MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO
AI SENSI DEL DECRETO LEGISLATIVO 231/01

PARTE SPECIALE E
REATI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI
(ARTICOLO 24-BIS DEL DLGS. 231/2001)

SOMMARIO

1 PREMESSA

Di seguito all'introduzione dell'art. 24 bis al Dlgs. 231/2001, in virtù dell'art 7 della Legge 18 marzo 2008, n. 48, modificato successivamente dal D.Lgs. n. 7 e 8/2016 e dal D.L. n. 105/2019, si è verificato un allargamento del novero dei reati per i quali si può configurare la responsabilità amministrativa dell’Ente, e precisamente:

- Delitti informatici e trattamento illecito dei dati (articolo 24-bis del Dlgs. 231/2001).

Nel corso dei primi mesi del 2022, ulteriori novità legislative sono intervenute a modificare il dettato normativo del D. Lgs. n. 231/2001 modificando ed allargando le maglie di alcune fattispecie incluse nel catalogo dei reati presupposto. In questo contesto, di particolare interesse risultano essere le previsioni di cui alla Legge n. 238/2021 recante "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea - Legge Europea 2019-2020" ("Legge Europea 2019-2020"),

In particolare, l'articolo 615-quater c.p. vede una nuova rubricazione, un ampliamento delle condotte punibili e una modificazione in termini di cornice edittale. La nuova disposizione, rubricata ora "Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici", prevede che sia punibile il soggetto che "abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza al fine di arrecare a sé o ad altri un profitto o di arrecare ad altri un danno". La pena della reclusione si estende sino a due anni nell'ipotesi base, mentre da uno a tre anni se ricorre una delle circostanze di cui all'articolo 617- quater comma 4.

L'articolo 615-quinquies c.p. ora rubricato "Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico" e così come modificato dalla suddetta legge, si connota per una nuova formulazione della condotta punibile ora rivolta a "Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, 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 adisposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329".

Con riferimento all'art. 617-quater c.p., vengono inasprite le pene per l'ipotesi di cui al primo comma ora punita con la reclusione "da un anno e sei mesi a cinque anni", nonché di quella prevista dal comma quarto per la quale si prevede un innalzamento della pena edittale "da tre a otto anni".

L'articolo 617-quinquies ora rubricato "Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche" si connota per una nuova formulazione relativa alle condotte punibili che prevedono ora l'attivazione della risposta sanzionatoria nei confronti di chiunque "procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi" con il fine di "intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle".

Per tale tipologia di reati, in sede di elaborazione delle singole Parti Speciali al Modello di organizzazione, gestione e controllo (di seguito denominato il “Modello”) dirette a prevenire o comunque ridurre fortemente il rischio di commissione di reati attraverso linee guida per le misure e procedure (quali, per esempio, la separazione tra funzioni, la partecipazione di più soggetti alla medesima attività decisionale a rischio, specifici obblighi di autorizzazione e di documentazione

per la fasi maggiormente sensibili) si è ritenuto, attraverso l’esecuzione di un processo di analisi e valutazione dei diversi fattori di rischio incentrato su quanto posto in essere per la gestione del regolamento UE 679/2016 (dettagliato maggiormente al successivo paragrafo 1.1), che la specifica attività svolta dalla Società non presentava profili di rischio tali da rendere ragionevolmente fondata la possibilità della loro commissione nell’interesse o a vantaggio della stessa.

Al riguardo, si è considerato pertanto esaustivo il richiamo ai principi contenuti nella Parte Generale del Modello, nel successivo paragrafo 1.1 e nel Codice Etico, che vincolano i Destinatari del Modello stesso al loro rispetto.

Tuttavia occorre rammentare che l'Italia oltre ad essere stato uno dei primi Paesi Europei ad aver adottato una disciplina organica in tema di delitti informatici (L. n. 547/1993) poi seguita da altre leggi relative a specifici settori (es. L. n. 248/2000 sulla pirateria informatica e L. n. 269/1998 contro lo scambio di materiale pedopornografico in rete) ha introdotto, per quanto di interesse, con la legge 190/2012, un nuovo campo d'azione attraverso la configurazione della “Corruzione tra privati” qualificando così come corruzione anche gli accordi illeciti tra privati, al pari di quelli che intercorrono tra il privato ed il Pubblico Ufficiale.

Il concetto di corruzione dal 2012 deve essere inteso in senso lato ed includere situazioni in cui, anche esorbitando dall'ambito della fattispecie penale, un soggetto, nell'esercizio dell'attività amministrativa - aziendale, abusi del potere attribuitogli al fine di ottenere un vantaggio privato o, comunque, situazioni in cui – a prescindere dalla rilevanza penale -venga in evidenza un malfunzionamento dell'Ente a causa dell'uso ai fini privati delle funzioni attribuite.

Pertanto per individuare la responsabilità amministrativa dell'Ente non occorre più che la commissione del reato da parte del dipendente, avvenga nell’interesse o a vantaggio dello stesso, basta semplicemente aver agito anche solo per vantaggio privato.

E' pertanto indubbio che, attraverso l'accesso e l'utilizzo degli strumenti "*informatici*" ordinariamente in uso, in vigenza della predetta normativa, si possano intravvedere profili di rischio.

Recentemente l’introduzione del D.L. 105/2019 convertito dalla L. 18 novembre 2019, n. 133 (in G.U. 20/11/2019, n. 272), istituisce il perimetro di sicurezza nazionale cibernetica, al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale (un maggiore approfondimento sugli obblighi è illustrato al successivo paragrafo 1.2)

Inoltre, a seguito dell’entrata in vigore a maggio 2018 del regolamento UE 679/2016 GDPR, la gestione dei dati informatici, trattata nella seguente sezione, viene effettuata con i documenti elaborati ai sensi della normativa (registro dei trattamenti, informative, ecc) tenendo conto delle risorse umane e tecniche esistenti alla data di valutazione.

A tal proposito la compliance allo stesso regolamento UE 679/2016 richiede l’adozione degli strumenti necessari per assicurare il più alto grado di tutela dei dati personali estratti dai database aziendali, tramite l’adeguamento al GDPR dei c.d. MOG 231, ossia i modelli di organizzazione e gestione aziendale previsti dagli artt. 6 e 7 del D. Lgs. n. 231/2001, che contribuiscono a tipizzare il nesso di imputazione soggettiva della responsabilità delle persone giuridiche, articolandolo sulla base di categorie soggettive a cui appartengono gli autori del reato-presupposto e, più precisamente, del legame funzionale di questi con l’ente.

Tali modelli organizzativi privacy, tenendo conto dei rischi emergenti dalle attività aziendali che richiedono il trattamento dei dati personali ex art. 4 n. 2) del Regolamento n.679/2016, risultano quindi utili, se non fondamentali, per garantire la prevenzione dell’eventuale responsabilità dell’azienda derivante da reati commessi in suo vantaggio e/o interesse da dipendenti o soggetti in posizioni apicali all’interno della stessa.

