 231;
- i soggetti e le funzioni coinvolti nello svolgimento dell'Attività Sensibile e/o i sistemi informativi utilizzati assicurano l'individuazione e la ricostruzione delle fonti, degli elementi informativi e dei controlli effettuati che supportano la formazione e l'attuazione delle decisioni della Società;
- non vi deve essere identità soggettiva fra coloro che assumono o attuano le decisioni e coloro che sono tenuti a svolgere sulle stesse i controlli previsti dalla legge e dalle procedure contemplate dal sistema di controllo interno;
- le fasi di formazione e i livelli autorizzativi degli atti della Società sono sempre documentati e ricostruibili;
- sono formalizzate le responsabilità di gestione, coordinamento e controllo all'interno della Società;
- l'assegnazione e l'esercizio dei poteri nell'ambito di un processo decisionale deve essere congruente con le posizioni di responsabilità dei soggetti coinvolti;

- sono formalizzati i livelli di dipendenza gerarchica e sono descritte le mansioni di ciascun Dipendente della Società;
- il sistema di deleghe e poteri di firma verso l'esterno è coerente con le responsabilità assegnate a ciascun amministratore; la conoscenza da parte dei soggetti esterni del sistema di deleghe e dei poteri di firma è garantito da strumenti di comunicazione e di pubblicità adeguati;
- la scelta dei fornitori avviene sulla base di requisiti predeterminati e verificati dalla Società.

1.2.3 Il Responsabile Interno per le Attività Sensibili

In linea con la *best practice*, la Società individua e nomina uno o più Responsabili Interni per le Attività Sensibili individuate. In assenza della nomina dei Responsabili Interni da parte della Società per una o più Attività Sensibili, il Responsabile Interno sarà ritenuto il coordinatore dei sistemi informativi.

Il Responsabile Interno:

- può chiedere informazioni e chiarimenti a tutte le funzioni aziendali, alle unità operative o ai singoli soggetti che sono coinvolti nella relativa Attività Sensibile;
- informa periodicamente l'OdV dei fatti rilevanti relativi alle operazioni a rischio della propria funzione con riferimento all'Attività Sensibile;
- può interpellare l'OdV in tutti i casi di inefficacia, inadeguatezza o difficoltà di attuazione dei protocolli di prevenzione o delle procedure operative di attuazione degli stessi o al fine di ottenere chiarimenti in merito agli obiettivi e alle modalità di prevenzione previste dal Modello.

La Società istituisce una procedura relativa ai flussi informativi nei confronti dell'OdV da parte del Responsabile Interno specificando le informazioni che devono essere inviate allo stesso e le relative modalità di trasmissione.

L'OdV cura l'emanazione e l'aggiornamento di istruzioni standardizzate relative a:

- la compilazione omogenea e coerente dei *reports* da inviare all'OdV;
- gli strumenti di controllo e monitoraggio sulle Attività Sensibili.

Inoltre, l'OdV comunica i risultati della propria attività di vigilanza e controllo in materia di Delitti Informatici all'Organo Amministrativo ed all'Organo di Controllo (revisore), secondo le modalità previste nel Modello.

1.2.4 Protocolli di Prevenzione

La Società definisce i seguenti protocolli di prevenzione[4] rilevanti in relazione alle operazioni effettuate dalla Società con riferimento alle Attività Sensibili identificate al precedente paragrafo 1.2.1. Tali protocolli sono contenuti nelle procedure aziendali adottate dalla Società al fine di prevenire il rischio di commissione dei Delitti Informatici nello svolgimento delle operazioni relative a tali attività.

Laddove l'Attività Sensibile ai fini dei Delitti Informatici sia svolta in regime di *outsourcing* da altra società, o in capo al socio unico, o ad un fornitore esterno, i protocolli di prevenzione potranno essere recepiti nell'ambito dei contratti di servizio relativi allo svolgimento dell'attività. Detti contratti potranno altresì prevedere apposite clausole che prevedono l'impegno delle controparti al rispetto del MOG e del Codice Etico 231, nonché adeguate sanzioni nel caso di violazione delle previsioni contenute negli stessi. Qualora ritenuto opportuno, il contratto potrà prevede inoltre l'obbligo in capo alla controparte di ottemperare alle richieste di informazioni o di esibizione di documenti da parte dell'Organismo di Vigilanza e di segnalare direttamente a quest'ultimo le violazioni del Modello o delle procedure stabilite per la sua attuazione.

