# DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

## ai sensi del Codice in materia di protezione dei dati personali art. 34 e Allegato B, regola 19, del D.lgs. 30 giugno 2003, n. 196

# INDICE

# 1. PREMESSA

## 1.1 PRESENTAZIONE

Dal 1° gennaio 2004 è entrato in vigore il D.Lgs. n. 196 del 30 giugno 2003 recante "Codice in materia di protezione dei dati personali" che ha abrogato la legge di riferimento n. 675 del 31 dicembre 1996.

Il Codice, che recepisce numerose pronunce e pareri già formulati dal Garante, nonché la direttiva UE 2000/58 sulla riservatezza nelle comunicazioni elettroniche, contiene importanti innovazioni in materia di informazione giuridica, di notificazioni di atti giudiziari, di dati sui comportamenti debitori.

*In primis*, viene riconosciuto un vero e proprio diritto soggettivo in capo alle persone fisiche alla protezione dei dati personali che le riguardano, andando ben oltre il diritto alla riservatezza sinora tutelato dalla legge n. 675 del 31 dicembre 1996.

Infatti, se la disciplina precedente consentiva all'interessato, a titolo esemplificativo, di conoscere l'ambito di divulgazione dei propri dati personali, ora questi avrà diritto alla comunicazione delle informazioni riguardanti lo scambio di dati ed i rapporti intercorrenti tra i Responsabili e gli Incaricati che effettuano il trattamento.

Resta confermata la necessità del consenso al trattamento dei dati, ma sono previste alcune ipotesi di esonero con riferimento a settori specifici[1].

In secondo luogo, il Codice introduce il "principio di necessità" nel trattamento dei dati, in base al quale l'uso di dati personali e di dati identificativi deve essere ridotto al minimo ed escluso quando le finalità perseguite possano essere realizzate mediante l'utilizzo di dati anonimi.

E' prevista, inoltre, l'emanazione di regolamenti che recepiscono prassi già attuate dagli enti pubblici, specie nell'ambito del settore pubblico, per l'identificazione delle categorie di dati sensibili e giudiziari utilizzati e dei tipi di operazioni di trattamento eseguibili.

Viene poi superata la distinzione del dato personale in "sensibile" e "ordinario" per introdurre nuove e specifiche regole per categorie omogenee di dati personali.

Le misure di sicurezza contro i rischi di distruzione o perdita, intrusione o uso improprio per il trattamento dei dati, con o senza l'ausilio di strumenti elettronici, vengono sviluppate e rafforzate rispetto a quelle previste dalla normativa precedente, come si evince dal Disciplinare Tecnico allegato al Codice. Queste misure configurano il livello minimo di protezione richiesto per evitare eventuali rischi e la prova della loro adozione riveste un'importanza fondamentale nell'ambito del regime della responsabilità civile ai fini dell'esclusione della colpa.
Punto centrale del Disciplinare Tecnico è costituito dal Documento Programmatico sulla Sicurezza ( c.d. "**DPS**") che consiste, in sostanza, in un piano per la sicurezza dei dati, avente data certa, che permette ai titolari del trattamento di provare formalmente l'adeguamento alle misure minime richieste dalla legge.

## 1.2 SCOPO

Il presente elaborato costituisce il DPS previsto dall'art. 34 e dall'allegato B del Codice , da aggiornarsi entro il 31 Marzo di ogni anno.
Tale documento e' stato redatto conformemente alle disposizioni contenute nella "Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS)".

[1] Ex art. 24, ricorre l'esonero per: *a) adempiere ad un obbligo legale; b) per eseguire obblighi contrattuali; c) dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da tutti; d) lo svolgimento di attività economiche; e) la salvaguardia della vita o incolumità fisica di un terzo; f) lo svolgimento delle investigazioni difensive o per la tutela in sede giudiziaria; g) perseguimento di un legittimo interesse del titolare o di un terzo destinatario dei dati; h) i membri di associazioni, enti ed organismi nelle relazioni interne; i) codici di deontologia; l) esclusivi scopi scientifici, statistici, storici .*

Scopo del DPS è quello di descrivere la situazione attuale in cui si trova il sistema interno (attraverso l'analisi dei rischi, della distribuzione delle mansioni, delle *policy* interne, della distribuzione di responsabilità, ecc.) e il percorso scelto per l'adattamento alle disposizioni del Codice.
L'aggiornamento del DPS dovrà essere effettuato dal Titolare del Trattamento dei dati (o da un responsabile, se designato) e dovrà esserne custodita copia presso la sede della azienda, per poter essere consultata in caso di controlli.
Il Titolare dovrà, inoltre, riferire dell'avvenuta adozione o dell'aggiornamento del DPS nella relazione accompagnatoria al bilancio d'esercizio, se dovuta.

Nel presente documento vengono definiti i compiti e le responsabilità in materia di sicurezza del trattamento e in particolare vengono descritti i criteri utilizzati per lo svolgimento delle attività di analisi e di valutazione dei rischi al fine di adottare un piano di interventi per la tutela e la protezione:

a) delle aree e dei locali;

b) dell'integrità dei dati;

c) delle trasmissioni dei dati.

Lo scopo è di elaborare criteri e procedure per il trattamento dei rischi.

I rischi in generale sono imputabili a due fattori caratteristici delle tecnologie dell'informazione:

- l'inaffidabilità: cioè la non garanzia di corretto funzionamento, sia nelle componenti hardware, sia in quelle software;
- l'esposizione alle intrusioni informatiche, ai quali si aggiunge l'imponderabilità dell'errore umano.

In termini più operativi è bene intendere la Sicurezza del Sistema Informativo Automatizzato non solo come «protezione del patrimonio informativo da rilevazione, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali", ma anche come "limitazione degli effetti causati dall'eventuale occorrenza di tali cause".

Inoltre, la sicurezza del Sistema Informativo Automatizzato non dipende solo da aspetti tecnici, ma anche da quelli organizzativi, sociali e legali.

Viene definito sicuro un Sistema Informativo Automatizzato che soddisfi le seguenti proprietà:

• disponibilità: l'informazione e i servizi che il sistema eroga devono essere a disposizione degli utenti del sistema compatibilmente con i livelli di servizio;

• integrità: l'informazione e i servizi erogati possono essere creati, modificati o cancellati solo dalle persone autorizzate a svolgere tale operazione;

• autenticità: garanzia e certificazione della provenienza dei dati;

• confidenzialità o riservatezza: l'informazione del Sistema Informativo può essere fruita solo dalle persone autorizzate a compiere tale operazione.

## 1.3 APPLICABILITA'

Il presente documento si applica a tutte le attività svolte all'interno di Venis S.p.A. (d'ora in poi "Venis") che abbiano riflesso sulle attività di trattamento dei dati personali e sensibili.

## 1.4 TERMINI E DEFINIZIONI

Di seguito vengono riportate alcune definizioni, riprese dal Codice che verranno utilizzate nel presente documento:

a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la

consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

b) "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

c) "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

d) "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

e) "misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

f) "strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

g) "autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

h) "credenziali di autenticazione", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

i) "parola chiave", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

l) "profilo di autorizzazione", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

m) "sistema di autorizzazione", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;

n) "banca dati": qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

o) "dati sensibili": dati idonei a rivelare l'origine razziale od etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico politico o sindacale, nonché i dati personali idonei a rilevare lo stato di salute e la vita sessuale;

p) "dato personale": qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

q) "comunicazione": il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

r) "diffusione": il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

## 1.5 RIFERIMENTI NORMATIVI

1. Decreto legislativo del 30 giugno 2003, n. 196, recante il "Codice per la protezione dei dati personali " (di seguito anche il "Codice")

2.. Legge 18 marzo 2008, n. 48 di ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, firmata a Budapest il 23 novembre 2001.

### 1.6 RIFERIMENTI REGOLAMENTARI

1. Provvedimento del Garante della Privacy del 17 gennaio 2008 sulla "Sicurezza dei dati di traffico telefonico e telematico" e successive modifiche;

2. Provvedimento del Garante per la protezione dei dati personali dal titolo del 27 novembre 2008, recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";

3. Provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008, recante "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali".

## 2. CONSERVAZIONE DEI DATI DI TRAFFICO

Con riferimento al provvedimento del Garante della Privacy del 17 gennaio 2008 sulla "Sicurezza dei dati di traffico telefonico e telematico" e successive modifiche, Venis ha affidato a soggetti distinti rispetto a quella/i a cui e' affidato il trattamento dei dati per la finalità di accertamento e repressione dei reati, l'incarico di svolgere con cadenza annuale, l'attività di controllo interno per verificare costantemente la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati di traffico previste dalle norme vigenti e dal provvedimento del Garante, anche per ciò che riguarda la verifica della particolare selettività degli incaricati legittimati.
I controlli comprendono le verifiche a posteriori, a campione o su eventuale allarme derivante da sistemi di *Alerting* e di *Anomaly Detection*, sulla legittimità e liceità degli accessi ai dati effettuati dagli incaricati, sull'integrità dei dati e delle procedure informatiche adoperate per il loro trattamento, nonché le verifiche periodiche sull'effettiva cancellazione dei dati decorsi i periodi di conservazione.
Venis si impegna a indicare nelle future edizioni del DPS l'esito dell'attività' di controllo effettuata, indicando gli interventi eventualmente necessari per adeguare le misure di sicurezza, e a mettere lo stesso DPS a disposizione del Garante o dell'autorità giudiziaria se richiesto.

## 3. AMMINISTRAZIONE DI SISTEMA

In relazione al provvedimento del Garante per la protezione dei dati personali dal titolo "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008, come modificato dal provvedimento del 25 giugno 2009, Venis intende provvedere a:

- nominare gli Amministratori di Sistema;
- predisporre la lettera di incarico e la lista degli Amministratori di Sistema;
- comunicare a tutto il personale:
  - i contenuti del provvedimento del Garante,
  - l'elenco degli Amministratori di Sistema;
- ·predisporre un sistema di *access log* per gli accessi effettuati dagli Amministratori di Sistema.