1.1 Policy informatica e principi di comportamento

La Politica informatica operata sinora della Società è stata ispirata ai principi introdotti dalla legge 196/03 entrata in vigore il 01.01.2004 noto anche come "Codice della Privacy" che ha stabilito le

misure minime da adottare per garantire la tutela dei dati personali trattati dall'Azienda e la sicurezza nell'ambito del loro trattamento ed archiviazione. Successivamente si è conformata a quanto previsto dal regolamento UE 679/2016 GDPR, entrato in vigore il 25/05/2018. A giugno 2022 è stata completata la revisione del sistema posto in essere per la gestione del regolamento UE 679/2016 GDPR. Il processo di revisione è stato sviluppato attraverso le seguenti fasi: AS IS - analisi dei processi aziendali e valutazione dei rischi; GAP ANALYSIS e sviluppo ed aggiornamento della documentazione tesa a colmare gli scostamenti individuati. I documenti prodotti, ai quali si rimanda per un’analisi di dettaglio, sono:

- Documento di Analisi dei Rischi in materia di trattamento dati personali emesso in data 15/05/2021;
- GAP ANALYSIS e ANALISI dei RISCHI in materia di trattamento dati personali emesso in data 24/06/2021 completo dell’allegato 1 “Misure di adeguamento e miglioramento - Scheda riassuntiva e di sintesi”;

in relazione a quanto emerso dalla gap analysis è stato avviato il processo di revisione dei documenti che vede nell’aggiornamento del registro delle attività di trattamento ai sensi dell’art.30 del regolamento 2016/679 il documento principale che riassume quanto posto in essere in materia di trattamento dei dati e sicurezza informatica.

Nel registro sono stati individuati i trattamenti dei dati (funzione/processo di riferimento, tipologia di trattamento, finalità, categorie degli interessati al trattamento, categorie di dati personali trattati e modalità di acquisizione degli stessi), le categorie dei destinatari del trattamento, le modalità di trattamento, i tempi e le modalità di conservazione/archiviazione.

Dallo stesso registro scaturiscono anche le misure legali applicabili ai trattamenti dei dati e la documentazione posta in essere per assicurare il trattamento conforme (in tal senso si veda nel dettaglio il Registro dei trattamenti ed il capitolo 10 dello stesso che riporta l’allegato “l’elenco della documentazione”).

Attraverso il registro dei trattamenti ed i documenti richiamati in esso, sono rappresentati dettagliatamente i sistemi operativi in uso, i livelli di accesso, la distribuzione dei compiti, delle responsabilità, le verifiche periodiche, l'individuazione degli amministratori dei servizi informatici e degli incaricati preposti al trattamento dei dati e, quindi, in sintesi all'utilizzo dei sistemi, nonché la politica di accesso pubblica alla rete informatica aziendale.

La società, inoltre, come previsto dallo stesso regolamento UE 679/2016 agli art. 37-39 ha provveduto alla nomina fin dal 12/06/2018 del Responsabile della Protezione dei Dati Personali (RPD o DPO) al fine di facilitare l’osservanza della normativa in materia e poter disporre di una figura di interfaccia fra i diversi soggetti coinvolti (autorità di controllo, utenti, ecc.) con i seguenti compiti:

- Informare e fornire consulenza al titolare del trattamento o al Responsabile del Trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni nazionali e dell’Unione, relative alla protezione dei dati;
- Sorvegliare l’osservanza del GDPR di altre disposizioni nazionali o dell’Unione relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresa l’attribuzione di responsabilità, la sensibilizzazione e formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- Fornire se richiesto una valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell’art.35 del GDPR;
- Cooperare con il Garante per la protezione dei dati personali;
- Fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all’art.36 ed effettuar se del caso consultazioni relativamente a qualunque questione.

In data 14/12/2021 con protocollo 5068 del 2021 è stata nominato un nuovo Responsabile della Protezione dei Dati Personali che ha successivamente provveduto ad approvare le Valutazioni di impatto sulla protezione dei dati (ex art.35 Reg. UE 679/2016) completate in data 01/06/2022

relative alla videosorveglianza, alla gestione COVID-19 ed alla geolocalizzazione.

Ad integrazione del sistema posto in essere nell’ambito della gestione e protezione dei dati, funzionale al controllo della commissione di reati ex 231/01, ed al fine di garantire il corretto comportamento di tutti i soggetti coinvolti nei processi interessati, si adottano i seguenti principi generali di comportamento finalizzati a vietare espressamente:

- l’istallazione, downloading e/o utilizzo di programmi e tools informatici che permettono di alterare, contraffare, attestare falsamente, sopprimere, distruggere e/o occultare documenti informatici pubblici o privati;
- l’istallazione, downloading e/o utilizzo di programmi e tools informatici che consentono l’introduzione abusiva all’interno di sistemi informatici o telematici protetti da misure di sicurezza o che permettono la permanenza al loro interno, in violazione delle misure poste a presidio degli stessi dal titolare dei dati o dei programmi che si intende custodire o mantenere riservati;
- reperire, diffondere, condividere e/o comunicare passwords, chiavi di accesso o altri mezzi idonei a permettere le condotte di cui ai due punti precedenti;
- utilizzare, reperire, diffondere, condividere e/o comunicare le modalità di impiego di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico;

devono essere pertanto adottati obbligatoriamente i seguenti principi generali e specifici di comportamento:

- rispetto delle licenze, dei diritti d’autore e di tutte le leggi e regolamenti locali nazionali ed internazionali che tutelano la proprietà intellettuale e le attività on-line
- Gestione e monitoraggio degli accessi ai sistemi informatici e telematici nel rispetto del sistema posto in essere per la gestione del regolamento UE 679/2016 relativa alla gestione del rischio informatico che individui le seguenti fasi:
  - identificazione e classificazione delle risorse e individuazione delle relative vulnerabilità ovvero delle carenze di protezione relativamente a una determinata minaccia - con riferimento alle seguenti componenti: (i) infrastrutture (incluse quelle tecnologiche quali le reti e gli impianti), (ii) hardware, (iii) software, (iv) documentazione, (v) dati/informazioni, (vi) risorse umane;
  - individuazione delle minacce, interne ed esterne, cui possono essere esposte le risorse, raggruppabili nelle seguenti tipologie: (i) errori e malfunzionamenti, (ii) frodi e furti, (iii) software dannoso, (iv) danneggiamenti fisici, (v) sovraccarico del sistema, (vi) mancato rispetto della legislazione vigente;
  - individuazione dei danni che possono derivare dal concretizzarsi delle minacce, tenendo conto della loro probabilità di accadimento;
  - identificazione delle possibili contromisure;
  - effettuazione di un'analisi costi/benefici degli investimenti per l’adozione delle contromisure;
  - definizione di un piano di azioni preventive e correttive da porre in essere e da rivedere periodicamente in relazione ai rischi che si intendono contrastare;
  - documentazione e accettazione del rischio residuo.
- Adozione completa di quanto previsto dal Sistema di gestione per il regolamento UE 679/2016 che disciplina i seguenti aspetti:
  - definizione del quadro normativo riferito a tutte le strutture/aree aziendali, con una chiara attribuzione di compiti e responsabilità e indicazione dei corretti comportamenti individuali;
  - costituzione di un polo di competenza in azienda che sia in grado di fornire il necessario supporto consulenziale e specialistico per affrontare le problematiche del trattamento dei dati personali e della tutela legale del software;
  - puntuale pianificazione delle attività di sicurezza informatica;
  - progettazione, realizzazione/test e gestione di un sistema di protezione preventivo;

- definizione di un sistema di emergenza, ovvero predisposizione di tutte le procedure tecnico/organizzative per poter affrontare stati di emergenza e garantire la business continuity attraverso meccanismi di superamento di situazioni anomale;
- applicazione di misure specifiche per garantire la controllabilità e la verificabilità dei processi, anche sotto il profilo della riconducibilità in capo a
- singoli soggetti delle azioni compiute.