I protocolli di prevenzione di seguito riportati sono da applicarsi in base alla tipologia e caratteristiche dell'apparato/applicazione informatica nonché alla classe di appartenenza nella catena tecnologica (come in seguito evidenziato):

- applicazioni;
- *database*;
- sistema operativo;
- apparato di sicurezza/accesso perimetrale (IDS, *firewall*, *proxy*, VPN);
- apparato di connettività (*router*, *switch*, centrale di comunicazione);
- altro *device* (centralina di misurazione e comunicazione).

Relativamente all'Attività Sensibile "**definizione delle regole da adottare in materia di sicurezza del sistema informatico e telematico**", i protocolli di prevenzione sono i seguenti:

- Disposizioni sulla sicurezza: le regole in materia di sicurezza del sistema informatico e telematico adottate dalla Società includono:

  (a) la definizione della metodologia nell'analisi e valutazione dei rischi, degli obiettivi della sicurezza, delle linee guida, degli

[4] In attesa di una sezione delle Linee Guida di Confindustria espressamente dedicata alla materia, i protocolli relativi ai delitti informatici e trattamento illecito dei dati sono stati elaborati sulla base:

- dello standard ISO 27001, che fornisce i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni (ISMS) finalizzato ad una corretta gestione dei dati sensibili dell'azienda;
- del *framework* CObIT, che rappresenta il modello di riferimento per la gestione della *Information and Communication Technology* (ICT);
- del SAS 70, *audit* standard riconosciuto a livello internazionale per i controlli di sicurezza rivolti ai fornitori di servizi, che prevedono controlli sulle reti, ambienti informatici e relativi processi.

strumenti normativi e delle modalità di aggiornamento, anche a seguito di cambiamenti significativi;

(b) l'identificazione dei ruoli e delle responsabilità dei soggetti coinvolti;

(c) i rapporti con gli *outsourcer* informatici;

(d) la definizione di clausole contrattuali relative alla gestione delle misure di sicurezza da parte degli *outsourcer*;

(e) la definizione di ruoli e responsabilità nel trattamento dei dati e delle informazioni e i relativi principi di classificazione (confidenzialità, autenticità e integrità).

- Risorse umane e sicurezza: nell'ambito della gestione delle risorse umane la Società provvede all'applicazione delle seguenti misure:

  (a) una valutazione (prima dell'assunzione o della stipula di un contratto) dell'esperienza delle persone destinate a svolgere attività IT, con particolare riferimento alla sicurezza del sistema informatico;

  (b) l'attuazione di specifiche attività di formazione e aggiornamenti periodici sulle procedure aziendali di sicurezza del sistema informatico per tutti i dipendenti e, dove rilevante, per i terzi;

  (c) l'obbligo di restituzione dei beni forniti per lo svolgimento dell'attività lavorativa (ad es. PC, telefoni cellulari, *token* di autenticazione, ecc.) per i dipendenti e i terzi al momento della conclusione del rapporto di lavoro e/o del contratto.

- Amministratori di sistema: la Società adempie alle prescrizioni del Garante per la protezione dei dati personali in tema di attribuzione delle funzioni di amministratore di sistema, con riferimento, in particolare, a quanto segue: a) la valutazione delle caratteristiche soggettive; b) le designazioni individuali; c) l'elenco degli amministratori di sistema; d) i servizi in *outsourcing* (servizi forniti da terze parti); e) la verifica delle attività; f) la registrazione degli accessi.

Relativamente all'Attività Sensibile "**gestione degli accessi al sistema informatico degli utenti interni ed esterni, dei profili utente e del processo di autenticazione**", i protocolli di prevenzione sono i seguenti:

- Organizzazione della sicurezza per gli utenti interni ed esterni: la Società definisce ruoli e responsabilità degli utenti interni ed esterni all'azienda ai fini della sicurezza del sistema, e i connessi obblighi nell'utilizzo del sistema informatico e delle risorse informatiche e telematiche (anche con riferimento all'accesso a risorse telematiche in possesso di enti terzi la cui gestione del sistema di sicurezza ricade sulla parte terza stessa).

