

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI CITYLIFE S.P.A.

ai sensi del decreto legislativo n. 231 dell'8 giugno 2001

PARTE SPECIALE B REATI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI

Approvato dal Consiglio di Amministrazione di CityLife S.p.A. in data 29 marzo 2022

INDICE

1. Introduzione	3
2. Le fattispecie di Reato in materia di delitti informatici e trattamento illecito dei dati	3
2.1 I reati presupposto.....	3
2.2 Sanzioni	6
2.3 Esclusione della responsabilità amministrativa della Società.....	6
3. Le “attività sensibili” ai fini del D.Lgs. 231/01.....	6
4. Sistema dei controlli	7
4.1 Premessa.....	7
4.2 Principi generali di comportamento	7
4.3 Protocolli di controllo	8

La presente Sezione costituisce parte integrante del Modello di Organizzazione, Gestione e Controllo di cui CityLife S.p.A. si è dotata al fine di soddisfare le esigenze preventive di cui al D.Lgs. 231/01.

Tutti i destinatari del Modello, così come individuati nella Parte Generale del medesimo, sono chiamati all'osservanza dei principi e delle linee di condotta di seguito indicati, nonché a porre in essere, ciascuno in relazione alla funzione in concreto esercitata, comportamenti conformi ad ogni altra procedura e/o policy adottata dalla Società, così come analiticamente indicate nella Parte Generale, Capitolo 2, Paragrafo 2.4, che regolino in qualsiasi modo le attività rientranti nell'ambito di applicazione del Decreto.

1. Introduzione

L'art. 7 della legge 18 marzo 2008 n. 48, mediante l'inserimento nell'ambito del D. Lgs. 231/01 dell'art 24 bis sui delitti informatici e trattamento illecito dei dati di seguito riportati, ha introdotto nuove fattispecie di reato che possono generare una responsabilità in capo alla Società.

L'adozione da parte di CityLife di un Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs 231/01 in grado di prevenire adeguatamente le differenti ipotesi di illecito introdotte con tale normativa, trova il proprio presupposto fondamentale nella volontà di gestire la propria rete informatica attraverso l'adozione di regole e procedure alla cui osservanza tutti i propri dipendenti sono chiamati.

A tale proposito, la Società ha adottato specifiche procedure e misure operative, a cui si compie espresso rinvio e che costituiscono parte integrante del presente Modello, finalizzate a garantire una gestione ed un utilizzo lecito e sicuro del proprio sistema informatico.

A tale scopo, CityLife ha appositamente designato un soggetto qualificato, al quale è stata attribuita la funzione di Responsabile IT, con lo specifico incarico di gestire i sistemi informatici della rete, anche attraverso un costante monitoraggio avente ad oggetto un corretto e sicuro utilizzo dei medesimi.

2. Le fattispecie di Reato in materia di delitti informatici e trattamento illecito dei dati

2.1. I reati presupposto

Di seguito si riporta il testo degli articoli del codice penale che descrivono i reati "presupposto" della responsabilità amministrativa della Società, in relazione ai delitti informatici e trattamento illecito dei dati.

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

1. Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione sino a tre anni.

2. La pena è della reclusione da uno a cinque anni:

1. 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;

2. se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3. se 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.

3. Qualora i fatti di cui al comma primo e secondo 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 pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

4. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.)

1. Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna 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, è punito con la reclusione sino ad un anno e con la multa sino ad euro 5.164.

2. La pena è della reclusione da uno a due anni e della multa da euro 5.164 ad euro 10.329 se ricorre taluna delle circostanze di cui al numero 1) e 2) del quarto comma dell'articolo 617 *quater*.

Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 quinquies c.p.)

1. Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino ad euro 10.329.

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

1. Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrente fra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

2. Salvo che il fatto costituisce più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

3. I delitti di cui al comma primo e secondo sono punibili a querela della persona offesa.

4. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1. in danno di un sistema informatico o telematico utilizzato dalla Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;
2. 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;
3. da chi esercita anche abusivamente la professione di investigatore privato.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.)

1. Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti fra più sistemi, è punito con la reclusione da uno a quattro anni.

2. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617 *quater*.

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

1. Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.
2. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio.

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.)

1. Salvo che il fatto costituisca più grave reato, 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, è punito con la reclusione da uno a quattro anni.
2. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.
3. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

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

1. Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'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 punito con la reclusione da uno a cinque anni.
2. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

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

1. Se il fatto di cui all'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, la pena è della reclusione da uno a quattro anni.
2. 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, la pena è della reclusione da tre a otto anni.
3. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (Art. 640 quinquies c.p.)

1. Il 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, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro

Documenti informatici (art. 491 bis c.p.)

1. Se alcune delle falsità previste dal presente capo riguardano un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenete dati o informazioni aventi efficacia probatoria o specificatamente destinati ad elaborarli

2.2. Sanzioni

L'articolo 24 bis del D. Lgs. 231/01, introdotto dall'articolo 7 della Legge 18 marzo 2008 n. 48, prevede sanzioni pecuniarie ed interdittive applicabili alla Società in caso di commissione degli illeciti ivi richiamati, nei termini di seguito indicati.

1. In relazione alla commissione dei delitti di cui agli articoli 615-ter, 617-quater, 617-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.
2. In relazione alla commissione dei delitti di cui agli articoli 615-quater e 615-quinquies del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.
3. In relazione alla commissione dei delitti di cui agli articoli 491-bis e 640-quinquies del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.
4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

2.3. Esclusione della responsabilità amministrativa della Società

Per una compiuta analisi dei presupposti di cui agli articoli 6 e 7 del Decreto, che consentono di addivenire ad una pronuncia che escluda la responsabilità della Società, si compie un espresso rimando al capitolo 1, paragrafo 4 della Parte Generale del presente Modello.

3. Le attività “sensibili” ai fini del D.Lgs. 231/01

Tali attività sono state individuate con riferimento al complessivo utilizzo dei sistemi informativi di cui la Società è dotata, realizzato mediante l'impiego di sistemi *hardware* e *software*, di accesso alla rete internet, di utilizzo di sistemi di posta elettronica o di altri sistemi di comunicazione telematica.

La funzione di gestione dei Sistemi Informativi costituisce l'area aziendale che, per le caratteristiche dell'attività e le competenze richieste, è maggiormente esposta al rischio potenziale di incorrere nei reati di cui all'art. 24 bis del Decreto; tuttavia, non si può realisticamente escludere alcuna area aziendale dal rischio di commissione dei delitti informatici, nella misura in cui in essa si faccia uso di sistemi *hardware*, *software* e telematici.

In particolare, adeguate procedure e controlli sono previsti per una corretta gestione dell'intero flusso comunicativo e informativo relativo alla Società, sia con riferimento alle informazioni ed ai documenti in fase di ingresso, che a quelli in fase di uscita.

Parimenti è necessario dotarsi di adeguati strumenti che permettano di evitare non solo la perdita di dati e/o informazioni importanti per la Società, ma altresì la loro modifica o alterazione attuata per scopi illeciti attraverso, in primo luogo, la possibilità di risalire con certezza al titolare del documento, rendendo in tal modo individuabile il soggetto a cui il medesimo è riconducibile.

Particolare attenzione viene altresì riservata alla necessità di garantire una certa flessibilità del Modello stesso, il quale è opportunamente costituito in modo da poter essere sempre oggetto di modificazione od integrazione alla luce di eventuali evoluzioni della struttura aziendale o di progressi tecnologici in materia.

4. Sistema dei controlli

4.1 Premessa

La Società, nell'adeguare il proprio Modello ai reati in materia di delitti informatici e trattamento illecito dei dati, ha tenuto conto dei seguenti indirizzi:

- delle previsioni del Decreto;
- della vigente disciplina legislativa in materia di protezione dei dati personali di cui al D. Lgs. 196 del 30 giugno 2003;
- del Codice di Comportamento delle imprese di costruzione ai sensi dell'art. 6, comma 3, del Decreto;
- delle Linee Guida Confindustria.