- Redazione, diffusione e conservazione dei documenti normativi, tecnici e di indirizzo necessari per un corretto utilizzo del sistema informatico da parte degli utenti e per una efficiente amministrazione della sicurezza da parte delle funzioni aziendali a ciò preposte.
- Attuazione di una politica di formazione e/o di comunicazione inerente alla sicurezza volta a sensibilizzare tutti gli utenti e/o particolari figure professionali.
- Attuazione di un sistema di protezione idoneo a identificare e autenticare univocamente gli utenti che intendono ottenere l’accesso a un sistema elaborativo o trasmissivo. L’identificazione e l’autenticazione devono essere effettuate prima di ulteriori interazioni operative tra il sistema e l’utente; le relative informazioni devono essere memorizzate e accedute solo dagli utenti autorizzati.
- Attuazione di un sistema di accesso logico idoneo a controllare l'uso delle risorse da parte dei processi e degli utenti che si esplichi attraverso la verifica e la gestione dei diritti d'accesso.
- Attuazione di un sistema che prevede il tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici.
- Proceduralizzazione e espletamento di attività di analisi degli eventi registrati volte a rilevare e a segnalare eventi anomali che, discostandosi da standard, soglie e prassi stabilite, possono essere indicativi di eventuali minacce.
- Previsione di strumenti per il riutilizzo di supporti di memoria in condizioni di sicurezza (cancellazione o inizializzazione di supporti riutilizzabili al fine di permetterne il riutilizzo senza problemi di sicurezza).
- Previsione e attuazione di processi e meccanismi che garantiscono la ridondanza delle risorse al fine di un loro ripristino in tempi brevi in caso di indisponibilità dei supporti.
- Protezione del trasferimento dati al fine di assicurare riservatezza, integrità e disponibilità ai canali trasmissivi e alle componenti di networking.
- Predisposizione e attuazione di una politica aziendale di gestione e controllo della sicurezza fisica degli ambienti e delle risorse che vi operano che contempli una puntuale conoscenza dei beni (materiali e immateriali) che costituiscono il patrimonio dell’azienda oggetto di protezione (risorse tecnologiche e informazioni).
- Predisposizione e attuazione di una policy aziendale che stabilisce (i) le modalità secondo le quali i vari utenti possono accedere alle applicazioni, dati e programmi e (ii) un insieme di procedure di controllo idonee a verificare se l’accesso è consentito o negato in base alle suddette regole e a verificare il corretto funzionamento delle regole di disabilitazione delle porte non attive.

Tutte le attività sopraindicate sono gestite opportunamente con i documenti elaborati ai sensi del Regolamento UE 679/2016 GDPR e dei regolamenti interni aziendali.

Per quanto sopra evidenziato, il rispetto del Codice Etico è requisito essenziale per prevenire la configurazione di uno dei reati stabiliti e puniti all’articolo 24-bis e, al contempo, strumento prerogativo da parte della Società per promuovere la cultura dell’etica, dell'integrità, della trasparenza, della correttezza gestionale, oltreché l’osservanza dei valori etici e un costante controllo preventivo della regolarità e della legalità dell’operato dei propri dipendenti e collaboratori.

Alla luce di quanto espresso precedentemente, ne discende che i Principi di comportamento del personale di AnconAmbiente S.p.A devono quindi conformarsi alle disposizioni del Codice Etico adottato e divulgato dalla Società, con particolare riferimento al:

- paragrafo 2.1 I valori etici nell’attività di AnconAmbiente Spa;

- paragrafo 3 I valori etici di AnconAmbiente:

  punto *3.1* Integrità: *"I Destinatari regolano la propria condotta in maniera professionale e responsabile al fine dirimere le situazioni in cui possono manifestarsi potenziali conflitti, assicurando che il comportamento sia caratterizzato da onestà, moralità e correttezza. Il personale, nell'esercizio delle proprie funzioni, ai diversi livelli di responsabilità, non deve assumere decisioni o svolgere attività in conflitto con gli interessi della Società o incompatibili con i doveri di ufficio. Anche gli Amministratori devono attenersi rigorosamente a questo principio";*

  punto *3.3* Legalità : *"I Destinatari regolano la propria condotta nel pieno rispetto delle procedure interne, di tutte le norme vigenti, nazionali e internazionali. I comportamenti dirigenziali, in particolare, devono essere sempre improntati alla correttezza e all'equità, poiché vengono a costituire dei modelli di riferimento per tutti i collaboratori. La Società, quale istituzione economica, produttrice di ricchezza, di lavoro e di tecnologia, a propria tutela disincentiva in ogni modo pratiche di corruzione";*

- paragrafo 4 Principi di comportamento:

  punto 4.4 Nei rapporti con la Pubblica Amministrazione;

  punto 4.6 Nel trattamento delle informazioni riservate o privilegiate;

  punto 4.7 Nella relazione con i mezzi di informazione;

  punto 4.8 Nella tenuta della contabilità e nella comunicazione delle informazioni economiche, patrimoniali e finanziarie;

  punto 4.10 Nella conservazione del patrimonio aziendale: "…. è fatto divieto di utilizzare gli strumenti e le risorse aziendali per scopi o finalità illecite o in contrasto con i principi del Codice."

Risulta infine necessario sensibilizzare tutti i soggetti che operano in AnconAmbiente a segnalare comportamenti non conformi alle prescrizioni in materia informatica ed alle altre norme e procedure interne, se informati, anche indirettamente, di illeciti passibili di conseguenze penalmente rilevanti.

1.2 I Delitti informatici

L'art. 24-bis del Dlgs 231/01 individua i seguenti delitti informatici:

- **falsità in documenti informatici**, previsto dall'art. 491-bis c.p. e costituito dalle ipotesi di falsità, materiale o ideologica, commesse su atti pubblici, certificati, autorizzazioni, scritture private o atti privati, da parte di un rappresentante della Pubblica Amministrazione ovvero da un privato, qualora le stesse abbiano ad oggetto un “documento informatico avente efficacia probatoria”, ossia un documento informatico munito quanto meno di firma elettronica semplice. Per “documento informatico” si intende la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (tale delitto estende la penale perseguibilità dei reati previsti all'interno del Libro II, Titolo VII, Capo III del Codice Penale ai documenti informatici aventi efficacia probatoria);

- **accesso abusivo ad un sistema informatico o telematico**, previsto dall'art. 615-ter c.p. e costituito dalla condotta di chi si introduce abusivamente, ossia eludendo una qualsiasi forma, anche minima, di barriere ostative all'ingresso in un sistema informatico o telematico protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà di chi ha diritto di escluderlo;

- **detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici** *(art. modificato dalla L. n.238/2021),* previsto dall'art. 615-quater c.p. e costituito dalla condotta di chi abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, 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 in questo senso, allo scopo di procurare a sé o ad altri un profitto, o di arrecare ad altri un danno;

- **detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi**

informatici diretti a danneggiare o interrompere un sistema informatico o telematico *(art. modificato dalla L. n.238/2021),* previsto dall'art. 615-quinquies c.p., e che sanziona la condotta di chi, allo scopo di danneggiare illecitamente un sistema informatico o telematico, 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,

- **intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche** *(art. modificato dalla L. n.238/2021),* previsto dall'art. 617-quater c.p., e che punisce la condotta di chi, in maniera fraudolenta, intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi ovvero le impedisce o le interrompe oppure rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto di tali comunicazioni;

- **detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche** *(art. modificato dalla L. n.238/2021),* previsto dall'art. 617-quinquies c.p., e che sanziona la condotta di chi, fuori dai casi consentiti dalla legge, al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi,

- **danneggiamento di informazioni, dati e programmi informatici**, previsto dall'art. 635-bis c.p. e costituito dalla condotta di chi distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui, salvo che il fatto costituisca più grave reato;

- **danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico, o comunque di pubblica utilità**, previsto dall'art. 635-ter c.p. e costituito dalla condotta di chi 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, salvo che il fatto costituisca più grave reato;

- **danneggiamento di sistemi informatici o telematici**, previsto dall'art. 635-quater c.p. e costituito dalla condotta di chi, mediante le condotte di cui all'art. 635-bis c.p., 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 salvo che il fatto costituisca più grave reato;

- **danneggiamento di sistemi informatici o telematici di pubblica utilità**, previsto dall'art. 635-quinquies c.p. e costituito dalla condotta descritta al precedente articolo 635-quater c.p., qualora essa sia diretta a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento;

- **frode informatica del soggetto che presta servizi di certificazione di firma elettronica**, previsto dall'art. 640-quinquies c.p. e costituito dalla condotta del 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 uncertificato qualificato.