L'operato degli Amministratori di Sistema verrà ad essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei Titolari del Trattamento o dei Responsabili, allo scopo di controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

## 4. RIFIUTI DI APPARECCHIATURE ELETTRICHE ED ELETTRONICHE (RAAE) E MISURE DI SICUREZZA DEI DATI PERSONALI

In relazione al Provvedimento del 13 ottobre 2008 del Garante per la protezione dei dati recante "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali"del 13 ottobre 2008, con cui detta Autorità ha prescritto che siano adottate appropriate misure organizzative e tecniche volte a garantire la sicurezza dei dati personali trattati e la loro protezione anche nei confronti di accessi non autorizzati che possano verificarsi in occasione della dismissione di apparati elettrici ed elettronici (artt. 31 ss. del Codice), Venis si impegna ad adottare tali misure e accorgimenti, conferendo l'incarico a terzi tecnicamente qualificati, quali centri di assistenza, produttori e distributori di apparecchiature che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.

## 5. CRIMINI INFORMATICI

Con la Legge 18 marzo 2008, n. 48 recante "Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica firmata a Budapest il 23 novembre 2001 e norme di adeguamento dell'ordinamento interno" sono state introdotte nuove disposizioni regolamentari finalizzate a garantire la sicurezza informatica. In particolare, la legge richiamata ha introdotto alcune modifiche sia al Codice in materia di protezione dei dati personali, che al Decreto Legislativo 8 giugno 2001, n. 231. In tal senso, Venis e' intenzionata a sensibilizzare tutto il personale dipendente, i collaboratori all'uopo nominati, circa le disposizioni prescritte dalla legge di cui sopra, incaricando l'Amministratore di Sistema di adottare ogni e qualsiasi misura, atta a dare attuazione alle prescrizioni di legge.

## 6. RESPONSABILITA'

Il Codice individua una serie di figure preposte all'adozione di misure di sicurezza e alla gestione delle stesse.

In particolare:

- il Titolare del Trattamento è responsabile anche penalmente dell'adozione delle misure di sicurezza;
- il Responsabile del Trattamento è corresponsabile con il Titolare, in base alle istruzioni specifiche ricevute;
- l'Amministratore di Sistema è il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzo;
- il Custode delle parole chiave è il soggetto preposto per iscritto alla custodia delle password o che ha accesso alle informazioni che concernono le stesse;
- l'Incaricato del Trattamento è la persona che effettua i trattamenti dei dati sulla base delle istruzioni scritte del Titolare o, se nominato, del/i Responsabile/i.

### 6.1 RESPONSABILE DEL TRATTAMENTO

Venis, nella qualità di Titolare del Trattamento, ha nominato la dottoressa **Alessandra Poggiani** Direttore Generale Responsabile del Trattamento, la quale attenendosi alle istruzioni impartite è soggetto, anche tramite verifiche periodiche, al potere di vigilanza del Titolare del Trattamento sulla puntuale osservanza delle disposizioni in materia di trattamento dei dati personali e di sicurezza dettate dal Codice e delle istruzioni ricevute dal Titolare stesso.

Si rileva che il Responsabile avvalendosi, ove necessario, di Incaricati del Trattamento, interni o esterni, all'uopo nominati, deve:

- redigere ed aggiornare almeno annualmente e conservare il Documento Programmatico della Sicurezza;
- aggiornare l'elenco dei trattamenti dei dati personali in azienda e garantire il diritto d'accesso come previsto dalle norme sulla privacy;
- individuare, predisporre, verificare, documentare e rendere note le misure di sicurezza (minime e più ampie) necessarie per la protezione dei dati personali;
- tenere ed aggiornare l'elenco degli Amministratori di Sistema, ai sensi del Provvedimento del Garante della protezione dei dati personali del 27 novembre 2008, recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", il quale dovrà essere reso disponibile al Garante, se richiesto:
- verificare, annualmente l'operato dell'Amministratore di Sistema:
- implementare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di Sistema, che assicurino che le registrazioni (*access log*) abbiano le caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste, e comprendano i riferimenti temporali e la descrizione dell'evento che le ha generate, assicurando che siano conservate per un congruo periodo, non inferiore a sei mesi;
- rendere nota in forma scritta ai dipendenti di Venis l'identità dell'Amministratore di Sistema, ove l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori.

## 6.2 AMMINISTRATORE DI SISTEMA

Venis, nella qualità di Titolare del Trattamento, ha nominato i signori :

- Pezuol Antonio - CC Sistemi e Sicurezza Informatica
- Boni Enrico - CC Reti
- Francesco Valente – CC Applicazioni
- Paolo Cotti Cometti - Responsabile Servizi e Sistemi

Amministratori di Sistema, i quali sono chiamati ad ottemperare alle funzioni ad essi attribuite, nei rispetto dei limiti di autorizzazione assegnati.

L'operato dell'Amministratore di Sistema sarà oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del Responsabile del Trattamento, in modo da controllare la rispondenza dello stesso alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previsti dalle norme vigenti.

## 6.3 INCARICATO DEL TRATTAMENTO

Il Responsabile del Trattamento dei dati potrà nominare come Incaricati del Trattamento sia i dipendenti, che i consulenti, agenti e procacciatori di affari di Venis, i quali dovranno operare sotto la diretta autorità del Responsabile del Trattamento stesso, attenendosi alle istruzioni impartite.

## 7. ORGANIGRAMMA AZIENDALE

Venis è un operatore autorizzato per la fornitura di servizi di comunicazione di accesso dati in modalità WISP, il quale si avvale di un'infrastruttura di rete in fibra ottica, abilitata alla trasmissione contemporanea di Voce/Dati ad alta velocità e con alti standard qualitativi. La sede legale e' in San Marco 4934, Palazzo Ziani, Venezia.

L'organigramma aziendale e' configurato come da allegato.

## 8. ELENCO DEI TRATTAMENTI DI DATI PERSONALI (regola 19.1) - ANALISI DEL TRATTAMENTO DEI DATI PERSONALI –

In ottemperanza al Codice, Venis non utilizza dati sensibili o giudiziari nell'ambito del citato trattamento, con la sola esclusione dei dati sensibili e giudiziari dei propri dipendenti o collaboratori e relativi parenti, nonché i dati dei candidati all'assunzione.

Venis tratta altresì i dati dei suoi clienti e gli altri dati non-sensibili necessari all'esecuzione dei contratti di fornitura di servizi di comunicazione elettronica nel rispetto delle misure di sicurezza prescritte.

Comunicazione dei dati

I dati inerenti ai lavoratori e trattati dal titolare allo scopo di adempiere agli obblighi contrattuali e di legge possono essere comunicati a Pubbliche Amministrazioni, Casse di previdenza e assistenza, assicurazioni, istituti di credito, associazioni e rappresentanze sindacali, medici designati dal titolare del trattamento per l'espletamento dei controlli sanitari previsti dalla legge, soggetti incaricati dalla società ad attività legate alla gestione del servizio paghe e contributi e/o elaborazioni dei dati nonché a professionisti o consulenti esterni e a tutti quei soggetti ai quali la comunicazione sia dovuta in base a specifici obblighi di legge e/o contrattuali.

Diffusione dei dati

I dati non sono oggetto di diffusione.

Trasferimento dei dati all'estero

Allo stato attuale, non sono previsti trasferimenti di dati personali di alcun tipo al di fuori del territorio nazionale.

## 9. LA DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA' NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI (regola 19.2)

Sotto sono riportati i nominativi dei responsabili ed incaricati:

| Nome | Funzione | Oggetto Responsabilità | Data incarico |
|---|---|---|---|
| **Paolo Bettio** | **Amm. Unico-Legale rappr.** | ***Titolare del Trattamento dei Dati Personali*** | **Automatico con assunzione carica A.U.** |
| **Alessandra Poggiani** | **Direttore generale** | **Responsabile del Trattamento dei Dati Personali** | **Assegnato per delega Rep. 108005 notaio Candiani** |
| **Marco Bettini** | **Condirettore generale** | **Incaricato del Trattamento dei Dati Personali** | **Lettera del** |

| Nome | Funzione | Oggetto Responsabilità | Data incarico |
|---|---|---|---|
| | | | **15/06/2015** |
| **Gianlivio Chiapatti** | **Responsabile Affari Generali e Sistema Qualità** | **Incaricato del Trattamento dei Dati Personali -** Incaricato del Trattamento di dati Personali e Sensibili per dipendente | **Lettera del 15/03/2017** |
| **Giuseppe Ghezzo** | **Responsabile dell'Unità Acquisti Contratti, Amministrazione e Bilancio** | Incaricato del Trattamento dei Dati Personali – Incaricato del Trattamento di dati Personali e Sensibili per dipendente | **Lettera del 1/10/2014** |
| **Giampietro Santoro** | **Responsabile Risorse Umane, Formazione e Comunicazione** | Incaricato del Trattamento di dati Personali e Sensibili per dipendente | **Lettera del 1/10/2014** |
| **Antonio Pezuol** | **CC Sistemi e Sicurezza Informatica** | **Incaricato del Trattamento dei Dati Personali e dei dati di traffico per finalità di giustizia.** Amministratore di Sistema | **Lettera del 1/10/2014** |
| **Enrico Boni** | **CC Reti** | **Incaricato del Trattamento dei Dati** Amministratore di Sistema | **Lettera del 1/10/2014** |
| **Francesco Valente** | **CC Applicazioni** | **Incaricato del Trattamento dei Dati** Amministratore di Sistema | **Lettera del 15/03/2017** |
| **Paolo Cotti Cometti** | **Responsabile Servizi e Sistemi** | **Incaricato del Trattamento dei Dati** Amministratore di Sistema | **Lettera del 15/03/2017** |
| **Adrian Dragos Trofin** | **Sistemista** | **Custode delle parole chiave** | **Lettera del 1/10/2014** |
| **Gabriella Lazzarini** | **Responsabile Gestione dei Documenti** | **Incaricato del Trattamento dei Dati Personali per finalità di Protocollo Informatico e Gestione Documentale** | **Lettera del 2/10/2015** |
| **Adele Troisi** | **Responsabile Prevenzione della Corruzione** | **Incaricato del Trattamento dei Dati Personali per finalità di Trasparenza e Prevenzione della Corruzione** | **Lettera del 2/10/2015** |

Al fine di garantire l'osservanza delle disposizioni riguardanti il trattamento dei dati, Venis ha preposto al trattamento dei dati personali in qualità di incaricati sia i propri dipendenti che i propri collaboratori.

Per quanto riguarda il trattamento dei dati sensibili sono stati nominati incaricati tutti i dipendenti e collaboratori dell'Ufficio Gestione Risorse Umane.