4.2 Principi generali di comportamento

Tutti i dipendenti di CityLife destinatari del Modello si devono attenere a principi di ordine generale al fine di prevenire, ed impedire, il verificarsi degli illeciti in materia informatica e di trattamento illecito dei dati.

In particolare essi:

- si astengono dalla falsificazione di qualsiasi documento informatico;
- si astengono dall'effettuare accessi abusivi a sistemi informatici o telematici e dal detenere o diffondere abusivamente codici di accesso a sistemi informatici o telematici;
- non usano né diffondono apparecchiature, dispositivi o programmi informatici che possano in qualsiasi modo danneggiare o interrompere un sistema informatico o telematico;
- si astengono dall'intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche e dall'installare apparecchiature idonee ad intercettare, impedire o interrompere illecitamente comunicazioni informatiche o telematiche;
- non effettuano alcuna attività rivolta al danneggiamento di informazioni, dati e programmi informatici o al danneggiamento di sistemi informatici e telematici;
- si attengono scrupolosamente alle istruzioni operative e alle procedure aziendali diffuse e in uso presso CityLife.

La Società, tramite il Responsabile IT, assicura che il collegamento alla rete aziendale (abilitato dal reparto IT) sia sempre tracciato tramite opportuni log.

Ulteriori regole di condotta di portata più specifica devono poi essere osservate da tutti i dipendenti della Società che hanno accesso e che utilizzano il sistema informatico di CityLife, ai quali viene assegnato un *computer*, portatile o fisso (di proprietà della medesima), al solo scopo di eseguire attività inerente alle mansioni esercitate.

A tutti i destinatari del Modello è vietato

- utilizzare il *computer* a propria disposizione per scopi esclusivamente personali;
- eseguire o tentare di eseguire installazioni di prodotti *software* in proprio possesso senza l'autorizzazione del Responsabile IT;
- consentire a soggetti, interni od esterni alla Società, di accedere al proprio *computer* anche temporaneamente, se non dopo essersi collegati alla rete con il proprio identificativo;
- salvare dati al di fuori del proprio profilo utente in modo che siano visibili da altri che si collegano al *computer* con un altro identificativo;
- copiare dati aziendali sui *computer* personali o su dispositivi rimovibili, qualora non sia strettamente necessario per fini lavorativi;

- inviare per posta elettronica dati sensibili;
- configurare l'accesso remoto a CityLife su *computer* diversi da quello in uso;
- consentire a chiunque esterno all'azienda di collegare il proprio *computer* alla rete aziendale senza previa autorizzazione del Responsabile IT.

Ogni Destinatario del Modello ha invece l'obbligo di:

- bloccare il *computer* mediante la sequenza Ctrl+Alt+Canc (blocco del computer) ogni qualvolta si allontana, anche per pochi minuti, dalla propria postazione;
- evitare di condividere documenti e *file* in genere con il *computer* personale o di altri;
- segnalare tempestivamente al Responsabile IT qualsiasi anomalia riconducibile ad un *virus* o ad un attacco informatico;
- utilizzare adeguatamente il *computer* stesso evitando inutili sprechi di traffico dati;
- avvisare immediatamente il Responsabile IT qualora sia notato personale presumibilmente non autorizzato che movimenta i cavi di rete, collega apparati di qualunque tipo alla rete informatica e/o telefonica, oppure accede ai locali tecnici;
- avvisare immediatamente il Responsabile IT qualora al medesimo venga indebitamente sottratto il proprio *computer* o qualsiasi altro dispositivo utilizzato per connettersi alla rete di CityLife;
- avvisare tempestivamente il Responsabile IT o il Responsabile Personale quando qualche collaboratore di CityLife termina il proprio rapporto di collaborazione, in modo tale che il Responsabile IT possa essere in grado di disabilitare gli accessi.