- **violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica** *(art. 1, comma 11, D.L. 21 settembre 2019, n. 105),* Il D.L. in questione istituisce il perimetro di sicurezza nazionale cibernetica, al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale, In funzione di quanto sopra, con decreto del Presidente del Consiglio dei Ministri, adottato su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR), vengono individuate le amministrazioni pubbliche e gli operatori nazionali, pubblici e privati inclusi nel perimetro di

sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti in materia. I soggetti di cui trattasi sono tenuti in particolare a predisporre, aggiornare e trasmettere ai ministeri competenti, con cadenza almeno annuale, un elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza. La condotta costituente reato consiste nel fornire - allo scopo di ostacolare o condizionare l'espletamento dei procedimenti di cui al comma 2, lettera b) o al comma 6, lettera a), o delle attività ispettive e di vigilanza previste dal comma 6, lettera c) - informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b), o ai fini delle comunicazioni di cui al comma 6, lettera a), o per lo svolgimento delle attività ispettive e di vigilanza di cui al comma 6), lettera c) od omette di comunicare entro i termini prescritti i predetti dati, informazioni o elementi di fatto. Il reato è punito con la reclusione da uno a tre anni.

1.3 Metodologia utilizzata per l’individuazione e la valutazione del rischio

La possibilità di commettere i reati di cui all’articolo 24-bis del D.lgs. 231/2001 fermo restando che la società potrebbe essere considerata responsabile anche qualora le fattispecie siano integrate nella forma di tentativo, è stata meticolosamente valutata e misurata per ciascun processo e settore aziendale tecnico/amministrativo/operativo sulla base dei compiti e responsabilità ad essi afferenti.

L’analisi dei rischi ad ampio spettro ha consentito di individuare che eventuali condotte illecite commesse nell’interesse o a vantaggio dell’azienda ovvero a proprio esclusivo vantaggio, possono riguardare ciascun settore, calcolando il rischio di commissione dell’illecito sulla base della possibilità che l’evento si verifichi rispetto alla frequenza di effettuazione di ciascuna attività "informatica" e sull’impatto conseguente.

Le considerazioni sopra espresse in forma analitica possono essere sinteticamente riassunte nella semplice formula matematica[1] sotto riportata:

$$\text{rischio che l’illecito si verifichi} = \frac{\text{P.I. x F.S.S}}{\text{N.S.}}$$

1 - P.I. = probabilità che l’illecito si verifichi; F.S.S. = frequenza di svolgimento del servizio; N.S. = natura del servizio.

alla possibilità di commettere uno dei reati previsti dall’articolo 24-bis è stata associata la probabilità che l’evento si verifichi, considerando i rischi immediati e differiti relativi a ciascun servizio, applicando la seguente scala di valori:

- MA: molto alta. Il rischio è connesso con la quotidiana attività di gestione dei sistemi informativi aziendali e replicato con continuità nell'ambito dell'orario lavorativo;
- A: alta. Il rischio è connesso con attività quotidiane di gestione dei sistemi informativi ma non replicato nell'ambito dell'orario lavorativo. L’attività a rischio deve essere scrupolosamente seguita da chi ha responsabilità del servizio;
- M: media. Il rischio è connesso con attività quotidiane che, per loro natura, rendono mediamente difficile la possibilità di porre in essere comportamenti previsti e puniti all’articolo 24-bis;
- B: bassa. Il rischio è connesso con attività che, per specifica operatività e continuo controllo preventivo interno ed esterno, rendono improbabile la commissione di reati;
- MB: molto bassa. Il rischio è connesso con attività marginali che presentano una potenzialità di rischio aleatoria;
- NA: non applicabile. Non riguarda l’attività di AnconAmbiente.

Nello specifico, come sarà meglio dettagliato per ogni singolo processo/servizio, i rischi di commettere azioni illecite riguardano tutti i settori aziendali coinvolti in attività connesse con l'utilizzo dei sistemi informativi aziendali.

1.4 Controlli preventivi

Assumono particolare rilevanza, quale misura di prevenzione dei suddetti reati, il sistema posto in essere per la gestione del regolamento UE 679/2016 GDPR ed i i seguenti processi e attività che sono finalizzati a realizzare il sistema degli adempimenti aziendali, nascenti dalla scelta di AnconAmbiente di dotarsi di un sistema certificato UNI EN ISO 9001:2015, 14001:2015, Regolamento n. 1221/2009 EMAS come modificato dai Regolamenti n. 2026/2018 e n.1505/2017 e UNI EN ISO 45001.2018:

- definizione delle politiche, degli indirizzi e dell’organizzazione connessi alla gestione informatica;
- valutazione dei rischi ed elaborazione dei documenti;
- organizzazione delle criticità;
- informazione e formazione dei lavoratori in materia di gestione dei mezzi informatici e trattamento dati;
- introduzione di specifiche clausole di auditing nei contratti di acquisto di beni e servizi di rilevanza informatica.

Integrano pertanto il Modello Organizzativo della presente parte Speciale, come già “Reati Informatici” il sistema di controllo posto in essere attraverso:

- il sistema per la gestione del regolamento UE 679/2016 (completo delle specifiche tecniche, istruzioni, procedure, regolamenti in esso richiamati)
- Il sistema di gestione certificato UNI EN ISO 9001:2015, UNI EN ISO 14001:2015, UNI EN ISO 45001:2018 ed il Regolamento n. 1221/2009 EMAS come modificato dai Regolamenti n. 2026/2018 e n.1505/2017 (completo delle specifiche tecniche, istruzioni, procedure, regolamenti in esso richiamati)
- il monitoraggio e le verifiche condotte dal RPD nell’ambito della gestione dei dati che comprende anche gli aspetti informatici le misure minime di sicurezza AGID,
- la sorveglianza delle modifiche a cura del Responsabile Qualità aziendale (AQ);

2 INDIVIDUAZIONE E DESCRIZIONE ANALITICA IPOTESI DI RISCHIO DI REATO

I rischi rappresentati nel seguito sono il risultato dell'analisi finalizzata a valutare nell'ambito della platea dei reati elencati all’articolo 24-bis quelli che possono potenzialmente ricadere su ciascuna delle attività e dei servizi quotidianamente effettuati da AnconAmbiente nell’ambito della sua *mission* istituzionale.

In relazione ad AnconAmbiente riesce difficile delineare precise aree di rischio in quanto isuddetti reati si possono astrattamente verificare in ogni momento dell'attività gestionale, laddovela stessa sia organizzata ed esercitata con il mezzo informatico e/o attraverso la connessionealla rete internet. Pertanto tali rischi di reato sono estesi a tutte le unità locali centrali e periferiche che sono coinvolte nell’esecuzione dei medesimi processi descritti nel seguito del documento.