- Controllo degli accessi: l'accesso alle informazioni, al sistema informatico, alla rete, ai sistemi operativi e alle applicazioni viene sottoposto a controllo da parte della Società attraverso l'adozione di misure selezionate in base alla tipologia dell'apparato e alla catena tecnologica in esame, tra le quali:

  (a) l'autenticazione individuale degli utenti tramite codice identificativo dell'utente e password o altro sistema di autenticazione sicura (valido per tutta la catena tecnologica ad eccezione degli apparati di misurazione e comunicazione);

  (b) le autorizzazioni specifiche dei diversi utenti o categorie di utenti (valido per tutta la catena tecnologica ad eccezione degli apparati di misurazione e comunicazione);

  (c) procedimenti di registrazione e deregistrazione per accordare e revocare, in caso di cessazione o cambiamento del tipo di rapporto o dei compiti assegnati, l'accesso a tutti i sistemi e servizi informativi, anche di terzi (valido per tutta la catena tecnologica ad eccezione degli apparati di misurazione e comunicazione);

  (d) la rivisitazione periodica dei diritti d'accesso degli utenti (valido per tutta la catena tecnologica ad eccezione degli apparati di misurazione e comunicazione);

  (e) l'accesso ai servizi di rete esclusivamente da parte degli utenti specificamente autorizzati e le restrizioni della capacità degli utenti di connettersi alla rete (anche se tali diritti permettono di connettersi a reti e dispositivi di terze parti, la cui gestione del sistema di sicurezza ricade sulla parte terza stessa);

  (f) la chiusura di sessioni inattive dopo un limitato periodo di tempo (valido per le postazioni di lavoro e per le connessioni ad applicazioni, come ad esempio *screen saver*).

Relativamente all'Attività Sensibile "**gestione degli aspetti concernenti la sicurezza informatica di documenti elettronici con valore probatorio, della protezione delle reti e delle comunicazioni**", i protocolli di prevenzione sono i seguenti:

- Crittografia: la Società utilizza controlli crittografici per la protezione delle informazioni e regolamenta la gestione delle chiavi crittografiche al fine di evitare un uso non appropriato della firma digitale.

- Gestione delle comunicazioni e dell'operatività*:* la sicurezza del sistema informatico e telematico viene garantita da parte della Società attraverso l'adozione di misure selezionate in base alla tipologia dell'apparato e alla catena tecnologica in esame, tra le quali:

(a) le misure volte a garantire e monitorare la disponibilità degli elaboratori di informazioni (valido per tutte le applicazioni sulla base delle funzionalità di sicurezza disponibili e per i database e i sistemi operativi da esse sottese);

(b) la protezione da *software* pericoloso (es. *worm* e *virus*) (valido, sottoforma di antivirus per gli ambienti Microsoft sia *client* che *server* e di *patch management* per gli altri sistemi e apparati di comunicazione come *router*, *switch* e per apparati *firewall*);

(c) il *backup* di informazioni di uso centralizzato e del *software* applicativo ritenuto critico (valido per le applicazioni e database da esse sottese) nonché delle informazioni salvate nelle aree condivise centralizzate;

(d) la previsione e la disponibilità, anche per gli utenti finali, di strumenti di protezione volti a garantire la sicurezza nello scambio di informazioni critiche per il *business* aziendale e di carattere confidenziale anche con terzi;

(e) gli strumenti per effettuare:

i) la registrazione delle attività eseguite sulle applicazioni, sui sistemi e sulle reti che abbiano diretto impatto sulla sicurezza o relative agli accessi alle risorse informatiche e telematiche;

ii) la registrazione delle attività effettuate dagli utenti verso l'esterno della rete aziendale (es. traffico *http*);

iii) la protezione delle informazioni registrate (*log*) contro accessi non autorizzati;

(f) una verifica periodica/a evento dei *log* che registrano, per quanto rilevante ai fini della sicurezza, gli eventi, le attività degli utilizzatori e le eccezioni (valido per applicazioni e per apparati a diretto impatto sulla sicurezza perimetrale (*proxy*, *firewall*, IDS, *router*);

(g) il controllo che i cambiamenti effettuati agli elaboratori e ai sistemi (valido per le applicazioni e per apparati a diretto impatto sulla sicurezza perimetrale (*proxy*, *firewall*, IDS, *router*) non alterino i livelli di sicurezza;

(h) le regole per la corretta gestione e custodia dei dispostivi di memorizzazione (ad es. PC, telefoni, chiavi USB, CD, *hard disk* esterni, ecc).

Relativamente all'Attività Sensibile "**gestione della sicurezza fisica, ambientale (include sicurezza apparecchiature, cablaggi, dispositivi di rete, informazioni, ecc.) e delle attività di inventariazione dei beni**", il protocollo di prevenzione è il seguente:

- Sicurezza fisica e ambientale: la Società:

(a) dispone l'adozione di controlli al fine di prevenire accessi non autorizzati, danni e interferenze ai locali e ai beni in essi contenuti tramite la messa in sicurezza delle aree e delle apparecchiature con particolare attenzione ai locali dedicati ai centri di elaborazione dati gestiti direttamente;

(b) dispone l'adozione di controlli al fine di prevenire danni e interferenze alle apparecchiature gestite direttamente che garantiscono la connettività e le comunicazioni;

(c) assicura l'inventariazione degli *asset* aziendali (inclusi i *database* in essi contenuti) utilizzati ai fini dell'operatività del sistema informatico e telematico.