## 10. IDENTIFICAZIONE DELLE RISORSE DA PROTEGGERE

### 10.1 COMPENDIO

Si procede innanzitutto dalla *Identificazione delle risorse da proteggere*, risorse che in diverso modo operano o comunque svolgono un ruolo significativo nei processi di trattamento dei dati personali. A questo proposito, tramite l'*Analisi dei rischi*, sono state analizzate le minacce e le vulnerabilità a cui tali risorse sono sottoposte, in modo da potere valutare gli elementi che possono insidiare la protezione, l'integrità, la conservazione di ogni singolo dato personale trattato.
Valutati i rischi, si è redatto un *Piano di sicurezza* nel quale si è provveduto a definire l'insieme delle misure fisiche, logiche ed organizzative adottate per tutelare le strutture e le risorse preposte al trattamento dati e quindi ai dati stessi.

Inoltre è stato definito un *Piano di verifica* delle misure adottate tramite il quale si provvederà ad accertare periodicamente la bontà delle misure individuate e ad apportare gli accorgimenti che si riveleranno necessari.
Parallelamente alla stesura del Piano di verifica è stato redatto un *Piano di formazione* tramite il quale si renderanno edotti gli incaricati del trattamento dei rischi e dei modi per prevenire i danni.

Le risorse coinvolte nel trattamento dei dati personali sono state divise in alcune categorie:

**Luoghi fisici.** Sono stati analizzati tutti i luoghi ove fisicamente si svolge il trattamento dei dati o si trovano i sistemi di elaborazione o i luoghi ove si conservano i dati.

**Risorse hardware.** Sono state analizzate le apparecchiature elettroniche che sono coinvolte nelle operazioni di trattamento. Tra queste particolare rilievo hanno: file e db server della rete locale di VENIS S.p.A., ove sono conservati i dati in formato elettronico.

**Risorse dati.** Sono stati analizzati tutti gli archivi contenenti dati personali trattati da VENIS S.p.A., siano essi in formato elettronico che in formato cartaceo.

**Risorse software.** Sono stati analizzati i programmi gestionali mediante i quali vengono effettuati i trattamenti automatizzati e i software anti virus utilizzati per monitorare la presenza di eventuali programmi maliziosi.

## 10.2 LUOGHI FISICI

La sede è a Palazzo Ziani, San Marco 4934, 30122 Venezia.
Il palazzo si compone di 3 piani con 73 locali.
I locali sono a norma per quanto riguarda il D.Lgs. 626/94 e relative modifiche apportate dal D.Lgs. 242/1996, sono dotati di rilevatori presenza fumi e sistema di aerazione adeguato.
Il palazzo ha un ingresso principale, una uscita di sicurezza.
Il Palazzo è sorvegliato da un servizio di Guardie Giurate e da sistemi antifurto.

La sede del Data Center è situata presso il Parco Scientifico e tecnologico Vega, edificio Pleaidi (Via delle Industrie, 27/B-C-D, 30175 Marghera-Venezia).
L'edificio si compone di numero 7 locali tecnici (oltre al locale "bombole" contenente le apparecchiature per lo spegnimento automatico degli incendi), predisposti per ospitare sistemi di elaborazione dati e telecomunicazione / reti e di altri locali destinati ad uso uffici e servizi, ed è in grado di garantire un elevato livello di sicurezza ed affidabilità grazie alla adozione di sistemi dedicati al controllo degli accessi, della sicurezza anti-intrusione e della climatizzazione.
Il Data Center, inoltre, costituisce una forma particolarmente specializzata nei servizi di housing / hosting verso il Comune di Venezia e di altri Clienti (grazie alle infrastrutture tecnologiche approntate, alla assistenza e alla connettività).
Si elencano, di seguito, le specifiche dei locali dedicati alla infrastrutture tecnologiche.

**Impianto di sicurezza e supervisione**: realizzato con sensori a doppia tecnologia (infrarossi e microonde), sensori a contatto, sensori anti-sfondamento, e microfonici.
La gestione del sistema è svolta attraverso un avanzato sistema di supervisione che consente di integrare la componente intrusiva, il controllo dei varchi (bussola, porte) e la componente di videosorveglianza. Il controllo degli accessi si basa su tecnologia RFID crittografata con aggiunta di password utente (PIN) per i varchi a maggior controllo. Il sistema di videosorveglianza,

completamente integrato nel sistema di supervisione, consente l'attivazione di allarmi video con l'uso di tecnologie "motion-detection".
Il sistema permette, inoltre, la concentrazione di allarmi fumo, allagamento, temperatura, segnali provenienti da apparecchiature (condizionatori, UPS, ecc.) o sensori presenti nel sito.

**Impianto di spegnimento incendi:** realizzato con distribuzione centralizzata, gestito automaticamente da un sistema di spegnimento con agente estinguente a gas inerte.

**Impianto di segnalazione allagamento:** è costituito da sensori posizionati sotto al pavimento flottante e collegati al sistema di supervisione allarmi.

**Distribuzione elettrica:** alimentazione proveniente dall'ente fornitore, con continuità di erogazione del servizio garantita dai gruppi di continuità ed anche dal gruppo elettrogeno diesel da 800 kVA.

**Gruppi di continuità**: due gruppi da 300 kVA, ridondati tra di loro, che alimentano armadi di distribuzione distinti.

**Alimentazione elettrica rack sistemi "one unit"**: erogata attraverso doppia alimentazione ridondata con una potenza massima erogabile di 7 kW/230 V oppure 10 kW/ 400 V; tipicamente, in corrispondenza di ogni locazione di armadi, atti ad ospitare sistemi di elaborazione, vengono predisposti numero 4 cavi di alimentazione. La gestione delle alimentazioni elettriche avviene mediante dispositivi di switching (dual power switch).

**Climatizzazione dei locali**: garantito da impianti di condizionamento ridondati ad espansione diretta con gas e temperatura interna impostata a 21 °C (+/- 2 °C). La ridondanza è garantita, oltre che dal doppio circuito interno, anche dal numero di unità termoventilanti posizionate all'interno del locale.

Nella tabella seguente sono elencati i locali tecnici e i dispositivi di protezione implementati.

| ***Id*** | ***Uso*** | ***Dispositivi di Sicurezza*** | ***Note*** |
|---|---|---|---|
| Sala Co-Location | Sala Server principale | Accesso al solo personale autorizzato | |
| Sala Espansione<br>(Sala Partecipate) | Sala Server aziende partecipate | Accesso al solo personale autorizzato | |
| Sala Transport<br>(Sala Reti) | Sala Reti e sistemi di rete | Accesso al solo personale autorizzato | |
| Sala TLC | Sala predisposta per accogliere operatori di telecomunicazioni | Accesso al solo personale autorizzato | |
| Sala Quadri | Sala quadri elettrici, UPS, controlli alimentazione elettrica | Accesso al solo personale autorizzato | |
| Sala Consolle (Collaudo Apparecchiature) | Sala Stampa e collaudo | Accesso al solo personale autorizzato | |
| Sala Housing<br>(Magazzino) | Magazzino | Accesso al solo personale autorizzato | |

Anche al locale Bombole può accedere solo il personale autorizzato.

### 10.3 RISORSE HARDWARE

Nella struttura informatica di VENIS S.p.A. sono presenti, complessivamente nelle due sedi di Palazzo Ziani e di Pleiadi, un centinaio di client; i server sono ospitati nel data center presso l'edificio Pleiadi.

La rete dati è compartimentata e protetta tramite firewall e sistema IPS (Intrusion Prevention System).

La sicurezza delle reti, in particolare di quella del Comune di Venezia, è garantita da distinti sistemi di firewalling:

- Coppia di Appliance Check Point 15400 NGFW a protezione del perimetro e per segmentazione in più segmenti di rete;
- Terminatori VPN basati su Cisco ASA 505.

Le appliance Check Point 15400 sono dotate di 4 porte 10 GbE direttamente connesse ai core switch del DC. La compartimentazione in segmenti di rete viene realizzata attraverso VLAN 802.1q.
La compartimentazione in segmenti di rete prevede le seguenti zone:

- **portale** (Portale dei servizi egov);
- **dmz-tcaps** (time capsule su Internet);
- **spc-infranet** (accesso internet SPC);
- **dmz-spcinfranet** (dmz server che escono su internet via SPC);
- **srv-icpsm** (server centro maree);
- **veritas** (accesso a rete Veritas);
- **inside** (rete interna comunale);
- **actv** (accesso a rete ACTV);
- **casino** (accesso a rete Casinò);
- **vds** (accesso a rete videosorveglianza);
- **lan-wirex** (server wirex);
- **mgmt-wirex** (management wirex);
- **mgmt-tropos** (management rete wifi);
- **cittadella** (accesso rete cittadella della giustizia);
- **ames** (accesso rete Ames);
- **dmz** (dmz Venis/Comune);
- **dmz-wirex** (dmz clickandplay);
- **dmz-pub** (dmz proxy nginx);
- **dmz-icpsm** (dmz server centro maree);
- **dmz-veritas** (dmz server veritas);
- **engsun** (dmz eGrammata/Global);
- **str** (segmento servizi STR);
- **manip-grt** (accesso rete di management pop);
- **outside** (internet);
- **manip-mgmt** (accesso rete di management cpe);
- **manip-mgmt-venis** (accesso rete di management lan);

- **dukenet** (segmento servizi Dukenet);
- ascotdb (segmento DB AscotWEB);
- **biblionat** (accesso rete biblioteche content filtering).

I sistemi di firewall condividono i seguenti segmenti di rete:

- Rete **dmz**;
- rete **Internet**;
- rete **interna**.

E' presente, inoltre, un firewall PIX 506E dedicato alla connettività VPN verso rete pubblica.

### 10.3.1 Zona Internet

Il firewall CheckPoint Series 15000 insiste sulla rete di accesso Internet con peering BGP a 2 x 600 Mbps (allo scopo di ottenere lo status di AS – Autonomous System) ed ha indirizzo 94.247.8.5/24.
Il segmento viene utilizzato per pubblicazione di contenuti ed accesso ai servizi Internet.

### 10.3.2 Zona Internet SPC

Il firewall ha i seguenti indirizzi: 89.96.56.34/29
Il segmento viene utilizzato per pubblicare e raggiungere servizi delle pubbliche amministrazioni che sono disponibili solo sulla rete SPC (Sistema Pubblico di Connettività), separata da Internet.