Il recente processo di revisione del regolamento per la gestione dei dati personali con lo svolgimento delle fasi di analisi dei processi aziendali e valutazione dei rischi e GAP ANALYSIS svolta anche in ambito di gestione dei dati informatici, ha portato al contenimento dei potenziali fattori di rischio. Ne discende che ai fini della tutela per la commissione di delitti informatici Risulteranno particolarmente a rischio tutte le attività attuate con il computer. Si indicano a titolo esemplificativo i processi, fasi e attività sensibili nell’ambito delle quali, potenzialmente, potrebbero essere commessi alcuni dei delitti informatici previsti dall’art. 24-bis del Decreto:

- la gestione integrale dei sistemi informativi aziendali, ed in ogni caso, l'attività di installazione manutenzione, programmazione e collegamento in rete dell'hardware aziendale;

- l'attività di creazione, gestione ed aggiornamento del software aziendale;

- la corrispondenza, a mezzo di posta elettronica, con clienti, fornitori, uffici ed enti pubblici;

- la circolazione delle e.mail interne all'azienda;

- i rapporti con i soggetti che prestano il servizio di certificazione elettronica;

- le operazioni di home banking;

- i rapporti con le CCIAA;

- i rapporti con gli enti pubblici, le Autorità ecc..

L'attività del personale coinvolto in tutte queste attività quindi risulta ad essere ad alto rischio di consumazione di reati informatici.

2.1 Gestione delle operazioni "informatiche"

Per le operazioni indicate a titolo esemplificativo e per tutte quelle riguardanti la gestione delle banche dati dei comuni soci, risulta necessario attenersi ai principi specifici di comportamento elencati al paragrafo 1.1 ed a quanto previsto nel sistema di sistema posto in essere per la gestione del regolamento UE 679/2016 relativa alla gestione del rischio informatico che devono individuare almeno le seguenti misure:

- siano definiti formalmente i requisiti di autenticazione ai sistemi per l’accesso ai dati e per l’assegnazione dell’accesso remoto agli stessi da parte di soggetti terzi, quali consulenti e fornitori;

- i codici identificativi (user-id) per l’accesso alle applicazioni ed alla rete siano individuali ed univoci;

- la corretta gestione delle password sia definita da linee guida, comunicate a tutti gli utenti, per la selezione e l’utilizzo della parola chiave;

- siano definiti i criteri e le modalità per la creazione delle password di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili (ad es. lunghezza minima della password, regole di complessità, scadenza);
- gli accessi effettuati dagli utenti, in qualsiasi modalità, ai dati, ai sistemi ed alla rete siano oggetto di verifiche periodiche;

- le applicazioni tengano traccia delle modifiche ai dati compiute dagli utenti;

- siano definiti i criteri e le modalità per l’assegnazione, la modifica e la cancellazione dei profili utente;

- sia predisposta una matrice autorizzativa – applicazioni/profili/richiedente – allineata con i ruoli organizzativi in essere e coerente con i principi di segregazione dei ruoli;

- siano eseguite verifiche periodiche dei profili utente al fine di verificare che siano coerenti con le responsabilità assegnate e coerenti con i principi di segregazione dei ruoli;

- la documentazione riguardante ogni singola attività sia archiviata allo scopo di garantire la completa tracciabilità della stessa.

Relativamente alla gestione delle infrastrutture, le misure da adottare devono prevedere che:

- siano definiti i criteri e le modalità per la gestione dei sistemi hardware che prevedano la compilazione e la manutenzione di un inventario aggiornato dell’hardware in uso presso laSocietà e che regolamentino le responsabilità e le modalità operative in caso di implementazione e/o manutenzione di hardware;

- siano definiti i criteri e le modalità per le attività di back up che prevedano, per ogni applicazione hardware, la frequenza dell’attività, le modalità, il numero di copie ed il periodo di conservazione dei dati;

- siano definiti i criteri e le modalità per la gestione dei sistemi software che prevedano la compilazione e manutenzione di un inventario aggiornato del software in uso presso la società,

- l’utilizzo di software formalmente autorizzato e certificato e l’effettuazione di verifiche periodiche sui software installati e sulle memorie di massa dei sistemi in uso al fine di controllare lapresenza di software proibiti e/o potenzialmente nocivi;

- siano definiti i criteri e le modalità per il *change management* (inteso come aggiornamento o implementazione di nuovi sistemi/servizi tecnologici);

- siano definite le credenziali fisiche di accesso ai siti ove risiedono i sistemi informativi e le infrastrutture IT quali, a titolo esemplificativo, codici di accesso, *token authenticator, pin, badge*, e la tracciabilità degli stessi;

- siano definite dettagliatamente le misure di sicurezza adottate, le modalità di vigilanza e la relativa frequenza, la responsabilità, il processo di reporting delle violazioni/effrazioni dei locali tecnici o delle misure di sicurezza, le contromisure da attivare;

- la documentazione riguardante ogni singola attività sia archiviata allo scopo di garantire la completa tracciabilità della stessa.

2.2. Ipotesi di reato perpetrabili o agevolabili. Principi speciali di comportamento

Nell'espletamento di tutte le operazioni compiute con i mezzi informatici e/o telematici, oltre alle indicazioni di cui al presente Modello, gli amministratori, i dipendenti ed i consulenti (nella misura necessaria alle funzioni svolte) devono conoscere e rispettare;

- le procedure aziendali esistenti, la documentazione e le disposizioni inerenti la struttura gerarchico-funzionale, aziendale ed organizzativa della società ed i compiti attribuiti;

- le norme inerenti i sistemi informativi della società.

- in generale, la normativa applicabile.

In particolare, i responsabili dei Servizi e le funzioni coinvolte sono tenute al rispetto delle norme di comportamento di seguito indicate.

Al personale di AnconAmbiente viene fatto espresso divieto di:

- porre in essere condotte tali da integrare le fattispecie di reato previste dall'art. 24 bis del D.lgs. 231/01;

- di utilizzare postazioni informatiche diverse da quelle aziendali per lo svolgimento della propria attività lavorativa;

- di connettersi alla rete internet o di inviare messaggi di posta elettronica per motivi connessi alla

propria attività di lavoro utilizzando un account diverso da quello fornito dall'Ufficio Sistemi Informativi a ogni dipendente;

- di utilizzare pc portatili e *pendrive* internet diversi da quelli forniti dall'Ufficio Sistemi Informativi, laddove ci si trovi a lavorare in postazioni esterne all'azienda;

- di utilizzare la propria o l'altrui postazione informatica per scopi diversi da quelli conformi allo svolgimento delle mansioni aziendali;

- di scaricare da internet *files* e/o software non strettamente inerenti l'attività lavorativa e senza espressa autorizzazione aziendale;

- di installare programmi di alcun tipo non autorizzati;

- di conoscere, registrare, trattare e divulgare i dati personali di dipendenti o di terzi, se non espressamente autorizzati nelle forme e nei termini del D.lgs. 196/03;

- di porre in essere qualsiasi comportamento che, pur non integrando in concreto alcuna delle ipotesi criminose sopra riportate, possa in astratto diventarlo.

In particolare si rammenta il divieto assoluto di:

- falsificare qualsiasi documento informatico pubblico o privato avente efficacia probatoria;

- introdursi abusivamente in sistemi informatici o telematici protetti da misure di sicurezza ovvero, permanervi, contro la volontà di chi ha diritto ad escluderlo;

-procurare, riprodurre, diffondere, comunicare o consegnare abusivamente codici, parole chiave, o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, o comunque, fornire indicazioni o istruzioni idonee al predetto scopo;

- procurare, produrre, riprodurre, importare, diffondere, comunicare, consegnare o comunque mettere a disposizione di altri, apparecchiature, dispositivi o programmi informatici, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti;

- distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato, Enti Pubblici o ad essi pertinenti, o comunque di pubblica utilità;

- distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi di pubblica utilità ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distruggerli, danneggiarli o renderli, in tutto o in parte, inservibili o ostacolarne gravemente il funzionamento.