4.3 Protocolli di controllo

Tutti i Destinatari del Modello, adottano regole di condotta conformi:

- ai principi contenuti nel Codice Etico (che qui si intende integralmente richiamato) che costituiscono presupposto e parte integrante dei protocolli di prevenzione di seguito declinati;
- ai protocolli di prevenzione generali previsti dal paragrafo 3.4.4., capitolo 3 della Parte Generale;
- ai protocolli di prevenzione specifici di seguito rappresentati.

Responsabili del processo
Amministratore Delegato

Responsabile Interno per le Attività Sensibili
Responsabile IT

Obbligo di inventario

Il Responsabile IT verifica almeno annualmente l'esatta consistenza del materiale informatico presente in CityLife, evidenziando, in particolare, la presenza di:

- *computers*;
- *softwares*;
- connessioni *internet*;
- *server*;
- contratti di licenza di programmi informatici;
- *account* di posta elettronica;
- altri supporti informatici.

L'Ufficio IT redige (e aggiorna) un documento nel quale, oltre alla descrizione del materiale informatico presente in azienda, indica per ciascun dipendente le dotazioni rispettivamente assegnate.

Protezione della rete da intrusioni informatiche, virus, etc.

L'Ufficio IT garantisce la protezione della rete informatica con misure tecnologicamente adeguate.

In particolare il Responsabile IT cura che:

- tutti i *computer* aziendali (fissi e portatili) ed il *server* siano dotati di sistemi antivirus, *firewall* e protezioni da eventuali aggressioni esterne;
- i sistemi antivirus siano quotidianamente aggiornati secondo un programma di *upgrade* aggiornato;
- ogni supporto che venga installato e/o utilizzato su *computer* aziendali sia preventivamente sottoposto a scansione antivirus.

Protezione del materiale informatico da utilizzi impropri

L'Ufficio IT cura che tutti i *computer* siano dotati di *username* personale riferibile al singolo utente, nonché di una *password* di protezione che deve essere inserita dall'utilizzatore.

I *computes* aziendali devono essere impostati in modo che durante la fase di *standby* l'utilizzo divenga possibile solo previo inserimento della *password*.

Il *server* aziendale deve essere collocato in un locale protetto e l'accesso al medesimo deve essere consentito solo ai componenti dell'Ufficio IT, che, ove strettamente necessario, possono a loro volta consentire l'accesso, alla loro presenza, di altri dipendenti di CityLife o di tecnici esterni autorizzati.

Utilizzo della posta elettronica

Ogni dipendente o collaboratore di CityLife ha assegnato un indirizzo di posta elettronica personale sul dominio di CityLife.

L'accesso all'indirizzo di posta elettronica è riservato esclusivamente al titolare e, a tal fine, ogni *account* viene protetto da un password inserita dallo stesso.

E' fatto divieto di utilizzare indirizzi di posta elettronica altrui, salvo che ciò non sia giustificato da motivi tecnici e purchè vi sia preventiva autorizzazione da parte del titolare.

L'*account* di posta elettronica deve essere utilizzato esclusivamente per ragioni connesse con l'attività lavorativa.

Programmi installati sui computer aziendali

I dipendenti e collaboratori di CityLife devono utilizzare esclusivamente i *software* loro assegnati. Senza la preventiva autorizzazione del Responsabile IT è fatto divieto di installare qualsiasi programma da parte dell'utente o di altri operatori.

Formazione dei dipendenti

Il Responsabile IT cura che sia impartita a tutti i dipendenti e collaboratori di CityLife adeguata formazione tecnica sull'utilizzo della strumentazione informatica e sulle regole comportamentali e procedurali a cui si devono attenere.

A tal fine il Responsabile IT cura che tutti i dipendenti e collaboratori abbiano conoscenza delle istruzioni operative adottate da CityLife in merito all'utilizzo di sistemi informatici, nonché dei presenti Protocolli.