### 10.3.3 Zona interna

Il firewall ha i seguenti indirizzi: 172.22.10.178/24

In questa zona insiste tutta la MAN MPLS in fibra ottica del Comune di Venezia con tutti i client ivi presenti, i server e i sistemi, lo storage centralizzato del Comune di Venezia, gestiti ed implementati da Venis.

### 10.3.4 Zona Comunicazione globale

Il firewall ha indirizzo 172.21.10.182/24. In questa zona sono presenti i server per l'insieme di applicazioni denominato "Comunicazione globale", che include le applicazioni relative al Protocollo e Delibere, Sportello unico edilizia residenziale (SUER), Sportello unico attività produttive (SUAP), Notifiche messi.

### 10.3.5 Zona DMZ

Il firewall ha i seguenti indirizzi: 172.24.10.182/24

In questa zona è presente il web server istituzionale ed una batteria di altri server web, alcuni dei quali front end per server interni.

### 10.3.6 Zona DMZ proxy

Il firewall ha i seguenti indirizzi: 172.24.12.1/24

In questa zona è presente la batteria di server reverse proxy Nginx utilizzata per la pubblicazione di numerosi servizi offerti dal Comune di Venezia, da Venis e da altri clienti. I reverse proxy si occupano anche di terminare in modo efficace e centralizzato le connessioni TLS. Tali sistemi risiedono su un segmento dedicato in modo da limitare e assicurare il massimo controllo sia sui flussi di traffico originati sulla rete pubblica che su quelli interni.

### 10.3.7 Zona DMZ SPC

Il firewall ha i seguenti indirizzi: 172.24.14.65/28
In questa zona sono presenti sistemi che hanno necessità di essere pubblicati sulla rete internet nazionale SPC o che utilizzano servizi disponibili solo su questa rete.

### 10.3.8 Zona DMZ Veritas

Il firewall ha i seguenti indirizzi: 172.24.14.1/26
In questa zona sono presenti sistemi di Veritas che vengono pubblicati sulla rete internet.

### 10.3.9 Zona portale

Il firewall ha indirizzo 172.21.12.182/24. In questa zona sono presenti i server relativi alle applicazioni del portale.

### 10.3.10 Zona STR

Il firewall ha indirizzo 172.21.13.182/24. In questa zona è presente il server dedicato alla applicazione gestionale destinata all'Edilizia Sportiva del Comune di Venezia. La necessità di risiedere in un segmento diverso dalla rete Interna è dovuta al fatto che tale applicazione, basata su Terminal Services Microsoft, viene utilizzata anche da aziende esterne connesse tramite VPN su rete pubblica.

### 10.3.11 Zona DukeNet

Il firewall ha indirizzo 172.21.14.182/24. In questa zona è presente il server dedicato al database della applicazione gestionale DukeNet (Contabilità LLPP, utilizzata, in prevalenza, dalle strutture museali comunali). La necessità di risiedere in un segmento diverso dalla rete Interna è dovuta al fatto che la manutenzione del database e dell'applicativo, viene effettuata dall'azienda fornitrice (888 Software Products Srl) tramite connessione VPN rete pubblica.

### 10.3.12 Zona AscotDB

Il firewall ha indirizzo 172.21.20.182/24. In questa zona sono presenti i server (database e application) dedicati alle applicazioni legacy del Comune di Venezia (AscotWeb SSDD, AscotWeb Contabilità, AscotWeb Personale-Stipendi, ecc.). Tali sistemi risiedono in un segmento diverso dalla rete Interna per motivi di sicurezza (architettura su più livelli).

### 10.3.13 Risorse dedicate ai servizi di connettività WiFi cittadina - VeniceConnected

La connettività Internet dedicata ai servizi WiFi (Hot-Spot distribuiti sul territorio comunale) prevede l'impiego di sistemi di autenticazione e Captive Portal (gestione di landing pages, walled-garden e accessibilità alla rete), basati su pfSense. Tutti i dispositivi sono installati presso il DC.

La sicurezza nel colloquio tra la rete privata dedicata al WiFi e alcuni segmenti di rete (DMZ, ad esempio) viene garantita dai sistemi di firewalling.
Gli HotSpot, distribuiti sul territorio comunale, sono connessi al DC mediante rilegamenti diretti alla rete a larga banda comunale (MAN MPLS in fibra ottica), oppure, tipicamente nel caso di apparati indoor, attraverso le reti LAN delle sedi comunali o di altri clienti all'interno delle quali è stato deciso di fornire il servizio di navigazione pubblico.
Nel caso di alcune sedi non collegate alla MAN il servizio è fornito utilizzando connessioni VPN OpenVPN terminate su un server ospitato nel datacenter.

### 10.3.14 Zona di interconnessione con la rete di navigazione aperta al pubblico del sistema bibliotecario comunale

Per motivi di tutela dei minori, tutto il traffico diretto verso internet da client della rete di navigazione aperta al pubblico del sistema bibliotecario comunale viene processato da un'appliance Cisco S170 che effettua content filtering e analisi di sicurezza. La rete in questione è isolata per motivi di sicurezza da tutto il resto della rete comunale e raggiungibile solo attraverso il firewall da server e client specifici per motivi di gestione e amministrativi. L'indirizzo del firewall in questa zona è 10.80.0.5/24.

### 10.3.15 Servizi dedicati all'istituzione ICPSM

I server dell'istituzione ICPSM sono ospitati su due segmenti di rete:

- La zona DMZ ICPSM è dedicata ai servizi che l'istituzione pubblica sulla rete internet. L'indirizzo del firewall è 172.24.13.1/24;
- la zona Server ICPSM è dedicata ai server di backend e ai server ad uso interno dell'istituzione. L'indirizzo del firewall è 172.23.160.129/25.

### 10.3.16 Servizi dedicati a www.clickandplay.it (Casinò di Venezia)

I server utilizzati per il gioco on-line sono ospitati in tre segmenti di rete:

- La zona DMZ Wirex è dedicata ai servizi che vengono pubblicati sulla rete internet. L'indirizzo del firewall è 172.24.20.1/24;
- la zona LAN Wirex è dedicata ai server di backend e a server ad uso interno. La zona ospita anche i terminatori VPN dedicati al colloquio con AAMS e Lottomatica. L'indirizzo del firewall è 172.19.10.1/24;
- la zona MGMT Wirex è dedicata alle interfacce di management di appliance e server. L'indirizzo del firewall è 172.19.12.1/24.

Ciascuna zona è isolata dalle altre e dalle altre zone configurate sul firewall, solo i flussi esplicitamente autorizzati sono consentiti.

### 10.3.17 Servizi di interconnessione con le reti dei clienti

Il firewall è utilizzato per le comunicazioni tra le reti dei clienti e la rete comunale; per questo motivo sono presenti alcune zone di interconnessione, ciascuna dedicata a un singolo cliente:

- Zona di interconnessione Ames: il firewall ha indirizzo 192.168.0.89/24;
- zona di interconnessione AVM: il firewall ha indirizzo 10.110.1.5/24;

- zona di interconnessione Veritas: il firewall ha indirizzo 192.168.174.5/24;
- zona di interconnessione Casinò di Venezia: il firewall ha indirizzo 192.168.42.5/24.

Le configurazioni attive consentono la pubblicazione sulle reti dei clienti di servizi offerti dal Comune di Venezia e da Venis, e viceversa, e consentono a client specifici presenti sulle reti dei clienti e del Comune di Venezia/Venis di accedere a questi servizi.

### 10.3.18 Servizi di videosorveglianza

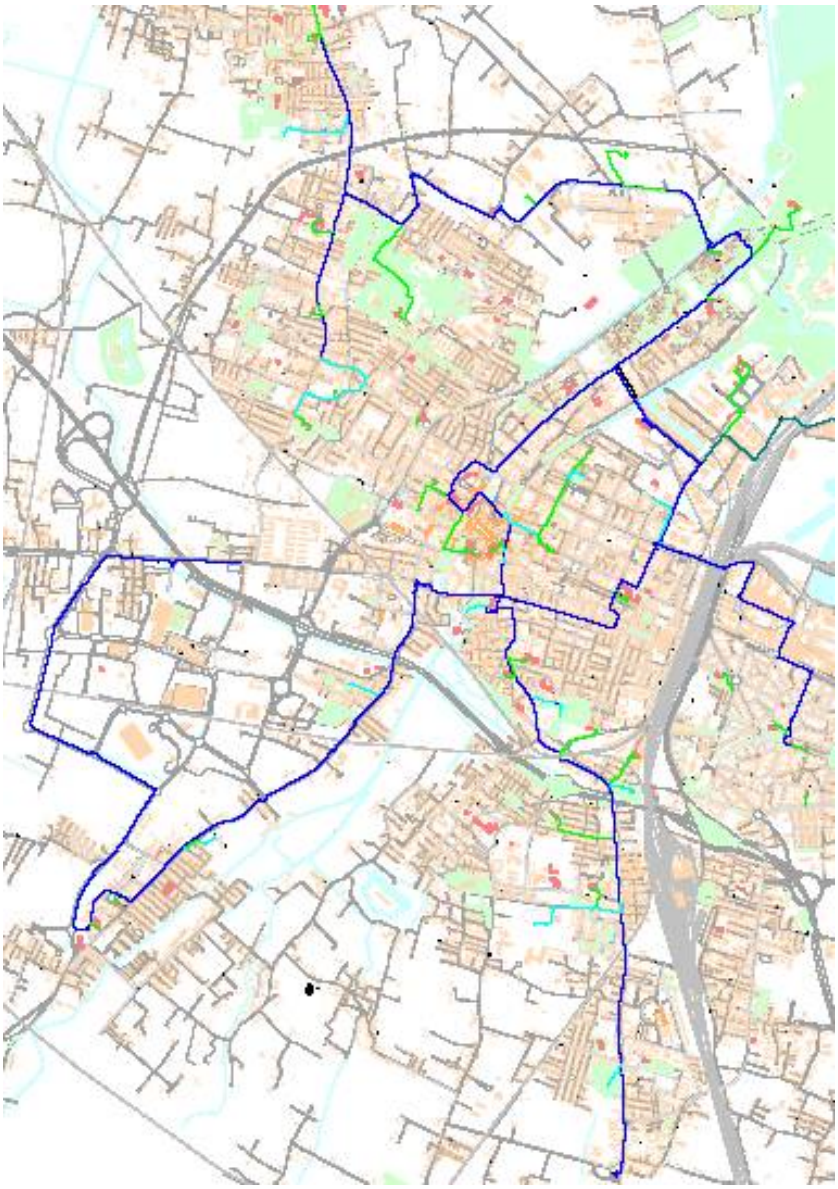
Il firewall è utilizzato per controllare gli accessi alla rete che ospita tutti gli apparati di videosorveglianza gestiti da Venis per conto del Comune di Venezia (telecamere distribuite sul territorio, server di registrazione e gestione, etc.). La comunicazione tra le reti interne e la rete di videosorveglianza viene effettuata utilizzando una zona di interscambio, su cui il firewall ha indirizzo 10.50.101.5/24. Solo i flussi specificamente autorizzati sono consentiti.