2.3 Le ipotesi residuali

Accanto alle ipotesi sopra descritte gli ulteriori rischi a cui la Società può andare incontro, a prescindere dalla loro attualità ed aleatorietà sono collegati a fattispecie penalmente rilevanti precedentemente descritte che hanno però solo una configurabilità teorica, da ricollegarsi essenzialmente alla realtà operativa del momento:

Delitti contro la persona:

- intercettazione, impedimento o interruzione illecita, di comunicazioni informatiche o telematiche (art. 617 c.p.). Il reato si configura allorquando il personale intercetti fraudolentemente, comunicazioni relative ad un sistema informatico o intercorrenti tra più sistemi, ovvero le impedisca o le interrompa;

- installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.).Il reato si configura allorquando il personale o amministratore della società, installi apparecchiature atte ad intercettare, impedire, interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

Delitti contro il patrimonio:

- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.). Il reato si configura allorquando il soggetto che presta servizi di certificazione di firma elettronica violi gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.

E' evidente che per tali fattispecie residuali i livelli di rischio per la Società risultano inesistenti.

2.4 Ipotesi di modalità di possibili commissioni di reato

Per meglio comprendere in cosa possano consistere le modalità di possibili commissioni di reato si ipotizzano le seguenti casistiche:

Accesso abusivo ad un sistema telematico o informativo

Il reato potrebbe verificarsi laddove gli amministratori o il personale dipendente si introduca abusivamente all'interno di un sistema informatico di altra società allo scopo di carpirne segreti aziendali o elenchi di informazioni.

Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Il reato potrebbe verificarsi se gli amministratori o il personale dipendente si procurino numeri seriali di apparecchi cellulari appartenenti ad altri soggetti, poiché attraverso la corrispondente modifica dl codice di un ulteriore apparecchio, è possibile realizzare una illecita connessione alla rete di telefonia mobile che costituisce un sistema telematico protetto.

Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico

A titolo di esempio si menziona il caso in cui ci si procuri un programma informatico utilizzabile al fine di danneggiare il sistema informatico di un terzo.

Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche

Si indica il caso di un dipendente o amministratore che intercetti la corrispondenza via e.mail di altri soggetti.

Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche

A titolo esemplificativo si indica il caso di dipendenti e/o amministratori che installino abusivamente apparecchiature atte ad intercettare comunicazioni relative ad un sistema informatico di un altro soggetto.

Danneggiamento di informazioni, dati e programmi informatici

Potrebbe essere il caso di chi distrugga informazioni o dati informatici di un dipendente sgradito e/o non idoneo allo svolgimento delle mansioni affidategli, alo scopo di precostituire cause di addebito disciplinare.

Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o altro ente pubblico o comunque di pubblica utilità

E' il caso del dipendente che tenti di alterare il sistema informatico dell'Agenzia delle Entrate.

Danneggiamento di sistemi informatici o telematici di pubblica utilità

A titolo di esempio si indica il caso in cui, attraverso l'invio di un messaggio di posta elettronica contenente in allegato un documento affetto da virus, si tenti di rendere inservibile la rete informatica del soggetto terzo.

Frode informatica del soggetto che presta servizi di certificazione di firma eletronica

Si indica il caso del soggetto che istighi chi presta il servizio di certificazione di firma elettronica per la società a violare gli obblighi di legge al fine di conseguire un ingiusto profitto.

Documenti informatici

A titolo di esempio si cita il caso di un soggetto che falsifichi un contratto, formatosi anche attraverso lo scambio di una e.mail nell'interesse o vantaggio della società o proprio.

3 SANZIONI

Nel quadro sinottico che segue vengono prese in considerazione le pene e le multe previste dal Codice Penale correlate con quelle stabilite dall’articolo 24-bis, Dlgs. 8 giugno, n.231, relative alla responsabilità penale di AnconAmbiente in occasione di reati commessi, a suo interesse o vantaggio, dalle Funzioni di rappresentanza o da dipendenti sottoposti all’altrui direzione ovvero per interesse o vantaggio privato.

Si rammenta che il D.lgs. 231/03 all'art. 11 prevede, in relazione ai delitti informatici e trattamento illecito dei dati, sanzioni pecuniarie a carico dell'ente secondo una quantificazione in quote e che *"nella commisurazione della sanzione pecuniaria il giudice determina il numero delle quote tenendo conto della gravità del fatto, del grado della responsabilità dell'ente nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti. L'importo della quota è fissato sulla base delle condizioni economiche e patrimoniali dell'ente allo scopo di assicurare l'efficacia della sanzione."* [2]

E' altresì prevista la possibilità di riduzione della sanzione pecuniaria. L'art. 12 del D.lgs. 231/01 prescrive: *"1. La sanzione pecuniaria è ridotta della metà e non può comunque essere superiore a lire duecento milioni se: a) l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo; b) il danno patrimoniale cagionato è di particolare tenuità. 2. La sanzione è ridotta da un terzo alla metà se, prima della dichiarazione di apertura del dibattimento di primo grado: a) l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso; b) è stato adottato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi. 3. Nel caso in cui concorrono entrambe le condizioni previste dalle lettere del precedente comma, la sanzione è ridotta dalla metà ai due terzi. 4. In ogni caso, la sanzione pecuniaria non può essere inferiore a lire venti milioni.".*

Inoltre in caso di delitto tentato il successivo articolo 26 stabilisce che: "1. Le sanzioni pecuniarie e interdittive sono ridotte da un terzo alla metà in relazione alla commissione, nelle forme del tentativo, dei delitti indicati nel presente capo del decreto. 2. L'ente non risponde quando volontariamente impedisce il compimento dell'azione o la realizzazione dell'evento."

---

[2] **Relazione Ministeriale al Decreto sub punto 5.1:** ...Quanto alle modalità di accertamento delle condizioni economiche e patrimoniali dell'ente, il giudice potrà avvalersi dei bilanci o delle altre scritture comunque idonee a fotografare tali condizioni. In taluni casi, la prova potrà essere conseguita anche tenendo in considerazioni le dimensioni dell'ente e la sua posizione sul mercato. ... il giudice non potrà comunque fare a meno di calarsi, con l'ausilio di consulenti, nella realtà dell'impresa, dove potrà attingere anche le informazioni relative allo stato di solidità economica, finanziaria e patrimoniale dell'ente ... **l'importo di una singola quota va da un minimo di lire cinquecentomila -€ 258,23- ad un massimo di tre milioni -€ 1.549,37-** ... Rispetto all'articolo 133-bis del codice penale che - come si è detto - prevede un aumento della pena pecuniaria fino al triplo o una diminuzione di un terzo, nel paradigma "per quote" il valore di ciascuna quota presenta un rapporto da "uno a sei" (cinquecentomila lire/tre milioni), evidentemente più ampio rispetto al modello penalistico: questa maggiore oscillazione serve proprio a garantire un adeguamento effettivo alla condizioni dell'ente, in considerazione del carattere estremamente variegato della realtà economica dell'impresa nel nostro paese.
Relazione Ministeriale al Decreto sub punto 5.1: ...il giudice determina l'ammontare del numero delle quote sulla scorta dei tradizionali indici di gravità dell'illecito; poi, determina il valore monetario della singola quota tenendo conto delle condizioni economiche dell'ente ... L'intera operazione si risolve nel combinarsi aritmetico di un moltiplicatore fissato dal fatto illecito con un moltiplicando ricavato dalla capacità economica dell'ente. Il tutto avviene nel rigoroso rispetto dell'ammontare minimo e massimo della sanzione pecuniaria fissato dalla delega. Così, si è previsto, nel comma 2 dell'articolo 10, che la sanzione pecuniaria viene applicata per quote non inferiori a cento né superiori a mille.