Relativamente all'Attività Sensibile "**acquisizione e gestione di apparecchiature, di dispositivi (anche di rilevazione) connessi con il sistema o di programmi informatici (ivi inclusi lo sviluppo degli stessi e i servizi di installazione e manutenzione)**", il protocollo di prevenzione è il seguente:

- Sicurezza nell'acquisizione, sviluppo e manutenzione del sistema informatico (o della componente informatica presente nel servizio) e/o delle componenti tecniche connesse con il sistema: la Società identifica i requisiti di sicurezza e di conformità tecnica (ove applicabile) in fase di acquisizione, sviluppo, fornitura e manutenzione del sistema informatico (inclusivo di componente *hardware*, *software* e delle componenti tecniche connesse).

Relativamente all'Attività Sensibile "**monitoraggio/verifica periodica del sistema informatico e gestione degli incidenti e dei problemi di sicurezza informatica**", i protocolli di prevenzione sono i seguenti:

- Gestione degli incidenti e dei problemi di sicurezza informatica: il trattamento degli incidenti e dei problemi relativi alla sicurezza informatica include:

  (a) l'adozione di canali gestionali per la comunicazione degli incidenti e problemi (relativamente a tutta la catena tecnologica);

  (b) la registrazione, conservazione e analisi periodica degli incidenti e problemi, singoli e ricorrenti e l'individuazione della *root cause* e delle azioni preventive (relativamente a tutta la catena tecnologica);

  (c) la gestione dei problemi che hanno generato uno o più incidenti, fino alla loro soluzione definitiva (relativamente a tutta la catena tecnologica).

- Audit/Monitoraggio: la Società assicura lo svolgimento di attività di monitoraggio/verifica periodica dell'efficacia e operatività del sistema di gestione della sicurezza informatica sia in ambito applicativo che in ambito infrastrutturale, adottando le misure di verifica definite in base alle diverse categorie tecnologiche.

- Amministratori di sistema: la Società adempie alle prescrizioni del Garante per la protezione dei dati personali in tema di attribuzione delle funzioni di amministratore di sistema, con riferimento, in particolare, a quanto segue: a) la valutazione delle caratteristiche soggettive; b) le designazioni individuali; c) l'elenco degli amministratori di sistema; d) i servizi in *outsourcing* (servizi forniti da terze parti); e) la verifica delle attività f) la registrazione degli accessi.

Costituiscono parte integrante del presente Modello le procedure aziendali che danno attuazione ai principi e alle misure di prevenzione sopra indicate per prevenire i Delitti Informatici.

L'Organismo di Vigilanza verifica che le procedure operative aziendali diano piena attuazione ai principi e alle prescrizioni contenute nella presente Parte Speciale C. La presente Parte Speciale C e le procedure operative aziendali che ne danno attuazione sono costantemente aggiornate, anche su proposta o segnalazione dell'Organismo di Vigilanza, al fine di garantire il raggiungimento delle finalità del presente Modello.

Di seguito l'estratto della tabella dei flussi verso l'OdV:

REATI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI			
Attività di riferimento	**Flusso informativo all'ODV**	**Referente**	**Periodicità**
Gestione eventi di sicurezza informatica	- Elenco vulnerabilità rilevate - Elenco *data breach* - Procedure sulla sicurezza informatica	ICTe Amministratore o suo delegato	Semestrale (*data breach* immediato ad evento)

Violazione del diritto d'autore

Anche se dall'analisi dei rischi non sono emerse criticità tali da considerare i reati che interessano le violazioni del diritto d'autore meritevoli di essere considerate in una parte speciale di codesto Modello, si è voluto garantire il flusso di informazione verso l'OdV come controllo costante di tali attività.

DELITTI IN VIOLAZIONE DEL DIRITTO D'AUTORE			
Attività di riferimento	**Flusso informativo all'ODV**	**Referente**	**Periodicità**
Gestione dei software aziendali e delle banche dati licenziati	- Elenco dei software utilizzati e licenze in essere - Elenco delle banche dati	ICT	Annuale

*****