### 10.3.19 Servizi di accesso alle reti di gestione degli apparati della MAN e delle LAN

Il firewall è utilizzato per controllare gli accessi alle interfacce di gestione degli apparati attivi della MAN in fibra ottica del Comune di Venezia e alle LAN di alcune sedi, che, per la loro importanza o dimensione, hanno VLAN dedicate alla gestione degli apparati:

- Zona di accesso alla rete di gestione GRT: la zona consente di raggiungere gli indirizzi di management dei router MPLS della MAN. L'indirizzo del firewall è 172.27.2.1/29;
- zona di accesso alla rete di gestione delle CPE: la zona consente di raggiungere gli indirizzi di management delle CPE installate presso tutte le sedi collegate alla MAN. L'indirizzo del firewall è 172.27.128.129/29;
- zona di accesso alla rete di gestione degli apparati LAN: la zona consente di raggiungere gli indirizzi di management degli apparati di rete installati presso alcune delle principali sedi collegate alla MAN. L'indirizzo del firewall è 172.28.128.129/29.

*Rete a larga banda comunale: Dorsali e rilegamenti Centro Storico*



*Rete a larga banda comunale: Dorsali e rilegamenti Terraferma*


***Rete a larga banda comunale: Dorsali e rilegamenti Hiperlan/wireless Isole***

## 10.4 RISORSE DATI

Le banche dati trattate dalla società sono principalmente in formato elettronico. In formato cartaceo vi sono pochi dati relativi al personale interno.

### 10.4.1 Archivi cartacei

Nella sede di Venezia, Palazzo Ziani, viene effettuata la Gestione del Personale, ove dislocati gli archivi cartacei del personale; questi dati sono custoditi in armadi muniti di serratura. Gli incaricati accedono ai soli dati personali la cui conoscenza è strettamente necessaria per adempiere ai compiti loro assegnati (riferimento art. 9 comma a) D.P.R. 318/99).

### 10.4.2 Archivi elettronici

Gli archivi elettronici sono custoditi nei server ospitati all'interno della sala Co-Location (sala server) del Data Center - Pleiadi. Gli accessi ai vari applicativi avviene previa autenticazione.
Ogni utente ha una sua password di accesso al sistema. Le password vengono scelte dai singoli utenti e consegnate al "custode delle password" tramite apposito modulo. Vengono poi custodite nella cassaforte sita nell'edificio Pleiadi.
VENIS S.p.A. custodisce, nella sua sede del Data Center, i vari server dei clienti. Bisogna evidenziare tra questi solo quelli che presentano dati sensibili ai sensi della legge.

| ***Nome Server*** | ***Database ospitato*** |
|---|---|
| casatest | database @ter casa di test |
| ikdb | database applicazioni infokeeper |
| db2-gatti | database server nodo 2 egrammata/epraxi/global atti |
| Db-gatti-test | database server di test egrammata/epraxi/global atti |
| sql-server | Server di test tributi |
| lxcasa | db oracle casa |
| db1-gatti | database server nodo 2 egrammata/epraxi/global atti |
| labikdb | db infokeeper e casino test |
| ascotdb11g3 | db server personale, ici, rap e contabilità enti |
| ascotdb11gtest | db server di test per ascotweb contabilità, personale, rap, anagrafe, ici |
| ascotdb11g1 | db server rac anagrafe e contabilità |
| ascotdb11g2 | db server rac anagrafe e contabilità |

*Elenco server e DBMS sottoposti al logging degli accessi effettuati con diritti amministrativi*

(in ottemperanza a: Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 - G.U. n. 300 del 24 dicembre 2008; Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento - 25 giugno 2009 - G.U. n. 149 del 30 giugno 2009)
I dati contenuti in questi server vengono amministrati solo per elaborazioni periodiche di manutenzione:

| ***Nome server*** | ***Instanza*** | ***Tipo Database*** | ***SO*** |
|---|---|---|---|

| | | | |
|---|---|---|---|
| casatest | TEST, TER_T | Oracle | Linux RHEL |
| ikdb | IKDB | Oracle | Linux RHEL |
| db2-gatti | GATTI2 | Oracle | Linux RHEL |
| Db-gatti-test | GTEST | Oracle | Linux RHEL |
| sql-server | MSSQL | SqlServer | Windows Server |
| lxcasa | A.TER | Oracle | Linux RHEL |
| db1-gatti | GATTI1 | Oracle | Linux RHEL |
| labikdb | LABIK | Oracle | Linux RHEL |
| ascotdb11g3 | PERS11G, DICI11G | Oracle | Linux RHEL |
| ascotdb11gtest | CONT11G, CANAL11G, ANAG11G, VCONN, DICI11G, ANAG10, PERS11G | Oracle | Linux RHEL |
| ascotdb11g1 | ANAG1, CONT1 | Oracle | Linux RHEL |
| ascotdb11g2 | ANAG2, CONT2 | Oracle | |

## 10.5 RISORSE SOFTWARE

Le risorse software utilizzate per il protezione dei dati sono:

- Antivirus;
- Firewall;
- Antispam.

### 10.5.1 Antivirus/end-point protection

Il prodotto utilizzato come antivirus è MacAfee.

L'aggiornamento dell'antivirus e delle relative policy avviene in modo automatico tramite console centralizzata.

### 10.5.2 Firewall

La rete dati è compartimentata e protetta tramite firewall e sistema IPS (Intrusion Prevention System).

La sicurezza delle reti, in particolare di quella del Comune di Venezia, è garantita da distinti sistemi di firewalling:

- Coppia di Appliance Check Point 15400 NGFW a protezione del perimetro e per segmentazione in più segmenti di rete;
- Terminatori VPN basati su Cisco ASA 505.

Le appliance Check Point 15400 sono dotate di 4 porte 10 GbE direttamente connesse ai core switch del DC. La compartimentazione in segmenti di rete viene realizzata attraverso VLAN 802.1q.

### 10.5.3 Antispam e antivirus posta

I servizi di posta prevedono due protezioni software contro la messaggistica indesiderata (spam). La prima interna alla piattaforma Zimbra. La seconda, invece, viene demandata ad due virtual appliance prodotte da Symantec e LibraEsva

## 11. ANALISI DEI RISCHI

Identificate le risorse coinvolte a vario titolo nelle operazioni viene operata l'Analisi dei rischi.
Per Analisi dei rischi si intende lo studio delle minacce e delle vulnerabilità a cui sono soggette le risorse.
Opereremo l'Analisi in maniera distinta sulle categorie di beni individuati precedentemente.

### 11.1 ANALISI DEI RISCHI SUI LOCALI

Dalla descrizione riportata al paragrafo 10 si può dire che l'esposizione al rischio di intrusione, incendio e allagamento dei locali di VENIS S.p.A. è poco significativa e non richiede l'aggiunta di particolari misure di sicurezza.

### 11.2 ANALISI DEI RISCHI SULLE RISORSE HARDWARE

I rischi sulle risorse hardware sono pochi. Infatti è remoto il rischio di utilizzo non autorizzato dell'hardware in quanto alle risorse accedono solo le persone autorizzate. Questo vale anche per il rischio di manomissione e di sabotaggio.
La manutenzione delle apparecchiature viene eseguita da tecnici di fiducia.
L'hardware acquistato è di qualità e storicamente non ha mai dato problemi rilevanti.
La soglia di rischio connessa all'improvvisa mancanza di elettricità è bassa; infatti i locali tecnici destinati ai sistemi di elaborazione prevedono l'impiego di UPS e gruppo elettrogeno (che impediscono l'improvvisa assenza di corrente elettrica e i danni conseguenti).

### 11.3 ANALISI DEI RISCHI DELLE RISORSE DATI

Per gli archivi elettronici si è effettuata una analisi del rischio basandosi su alcuni punti:

- Accesso non autorizzato: l'accesso alle risorse dati in formato elettronico è protetto da password. La soglia di rischio individuata è bassa.
- Cancellazione non autorizzata, manomissione: l'accesso alle risorse dati in formato elettronico avviene solo tramite elaboratori protetti da password. Solo il personale autorizzato può accedere ai vari database. La soglia di rischio individuata è media.
- Perdita dei dati: sono effettuate giornaliere copie di backup e le cassette di copia vengono conservate in cassaforte ignifuga. E' in fase di formalizzazione un contratto per il servizio di conservazione nastri presso locali esterni al Data Center di VENIS S.p.A.. La soglia di rischio individuata è bassa.
- Incapacità di ripristinare le copie di backup: controlli periodici effettuati sui supporti di backup hanno sempre fornito esiti positivi. Anche in questo caso la soglia di rischio individuata è bassa.

Per gli archivi cartacei il rischio di accesso non autorizzato è basso. Gli unici dati sensibili trovati nei locali sono custoditi in un armadio munito di serratura.

## 11.4 ANALISI DEI RISCHI DELLE RISORSE SOFTWARE

Il server per l'antivirus e il server del firewall sono custoditi nella sala server.
Periodiche verifiche delle regole del firewall e la bontà del prodotto antivirus scelto hanno permesso di individuare una soglia di rischio bassa per queste risorse.

## 12. DEFINIZIONE ED ATTUAZIONE DELLA POLITICA DI SICUREZZA

Al fine di assicurare l'integrità dei dati trattati ed impedirne la comunicazione e/o diffusione non autorizzata, VENIS S.p.A. ha elaborato una precisa Politica di sicurezza basata sull'adozione di misure di tipo fisico, logico ed organizzativo. Tali misure hanno il compito di garantire sia i minimi requisiti di sicurezza contemplati dal Decreto Legislativo 196/2003, sia un livello idoneo di sicurezza relativamente alle tipologie dei dati trattati, alle modalità di trattamento ed agli strumenti utilizzati.