Reato	COSA PREVEDE Il Codice Penale	COSA PREVEDE IL Dlgs 231/01
Accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.) **Se il fatto è commesso:** **1) Da un pubblico ufficiale o da un incaricato di pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti la funzione o il 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 e´ 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** **Qualora i fatti riguardinosistemi informatici o telematici di interesse militare o relativi all’ordine pubblico o alla sicurezza pubblica o allasanità o alla protezione civile o comunque di interesse pubblico**	Pena della reclusione fino a treanni Pena della reclusione da uno acinque anni Pena della reclusione da uno a cinque anni e da tre ad otto anni	Sanzione pecuniaria da 100 a 500 quote.

Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (art. 615-quater c.p.) *[articolo modificato dalla Legge n. 238/2021]*	Pena della reclusione fino a due anni e della multa fino ad € 5.164,00	Sanzione pecuniaria sino a 300 quote.
Se ricorre taluna delle circostanze elencate dai numeri 1) e 2) quarto comma dell'art. 617 quater	Pena della reclusione da uno a tre anni e della multa da € 5.164 ad €10.329,00.	
Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.) *[articolo modificato dalla Legge n. 238/2021]*	Pena della reclusione fino a due anni e della multa sino ad € 10.329,00	Sanzione pecuniaria sino a 300 quote
Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.) *[articolo modificato dalla Legge n. 238/2021]*	Pena della reclusione da un anno e sei mesi a cinque anni	
Se il fatto è commesso: **1) 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 utilità;** **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**	Pena della reclusione da tre ad otto anni	Sanzione pecuniaria da 100 a 500 quote

Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.) *[articolo modificato dalla Legge n. 238/2021]*	Pena della reclusione da uno a quattro anni	Sanzione pecuniaria da 100 a 500 quote
Nei casi previsti dal quartocomma dell’art. 617 quater	Pena della reclusione da uno a cinque anni	
Danneggiamento di informazioni, dati e programmi informatici (art. 635-*bis* c.p.)	Pena della reclusione da sei mesi a tre anni	Sanzione pecuniaria da 100 a 500 quote
Se commesso con abuso della qualità di operatore disistema	Pena della reclusione da uno a quattro anni	
Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altroente pubblico o comunque dipubblica utilità (art. 635-ter c.p.)	Pena della reclusione da uno a quattro anni	
Se dal fatto deriva la distruzione, il deterioramento,la cancellazione, l’alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici	Pena della reclusione da tre a otto anni	Sanzione pecuniaria da 100 a 500 quote
Se commesso con abuso della qualità di operatore disistema	La Pena è aumentata	
Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.)	Pena della reclusione da uno a cinque anni	Sanzione pecuniaria da 100 a 500 quote
Se commesso con abuso della qualità di operatore disistema	La Pena è aumentata	
Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635- quinquies c.p.)	Pena della reclusione da uno a quattro anni	
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	Pena della reclusione da tre a otto anni	Sanzione pecuniaria da 100 a 500 quote
Se commesso con abuso della qualità di operatore disistema	La Pena è aumentata	

Frode informatica del soggetto che presta servizi dicertificazione di firma elettronica (art. 640 quinquiesc.p.)	Pena della reclusione fino a tre anni e della multa da € 51,00 ad € 1.032,00	Sanzione pecuniaria sino a 400 quote Se commessa nei confronti dello Stato o di altro E.P. sino a 500 quote
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 (art. 491 bis c.p.)		Sanzione pecuniaria sino a 400 quote
Violazione delle norme in materia di Perimetro di sicurezza nazionale cibernetica (art. 1, comma 11, D.L. 21 settembre 2019, n. 105)	Pena della reclusione da uno a tre anni	Sanzione pecuniaria sino a 400 quote

4 AREE AZIENDALI A RISCHIO DI REATO

4.1 Servizi Informativi

L'art. 6, comma 2, lettera a) del D.lgs. 231/01 indica, come uno degli elementi essenziali dei modelli di organizzazione, gestione e controllo previsto, l'individuazione delle cosiddette attività sensibili, ossia di quelle attività aziendali nel cui ambito potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati.

L'analisi dei processi aziendali di AnconAmbiente ha consentito di individuare prioritariamente nel processo di gestione dei sistemi informativi e della sicurezza informatica, le attività nel cui ambito potrebbero astrattamente realizzarsi le fattispecie di reato richiamate dall'art. 24-bis del Decreto, compresi alcuni processi che potrebbero essere considerati strumentali alla commissione dei reati c.d. "presupposto" .

In particolare si tratta della attività di gestione dei profili utente e del processo di autenticazione, gestione dei processi di creazione, trattamento, archiviazione di documenti con valore probatorio, protezione della postazione di lavoro, gestione degli accessi da e verso l'esterno oltre che verso i sistemi informativi degli Enti Locali e delle Pubbliche Amministrazioni in generale, la gestione protezione delle reti e degli output di sistema e dei dispositivi di memorizzazione nonché la sicurezza fisica (dispositivi di rete, cablaggi…), la gestione dei software e delle banche dati protetti da licenza.

Nell’ambito del processo Servizi informativi si riscontrano potenziali rischi di reato nell’attività inerente le diverse fasi sopra descritte.

Rischi di reato

I potenziali comportamenti illeciti sono i seguenti:

- alterare o modificare documenti informatici aventi efficacia probatoria presenti sul sistema informativo aziendale o in quello di terzi - rischio: B
- accedere senza avviso ed in maniera non autorizzata ai documenti esterni/interni - rischio: A
- manomettere o acquisire indebitamente dati che possono produrre un indebito vantaggio alla società e/o proprio- rischio: B
- acquisire, modificare o danneggiare dati telematici-rischio: A
- acquisire, interrompere o danneggiare sistemi informatici o telematici- rischio: B
- interrompere il corretto salvataggio (backup)- rischio: M

MISURE DI PREVENZIONE

Per il contenimento dei rischi evidenziati sono stati introdotti controlli organizzativi previsti dal sistema posto in essere per la gestione del regolamento UE 679/2016 comprendente anche la specifica tecnica di servizio IO1_P01 “sistemi Informativi Aziendali” ed i relativi ordini di servizio per tutto il personale relative “all’accesso e utilizzo delle risorse informatiche e telematiche aziendali”. A questo si associano i principi generali e speciali di comportamento con le relative misure di contenimento individuate nei paragrafi 2.1 e 2.2 che tengono conto dell’implementazione degli standard di controllo che il Responsabile incaricato deve adottare secondo i seguenti principi generali:

a) segregazione dei compiti (separazione delle attività tra chi autorizza, esegue e controlla);
b) tracciabilità (ogni operazione relativa alla propria attività sensibile sia, ove possibile, di adeguatamente registrata);
c) i codici identificativi (user-id) per l’accesso alle applicazioni ed alla rete siano individuali ed univoci;

d) la corretta gestione delle password sia definita da linee guida, comunicate a tutti gli utenti, per la selezione e l’utilizzo della parola chiave;

e) siano definiti i criteri e le modalità per la creazione delle password di accesso alla rete, alle applicazioni, al patrimonio informativo aziendale e ai sistemi critici o sensibili (ad es. lunghezza minima della password, regole di complessità, scadenza proporzionata al tipo di dato trattato);

f) gli accessi effettuati dagli utenti, in qualsiasi modalità, ai dati, ai sistemi ed alla rete siano oggetto di verifiche periodiche se il software utilizzato lo consente;

g) le applicazioni tengano traccia delle modifiche ai dati compiute dagli utenti se il software utilizzato lo consente;

h) siano definiti i criteri e le modalità per l’assegnazione, la modifica e la cancellazione dei profili utente;

i) sia predisposta una matrice autorizzativa – applicazioni/profili/richiedente – allineata con i ruoli organizzativi in essere e coerente con i principi di segregazione dei ruoli;

j) siano eseguite verifiche in caso di modifiche organizzative dei profili utente al fine di valutare che siano coerenti con le responsabilità assegnate e coerenti con i principi di segregazione dei ruoli;

Devono essere, inoltre previste riunioni periodiche annuali con l ’ODV per verificare il rispetto delle procedure e dei sopra descritti standard di controllo

4.1.1 Flussi informativi verso l’Organismo di Vigilanza

Flussi Spot: qualsiasi non conformità rilevata riscontrata in fase di ispezione da parte degli Organi di controllo o da *audit* di certificazione in relazione al presente Modello e/o al Codice Etico.