## 12.1 MISURE FISICHE

| *Descrizione misure* | *Note ed indicazioni per la corretta applicazione* |
|---|---|
| **Custodia degli archivi cartacei in armadi muniti di serratura** | Tutti i documenti cartacei contenenti dati personali sensibili sono conservati in armadietti o contenitori dotati di serratura. Gli incaricati potranno prelevare i documenti necessari per il trattamento per il tempo necessario a tale operazione dopo di che avranno il compito di riporli nei luoghi preposti alla loro conservazione. Sarà compito dell'incaricato che preleva i documenti garantire che questi ultimi siano rinchiusi, sotto chiave, in un cassetto della propria scrivania nel periodo di temporanea assenza dal posto di lavoro. |
| **Custodia dei supporti magnetici** | I supporti magnetici utilizzati per l'attività di backup sono conservati in una cassaforte presso un locale esterno alla sede. |
| **Dispositivi antincendio** | I locali della sede sono dotati di estintori per la soppressione di focolai di incendio (I locali sono conformi alla normativa sulla sicurezza dei luoghi di lavoro) e in ogni stanza di palazzo Ziani è presente un sensore di fumo. La stessa cosa avviene per gli uffici delle Pleiadi mentre il data center delle Pleiadi è dotato di sistema di rilevazione fumi e spegnimento automatico degli incendi. |
| **Continuità dell'alimentazione elettrica** | I server sono collegati ad un doppio gruppo di continuità che garantisce una stabilizzazione dell'energia elettrica erogata. Tale gruppo di continuità, ed il gruppo elettrogeno che eventualmente interviene successivamente, garantisce il corretto funzionamento delle macchine assicurando un'autonomia di parecchie ore. |
| **Verifica della leggibilità dei supporti di backup** | Periodicamente i supporti e le procedure di backup sono testati al fine di verificare l'integrità dei dati registrati. |

## 12.2 MISURE LOGICHE

| *Descrizione misure* | *Note ed indicazioni per la corretta applicazione* |
|---|---|
| **Identificazione degli incaricati preposti alle attività di trattamento** | Sono stati individuati e nominati gli incaricati preposti al trattamento.<br>Agli incaricati vengono indicate le norme operative e di sicurezza a cui attenersi. |
| **Indicazione dei codici identificativi e delle parole chiave agli incaricati.** | Gli incaricati sono stati contraddistinti da codici identificativi univoci (USER ID) che neppure in futuro potranno essere associati ad altre persone. Gli incaricati depositano le loro parole chiave al custode delle password:<br>USER ID e parola chiave per accedere alle risorse di rete.<br>Nel caso l'incaricato voglia cambiare la propria parola chiave, la procedura prevede la consegna di quest'ultima nell'apposito modulo al custode delle password, che provvederà a depositarla in cassaforte. |
| **Indicazione del custode delle password** | È stato individuato e nominato il "custode delle password" a cui spetta la Custodia in un luogo sicuro (cassaforte), delle password a lui affidate dagli incaricati. |
| **Nomina a ruolo del responsabile del trattamento** | È stato nominato, il responsabile per il trattamento dei dati personali. |
| **Predisposizione ed aggiornamento degli antivirus** | Gli elaboratori sono stati protetti mediante il software antivirus descritto nel paragrafo 10.5.1. Il sistema di scansione e gestione è centralizzato e le firme dei virus sono segnalate tramite una e-mail di avviso. |

## 12.3 MISURE ORGANIZZATIVE

| *Descrizione misure* | *Note ed indicazioni per la corretta applicazione* |
|---|---|
| **Analisi dei Rischi e Documento Programmatico Per la Sicurezza** | Sulla base dell'analisi dei rischi è stato redatto il presente documento programmatico per la sicurezza (DPPS). Questo documento sarà divulgato a tutte le funzioni della società. |
| **Piano di verifica delle misure adottate** | È stato stabilito un piano di verifica delle misure adottate. Tale piano è illustrato nel presente DPPS al capitolo 13. |
| **Piano di formazione degli incaricati** | È stato predisposto un Piano di formazione degli incaricati. Tale piano è illustrato nel presente DPPS al capitolo 14. |
| **Dotazione di dispositivi anti intrusione** | I locali sono protetti mediante un sistema di antintrusione e/o di sorveglianza di Guardie Giurate 24 ore su 24. |
| **Custodia di documenti cartacei** | Tutti i documenti cartacei contenenti dati personali sensibili, tranne per i periodi strettamente necessari alle operazioni di trattamento, sono custoditi in armadi dotati di serratura. |

### Piano di verifica

| *Cosa Verificare* | *Chi deve verificare* | *Quando effettuare le verifiche* |
|---|---|---|
| Aggiornamento antivirus | Amministratore di sistema | Almeno ogni 6 mesi |
| Aggiornamento firewall | Amministratore di sistema | Almeno ogni 6 mesi |
| Accesso fisico ai locali dove si svolge il trattamento | Amministratore di sistema | Almeno ogni 6 mesi |
| Corretto uso delle password | Amministratore di sistema | Almeno ogni 6 mesi |
| Disattivare i codici d'accesso e relativa password che non sono utilizzati per più di sei mesi | Amministratore di sistema | Almeno ogni 6 mesi |
| La policy di backup | Amministratore di sistema | Almeno ogni 6 mesi |
| La distruzione dei supporti magnetici che non possono più essere utilizzati per il backup | Amministratore di sistema | Almeno ogni 3 mesi |
| La conservazione dei documenti cartacei | Responsabile | Almeno ogni 6 mesi |

| | | |
|---|---|---|
| Il livello di formazione degli incaricati | Titolare | Almeno una volta l'anno |

## 12.4 ANALISI DEI RISCHI CHE INCOMBONO SUI DATI (regola 19.3)

Nella tabella che segue sono individuati i principali eventi potenzialmente dannosi per la sicurezza dei dati, le possibili conseguenze, il livello di gravità e le misure previste per contrastare l'evento dannoso.

**Legenda:**
A= Gravità Alta
M = Gravità Media
B = Gravità Bassa

| *Rischi* | *Descrizione dell'impatto sulla sicurezza (gravità: alta/media/bassa)* | | *Misure d'azione* |
|---|---|---|---|
| Comportamenti degli operatori | Sottrazione di credenziali di autenticazione | Accesso a dati personali non consentito (bassa) | Cambio periodico delle credenziali |
| | Carenza di consapevolezza, disattenzione o incuria | Accesso a dati personali non consentito (bassa) | Cambio periodico delle credenziali |
| | Comportamenti sleali o fraudolenti | Accesso, cancellazione, alterazione di dati personali non consentito (medio) | Cambio periodico delle credenziali; assegnazione di diversi livelli di autorizzazione |
| | Errore materiale | Cancellazione, alterazione di dati personali non consentito (medio) | Assegnazione di diversi livelli di autorizzazione; uso di procedure di backup e ripristino dati |
| | Alterazione/ danneggiamento accidentale o doloso del sistema, dei programmi, dei dati | Cancellazione, alterazione di dati personali non consentito (medio) | Assegnazione di diversi livelli di autorizzazione; uso di procedure di backup e ripristino dati. |
| | Diffusione/ comunicazione accidentale o dolosa | Diffusione/comunicazione di dati personali in modo incontrollato (basso) | Adozione di sistemi antivirus e antispam; assegnazione di diversi livelli di autorizzazione |
| Eventi relativi agli strumenti | Azione di virus informatici o di programmi suscettibili di recare danno | Accesso, alterazione, distruzione, comunicazione, diffusione di dati (basso) | Uso ed aggiornamento costante di programmi antivirus, e patches dei sistemi operativi. Uso di sistemi di analisi delle vulnerabilità. Uso di procedure di backup e ripristino dati. |
| | Spamming o altre tecniche di sabotaggio | Invio da account inconsapevoli di email verso utenti terzi, potenzialmente anche con dati personali (basso) | Uso ed aggiornamento costante di programmi antispam e patches dei sistemi operativi. |
| | Malfunzionamento, indisponibilità o degrado degli strumenti | Eventuale accesso, alterazione, distruzione di dati (basso) | Uso di sistemi di analisi delle vulnerabilità. Uso di procedure di back-up e ripristino dei dati; uso di banche dati in mirroring |
| | Accessi esterni non autorizzati | Accesso a dati da parte di terzi non autorizzati (basso) | L'accesso alla banche dati avviene in modalità VPN o in modalità via web tramite implementazione del protocollo SSL. Uso di diversi livelli di autorizzazione. Uso di sistema di log delle attività. Uso di sistemi di sicurezza perimetrali (firewall). |
| | Intercettazione di informazioni in rete e intrusioni dall'esterno | Accesso a dati da parte di terzi non autorizzati (medio) | Uso di sistemi di sicurezza perimetrali (firewall). Uso di sistemi di log delle attività. |
| | Danneggiamento risorse informatiche per disastri naturali o mancanza energia elettrica | Alterazione, perdita di dati (basso). | Uso di sistemi di back-up, con copie custodite in luoghi geografici differenti. Uso di sistemi di UPS e/o generatori diesel |
| | Sottrazione degli elaboratori, programmi, supporti e dati | Accesso, alterazione, perdita di dati (basso). | Uso di sistemi di accesso controllato alle sale dati ed in presenza di personale Venis. Uso di procedure di back-up e ripristino dati. |
| Eventi relativi al | Accessi non autorizzati a | Sottrazione, alterazione hardware; | Uso di sistemi di accesso |

| | | | |
|---|---|---|---|
| contesto | locali/reparti ad accesso ristretto | disfunzioni nell'erogazione dei servizi (medio) | controllato alle sale dati ed in presenza di personale Venis. Uso di procedure di back-up e ripristino dati. |
| | Asportazione e furto di strumenti contenenti dati | Accesso non consentito a dati personali (basso). | Uso di sistemi di accesso controllato alle sale dati ed in presenza di personale Venis. Uso di procedure di back-up e ripristino dati. |
| | Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc), nonché dolosi, accidentali o dovuti ad incuria | Perdita di dati (medio) | Uso di procedure di back-up da copie conservate in luoghi fisicamente differenti. Adozione di sistemi antincendio, di condizionamento della temperatura. |
| | Guasto ai sistemi complementari (es. impianto elettrico, climatizzazione) | Alterazione, perdita di dati (medio) | Uso di sistemi di UPS e generatore diesel; impianto di condizionamento ridondato. Contratti di manutenzione ordinaria /straordinaria con le società fornitrici. |
| | Errori umani nella gestione della sicurezza fisica | Alterazione, perdita di dati (medio) | Uso di sistemi antincendio, allarme per accesso non autorizzato, polizza RC per personale Venis e di società terze |

## 12.5 MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE (regola 19.4 e 19.5)

Tabella relativa alle misure di sicurezza adottate o da adottare

| *Misure* | *Descrizione dei rischi contrastati* | *Trattamenti interessati* | *Misura già in essere* | *Misura da adottare (*)* | *Struttura o persone addette all'adozione* |
|---|---|---|---|---|---|
| Adozione sistema di autenticazione | Comportamenti sleali o fraudolenti,<br>Accessi non autorizzati a locali/reparti ad accesso ristretto | Trattamento dati anagrafici, c.f., sede, recapiti;<br>Trattamento dati anagrafici, stato di salute, appartenenza sindacati, esperienze professionali;<br>trattamento dati anagrafici, recapiti telefonici e relativi all'uso del servizio;<br>trattamento dati relativi alla solvibilità;<br>trattamento dati per finalità di giustizia | X | | Operations;<br>Oder mgmt & Process - System Information, Personnel, Administration, Marketing |
| Adozione sistema di autorizzazione | Comportamenti sleali o fraudolenti;<br>alterazione/danneggiamento doloso del sistema dei programmi dei dati; accessi non autorizzati | Trattamento dati anagrafici, c.f., sede, recapiti;<br>trattamento dati anagrafici, stato di salute, appartenenza sindacati, esperienze professionali;<br>trattamento dati anagrafici, recapiti telefonici e relativi all'uso del servizio;<br>trattamento dati relativi alla solvibilità; | X | | Operations;<br>Oder mgmt & Process - System Information, Personnel, Administration, Marketing |
| Adozione Sistema di antintrusione | Intercettazioni di informazioni in rete e intrusioni dall'esterno | Trattamento dati anagrafici, recapiti telefonici e relativi all'uso del servizio | X | | Operations;<br>Oder mgmt & Process/ System Information |
| Aggiornamento programmi antivirus | Azioni di virus informatici o di programmi suscettibili di recare danno; malfunzionamento, indisponibilità o degrado degli strumenti | Trattamento dati anagrafici, c.f., sede, recapiti;<br>trattamento dati anagrafici, stato di salute, appartenenza sindacati, esperienze professionali;<br>trattamento dati anagrafici, recapiti telefonici e relativi all'uso del servizio;<br>trattamento dati relativi alla solvibilità; | X | | Operations |
| Salvataggio dei dati | Asportazione e furto di strumenti contenenti dati | Trattamento dati anagrafici, c.f., sede, recapiti;<br>trattamento dati anagrafici, stato di salute, appartenenza sindacati, esperienze professionali;<br>trattamento dati anagrafici, recapiti telefonici e relativi all'uso del servizio;<br>trattamento dati relativi alla solvibilità | X | | Operations;<br>Oder mgmt & Process - System Information |
| Backup dei dati | Danneggiamento risorse informatiche | Trattamento dati anagrafici, c.f., sede, recapiti;<br>trattamento dati anagrafici, stato di salute, appartenenza sindacati, esperienze professionali;<br>trattamento dati anagrafici, recapiti telefonici e relativi all'uso del servizio;<br>trattamento dati relativi alla solvibilità | X | | Operations;<br>Oder mgmt & Process - System Information |
| Uso di strumenti elettronici contro l'accesso abusivo ai dati | Accesso abusivo ai dati | Trattamento dati anagrafici, c.f., sede, recapiti;<br>trattamento dati anagrafici, stato di salute, appartenenza sindacati, esperienze professionali;<br>trattamento dati anagrafici, recapiti telefonici e relativi all'uso del servizio;<br>trattamento dati relativi alla solvibilità | X | | Operations;<br>Oder mgmt & Process - System Information |
| Ripristino dei dati | Comportamenti sleali o fraudolenti | Trattamento dati anagrafici, c.f., sede, recapiti;<br>trattamento dati anagrafici, stato di salute, appartenenza sindacati, esperienze professionali;<br>trattamento dati anagrafici, recapiti telefonici e relativi all'uso del servizio; | X | | Operations;<br>Oder mgmt & Process - System Information |

| | | | | | |
|---|---|---|---|---|---|
| | | trattamento dati relativi alla solvibilità | | | |
| Gruppo di continuità dell'alimentazione elettrica | Guasto ai sistemi complementari (es. impianto elettrico, climatizzazione) | Trattamento dati anagrafici, c.f., sede, recapiti;<br>trattamento dati anagrafici, stato di salute, appartenenza sindacati, esperienze professionali;<br>trattamento dati anagrafici, recapiti telefonici e relativi all'uso del servizio;<br>trattamento dati relativi alla solvibilità | X | | Operations |

*(*) Indicare eventualmente i tempi previsti per l'adozione delle misure*

Con particolare riferimento al trattamento dei dati effettuato con strumenti elettronici, gli incaricati al trattamento dei dati, dovranno osservare le seguenti istruzioni per l'utilizzo degli strumenti informatici:

- obbligo di custodire i dispositivi di accesso agli strumenti informatici (username e password);
- obbligo di non lasciare incustodito ed accessibile lo strumento elettronico assegnato durante una sessione di trattamento e, più in generale, durante i periodi di assenza dalla postazione di lavoro;
- obbligo di assoluta riservatezza;
- divieto di divulgazione della password di accesso al sistema;
- aggiornamento settimanale del sistema di protezione per le banche dati da parte degli amministratori di sistema.

***Misure di sicurezza adottate o da adottare per il trattamento dei dati per finalità di giustizia***

| ***Misure*** | ***Descrizione dei rischi contrastati*** | ***Misura già in essere*** | ***Misura da adottare (*)*** |
|---|---|---|---|
| Adozione sistema di autenticazione | Comportamenti sleali o fraudolenti,<br>Accessi non autorizzati a locali/reparti ad accesso ristretto | X | |
| Adozione sistema di autorizzazione | Comportamenti sleali o fraudolenti; alterazione/danneggiamento doloso del sistema dei programmi dei dati; accessi non autorizzati | X | |
| Adozione Sistema di antintrusione | Intercettazioni di informazioni in rete e intrusioni dall'esterno | X | |
| Aggiornamento programmi antivirus | Azioni di virus informatici o di programmi suscettibili di recare danno; malfunzionamento, indisponibilità o degrado degli strumenti | X | |
| Salvataggio dei dati | Asportazione e furto di strumenti contenenti dati | X | |
| Backup dei dati | Danneggiamento risorse informatiche | X | |
| Uso di strumenti elettronici contro l'accesso abusivo ai dati | Accesso abusivo ai dati | X | |
| Ripristino dei dati | Comportamenti sleali o fraudolenti | X | |
| Gruppo di continuità dell'alimentazione elettrica | Guasto ai sistemi complementari (es. impianto elettrico, climatizzazione) | X | |

## 13. PIANO DI VERIFICA DELLE MISURE ADOTTATE

La bontà delle misure adottate deve essere periodicamente verificata. Durante queste operazioni di verifica, da effettuarsi al più ogni sei mesi, sarà data particolare importanza ai seguenti punti:

- Verificare la bontà delle misure di anti intrusione adottate.
- Corretto utilizzo delle parole chiave e dei profili di accesso degli incaricati. Occorre prevedere la disattivazione dei codici di accesso non utilizzati per più di sei mesi.
- Aggiornamento del software antivirus.
- Integrità dei dati e delle loro copie di backup.
- Bontà della conservazione dei documenti cartacei.
- Accertamento della distruzione dei supporti magnetici che non possono più essere utilizzati.
- Accertamento del livello di formazione degli incaricati. Prevedere sessioni di aggiornamento anche in relazione all'evoluzione tecnica e tecnologica avvenuta in azienda.

Di queste verifiche sarà redatto un documento che potrà essere allegato al documento programmatico per la sicurezza.

## 14. PIANO DI FORMAZIONE DEGLI INCARICATI (Regola 19.6)

Gli incaricati dovranno essere edotti sui rischi individuati e sui modi per prevenire i danni.
La formazione ha i seguenti contenuti:

- Una analisi dettagliata ed aggiornata delle vigenti disposizioni di legge, con riferimenti anche alle normative europee.
- Analisi dettagliata del Decreto Legislativo 196/2003.
- Analisi e spiegazione dei ruoli: titolare, responsabile, incaricato, amministratore di sistema, custode delle password, interessato.
- Panoramica sugli adempimenti: notificazione, rapporti con gli interessati, rapporti con il Garante.
- Misure minime ed appropriate di sicurezza con particolare riferimento a:
  - criteri logici, fisici ed organizzativi per la protezione dei sistemi informativi.
  - prevenzione e contenimento del danno.
  - strumenti di protezione hardware e software (in particolare antivirus e misure antihacker), contenitori di sicurezza, sistemi anti intrusione.
  - importanza e modalità di realizzazione delle operazioni di backup.

Coerentemente con l'evoluzione degli strumenti tecnici adottati da VENIS S.p.A. e/o dall'insorgere di nuove disposizioni legislative in materia, verranno istituiti incontri formativi. In ogni caso, almeno una volta l'anno, verrà comunque istituito un incontro per risensibilizzare gli incaricati sull'importanza di adottare le norme di sicurezza predisposte e per recepire eventuali suggerimenti in materia derivanti dalla constatazione della presenza di minacce o vulnerabilità riscontrate.

## 15. STANDARDS

In questo capitolo vengono riportati i fac-simile delle lettere di designazione degli Incaricati, le lettere di nomina del Responsabile del Trattamento, degli Amministratori di Sistema e del Custode delle parole chiavi. Vengono, inoltre, fornite le lettere di richiesta dei nominativi delle persone che lavorano per le imprese di pulizia e di vigilanza e il verbale di partecipazione ai corsi di formazione.

## 15.1 STANDARD LETTERA DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO

Lugo, data

Egregio
Sig._____
Via_____
_____

Via raccomandata A/R / Consegnata a mano

Oggetto: Lettera di nomina del Responsabile del Trattamento.