In particolare, il Responsabile del Trattamento, sia con l’ausilio del Responsabile dei Sistemi Informativi che dell’incaricato interno alla gestione del sistema del trattamento dei dati, dove opportuno, dovrà trasmettere:

- Flussi periodici semestrali in ordine agli aggiornamenti richiesti (procedure, aggiornamenti documentali del sistema GPDR, ecc)
- Dati sull'operato degli amministratori di sistema;
- Report sui log effettuati;
- Registro fornitori (software, hardware) qualificati;
- Lista aggiornata delle licenze d'uso dei programmi informatici;
- Indicazioni sulle garanzie di custodia fisica dei supporti magnetici;
- Informazioni sulla distruzione dei dati sui supporti magnetici da dismettere/riutilizzare

4.2 Tutti i Servizi e le Aree coinvolte

Come già indicato in premessa, il trattamento informatico dei dati è definito con il sistema posto in essere per la gestione del regolamento UE 679/2016 al quale si rimanda per maggior dettaglio.

In particolare, nel “Registro dei Trattamenti”, risultano evidenziati i trattamenti dei dati effettuati dalla società, la distribuzione dei compiti, delle responsabilità e l'elenco degli incaricati al trattamento informatico e telematico dei dati.

Dall'esame del documento risultavano evidenziati i servizi e le aree coinvolte nel trattamento dei dati informatici. La situazione attuale che da allora si è evoluta riflette un coinvolgimento di tutte le aree e servizi aziendali quali ad es.:

- Magazzino
- Ufficio Appalti, Segreteria AA.GG.LL., Protocollo
- Centrale Operativa
- Controllo di Gestione
- Officina
- Gestione Assicurazioni
- Pubblica Illuminazione
- Servizi Cimiteriali e Lampade Votive
- Sistemi Informativi
- Comunicazione Istituzionale
- Ufficio Relazioni con il Pubblico (URP)
- Ragioneria
- Gestione del Personale
- Ufficio Tecnico, Gestione Qualità ed Ambiente
- Servizio Prevenzione e Protezione
- Servizi di Raccolta Rifiuti per i Comuni serviti (anche conto terzi, a chiamata da parte di privati):

E' evidente che oltre alla continua evoluzione organizzativa, i soggetti che accedono ai mezzi informatici seppure non espressamente indicati quali incaricati del trattamento, siano quasi coincidenti con l'intero personale aziendale.

Pertanto nell’ambito di tutti i processi aziendali è riscontrabile un rischio teorico di commissione dei reati ex art. 24-bis D.lgs. 231/01.

Rischi di reato

I potenziali comportamenti illeciti sono i seguenti:

- alterare o modificare documenti informatici aventi efficacia probatoria presenti sul proprio sistema informativo o in quello di terzi - rischio: A
- accedere in maniera non autorizzata a sistemi esterni/interni mediante possesso abusivo di password o mediante software particolare al fine di manomettere o di acquisire indebitamente dati che possono produrre un indebito vantaggio alla società e/o proprio - rischio A
- acquisire, modificare o danneggiare dati telematici - rischio B;
- interrompere o danneggiare sistemi informatici o telematici- rischio B;

MISURE DI PREVENZIONE

Per il contenimento dei rischi evidenziati sono stati introdotti controlli organizzativi previsti dal sistema posto in essere per la gestione del regolamento UE 679/2016 comprendente anche la specifica tecnica di servizio IO1_P01 “sistemi Informativi Aziendali” ed i relativi ordini di servizio per tutto il personale relative “all’accesso e utilizzo delle risorse informatiche e telematiche aziendali”. A questo si associano i principi generali e speciali di comportamento con le relative misure di contenimento individuate nei paragrafi 2.1 e 2.2.

I relativi punti di controllo possono essere individuati e definiti come di seguito elencato:

- Osservanza del Codice Etico;
- Osservanza dei principi generali e speciali di comportamento così come previsti nel presente Modello e nel sistema di gestione del regolamento UE 679/2016;
- Verifica da parte del Responsabile Area aziendale in collaborazione con Responsabile

dei Sistemi informativi o, dove opportuno, con l’incaricato interno della gestione del regolamento UE 679/2016 (supportato eventualmente dal RPD) in ordine a:

- Politica di riservatezza dei dati
- Verifica uso della postazione locale;
- Verifica uso della posta elettronica;
- Verifica corretto utilizzo delle aree ad accesso limitate;
- Verifica corretto utilizzo accessi ad internet, ecc.
- Aggiornamenti periodici dei sistemi operativi;
- Aggiornamento giornaliero del sistema centrale antivirus;
- Sistema hardware firewall;
- Rispetto delle attività formative programmate sulla sicurezza e sul corretto trattamento dei dati informatici

4.2.1 Flussi informativi verso l’Organismo di Vigilanza

Spot: Qualsiasi verbale emesso a seguito di visita ispettiva dagli Organi di Controllo.

- Verbali relativi a danneggiamenti o guasti ai sistemi informatici non giustificabili in relazione ad un normale utilizzo degli stessi;
- La lista aggiornata annuale in merito all'eventuale utilizzo improprio dei servizi internet e di posta elettronica;
- La lista aggiornata sull'eventuale utilizzo improprio delle password per l'accesso alle postazioni informatiche e/o per l'accesso alle home banking e/o per l'accesso ai sistemi informatici di Enti Pubblici;
- L'elenco delle eventuali anomalie riscontrate nell'utilizzo di hardware e/o di software aziendali;
- l'elenco delle eventuali deroghe (autorizzate) alle procedure previste

4.3 Gestione banche dati Enti Pubblici Soci

Le attuali modalità poste in essere per la gestione dei rifiuti o di altri servizi (es. servizi cimiteriali) in risposta all’evoluzione delle normative e/o alle esigenze di servizio (es. raccolta porta a porta, gestione delle segnalazioni utenti, ecc.) ha portato alla necessità di acquisire o accedere ai dati anagrafici delle famiglie dei Comuni Serviti al fine di potere adeguatamente ottemperare al servizio richiesto.

Nei casi previsti, l’accesso alla banca dati è per sola consultazione e finalizzate all’espletamento del servizio. Tale aspetto è regolamentato da opportune convenzioni dove AnconAmbiente è nominata come Responsabile del Trattamento dei Dati e gestito in forma controllata attraverso il sistema di gestione del regolamento UE 679/2016.

In generale, in tale ambito, si rinvengono solo teorici rischi di commissione dei reati informatici ex Dlgs. 231/2001 nelle predette fasi di processo/attività della gestione delle banche dati del predetto EntePubblico.

Il Rischio di commissioni di reato risulta pertanto ininfluente.