Egregio Sig. _____,
la scrivente società, in qualità di Titolare del Trattamento dei dati personali, conformemente a quanto stabilito dal Codice in materia di protezione dei dati personali, Le affida l'incarico di Responsabile del Trattamento, il quale attenendosi alle istruzioni impartite e' soggetto, anche tramite verifiche periodiche, al potere di vigilanza esercitato dall'organo amministrativo di Venis S.p.A. sulla puntuale osservanza delle disposizioni in materia di trattamento dei dati personali e di sicurezza dettate dal Codice in materia di protezione dei dati personali e delle istruzioni ricevute dal Titolare stesso.

A tal riguardo, si significa che, in qualità di Responsabile del Trattamento nominato, avvalendosi ove necessario anche della collaborazione di Incaricati del Trattamento, interni o esterni, all'uopo nominati dovrà:

- redigere ed aggiornare almeno annualmente, e conservare il Documento Programmatico della Sicurezza presso la sede aziendale;
- riferire dell'avvenuta adozione e/o dell'aggiornamento del DPS nella relazione accompagnatoria al bilancio d'esercizio, se dovuta, senza doverne allegare una copia;
- aggiornare l'elenco dei trattamenti dei dati personali in azienda e garantire il diritto d'accesso come previsto dalle norme sulla privacy;
- individuare, predisporre, verificare, documentare e rendere note le misure di sicurezza (minime e più ampie) necessarie per la protezione dei dati personali;
- tenere ed aggiornare l'elenco degli Amministratori di Sistema, ai sensi del Provvedimento del Garante della protezione dei dati personali del 27 novembre 2008, recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", il quale dovrà essere reso disponibile al Garante, se richiesto;
- verificare, annualmente l'operato degli Amministratori di Sistema;
- implementare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli Amministratori di Sistema, che assicurino che le registrazioni (*access log*) abbiano le caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste, e comprendano i

riferimenti temporali e la descrizione dell'evento che le ha generate, assicurando che siano conservate per un congruo periodo, non inferiore a sei mesi;

- rendere nota in forma scritta ai dipendenti di Venis S.p.A. l'identità degli Amministratori di Sistema, ove l'attività degli Amministratori di Sistema dovesse riguardare anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori.

Cordiali Saluti.

Venis Spa

Il Titolate del Trattamento

## 15.2 STANDARD LETTERA INCARICATO DEL TRATTAMENTO DI DATI PERSONALI PER DIRIGENTI – RESPONSABILI DI AREA

VENIS S.P.A.

MANSIONI DEI DIPENDENTI INCARICATI DEL TRATTAMENTO DI DATI PERSONALI DIRIGENTI – RESPONSABILI DI AREA

(ai sensi del Codice in materia di protezione dei dati personali)

Luogo, data

Egregio Signor, [indicare NOME COGNOME]

Con la presente La informiamo che, le Sue attività professionali includono anche, ai sensi del Decreto legislativo n. 196/03 (d'ora in poi il «Codice»), quella di Incaricato del Trattamento di dati personali (intendendosi per dato personale qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale, ai sensi dell'art. 4, c. 1, lett. b) del Codice), attività che deve svolgere secondo le procedure stabilite dalla competente funzione aziendale. In particolare, le Sue attività professionali includono tutte le operazioni rientranti nella nozione di trattamento di cui all'art. 4, c. 1, lett. a) del Codice svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati.

I dati personali di cui ha preso o prenderà conoscenza in conseguenza dell'esercizio delle mansioni così assegnate dovranno essere trattati in modo lecito e secondo correttezza, nonché custoditi in maniera tale da ridurre al minimo, mediante l'adozione delle idonee misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, degli stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Qualora avesse dubbi in merito a quanto sopra, La invitiamo a chiedere chiarimenti al sottoscritto.

In particolare, Lei è tenuto/a ad utilizzare i dati personali di cui è a conoscenza oppure venga a conoscenza nell'esercizio delle su indicate mansioni solo ed esclusivamente ai fini del trattamento di cui è incaricato ed a comunicarli, diffonderli o trasmetterli solo in ambito aziendale e/o secondo le istruzioni che Le saranno come sopra impartite, nonché a rispettare, più in generale, il divieto di comunicazione e diffusione dei dati trattati nell'esercizio di tali mansioni.

Poiché la violazione degli obblighi sanciti dal Codice è tale da determinare (anche a Suo carico) responsabilità civili e penali, la violazione delle disposizioni di cui sopra può esporLa alle conseguenti sanzioni disciplinari. In tal caso, Venis S.p.A. si riserva di attivare contro di Lei ogni ulteriore mezzo legale a salvaguardia propria e dei terzi interessati.

Le intervenute modifiche di cui sopra alle Sue mansioni, originate dall'entrata in vigore della Legge, lasciano intatta ed immodificata ogni ulteriore condizione economica e normativa del Suo rapporto di lavoro.

Copia del Documento Programmatico sulla Sicurezza e del Codice e sono conservati e consultabili presso l'Ufficio del Direttore dei Sistemi e Servizi Tecnologici – Sicurezza Informatica.

Cordiali Saluti

Venis Spa

Il Titolate del Trattamento

## 15.3 STANDARD LETTERA INCARICATO DEL TRATTAMENTO DI DATI PERSONALI PER DIPENDENTE

VENIS S.P.A.

MANSIONI DEI DIPENDENTI INCARICATI DEL TRATTAMENTO DI DATI PERSONALI

(ai sensi del Codice in materia di protezione dei dati personali)

Luogo, data

Egregio Signor, [indicare NOME COGNOME]

Con la presente La informiamo che, le Sue attività professionali includono anche, ai sensi del Decreto legislativo n. 196/03 (d'ora in poi il «Codice»), quella di Incaricato del Trattamento di dati personali (intendendosi per dato personale qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale, ai sensi dell'art. 4, c. 1, lett. b) del Codice), attività che deve svolgere secondo le procedure stabilite dalla competente funzione aziendale. In particolare, le Sue attività professionali includono tutte le operazioni rientranti nella nozione di trattamento di cui all'art. 4, c. 1, lett. a) del Codice svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati.

I dati personali di cui Lei ha preso o prenderà conoscenza in conseguenza dell'esercizio delle mansioni così assegnate dovranno essere trattati in modo lecito e secondo correttezza, nonché custoditi in maniera tale da ridurre al minimo, mediante l'adozione delle idonee misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, degli stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Qualora avesse dubbi in merito a quanto sopra, La invitiamo a chiedere chiarimenti al Suo Responsabile di riferimento oppure al sottoscritto.

In particolare, Lei è tenuto/a ad utilizzare i dati personali di cui venga a conoscenza nell'esercizio delle su indicate mansioni solo ed esclusivamente ai fini del trattamento di cui è incaricato ed a comunicarli, diffonderli o trasmetterli solo in ambito aziendale e/o secondo le istruzioni che Le saranno come sopra impartite, nonché a rispettare, più in generale, il divieto di comunicazione e diffusione dei dati trattati nell'esercizio di tali mansioni.

Nell'assolvimento del compito in questione dovrà osservare le seguenti istruzioni:

- può accedere alle banche dati (informatiche) utilizzando sempre il proprio codice di accesso personale, evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- senza preventiva autorizzazione del Titolare, o del proprio Responsabile di riferimento, non è possibile creare nuove autonome banche dati;
- nessun dato può essere utilizzato o trasmesso all'esterno se non dietro autorizzazione del Titolare o del proprio Responsabile di riferimento;
- è tenuto ad osservare tutte le misure di protezione e sicurezza atte ad evitare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito, già in atto o successivamente indicate dal Titolare o dal proprio Responsabile di riferimento;

- nel caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al Titolare oppure al proprio Responsabile di riferimento;
- deve consegnare al Custode delle chiavi in busta chiusa la parola chiave da lei adottata e le eventuali modificazioni nonché provvedere a fornire, secondo le istruzioni del Titolare, i dati necessari per la *strong authentication.*

Poiché la violazione degli obblighi sanciti dal Codice è tale da determinare (anche a Suo carico) responsabilità civili e penali, la violazione delle disposizioni di cui sopra può esporLa alle conseguenti sanzioni disciplinari. In tal caso, Venis S.p.A. si riserva di attivare contro di Lei ogni ulteriore mezzo legale a salvaguardia propria e dei terzi interessati.

Le intervenute modifiche di cui sopra alle Sue mansioni, originate dall'entrata in vigore della Legge, lasciano intatta ed immodificata ogni ulteriore condizione economica e normativa del Suo rapporto di lavoro.

Copia del Documento Programmatico sulla Sicurezza e del Codice e sono conservati e consultabili presso l'Ufficio del Direttore dei Sistemi e Servizi tecnologici – Sicurezza Informatica.

Cordiali Saluti.

Venis Spa

Il Titolate del Trattamento

## 15.4 STANDARD LETTERA INCARICATO DEL TRATTAMENTO DI DATI DI TRAFFICO PER FINALITA' DI GIUSTIZIA PER DIPENDENTE

VENIS S.P.A.

MANSIONI DEI DIPENDENTI INCARICATI DEL TRATTAMENTO DI DATI DI TRAFFICO PER FINALITA' DI GIUSTIZIA

(ai sensi del Codice in materia di protezione dei dati personali)

Luogo, data

Egregio Signor, [indicare NOME COGNOME]

Con la presente La informiamo che, le Sue mansioni includono anche, ai sensi del Decreto legislativo n. 196/03 (d'ora in poi il «Codice») e del Provvedimento del Garante per la protezione dei dati personali del 17 gennaio 2008 recante "Sicurezza dei dati di traffico telefonico e telematico" (di seguito, il "Provvedimento"), quella di Incaricato del Trattamento di dati di traffico per finalità di giustizia (intendendosi per dati di traffico trattato per finalità di giustizia qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione che venga trattato per finalità di accertamento e repressione dei reati ai sensi del combinato disposto dell'art. 4, c. 1, lett. h) e dell'art. 132 c. 1 del Codice), mansioni che deve svolgere secondo le procedure stabilite dalla competente funzione aziendale. In particolare, le Sue mansioni includeranno tutte le operazioni rientranti nella nozione di trattamento di cui all'art. 4, c. 1, lett. a) del Codice nonché quelle necessarie a garantire l'accesso ai dati di traffico trattati per finalità di giustizia ai sensi dell'art. 7 del Codice medesimo.

I dati di traffico di cui Lei ha preso o prenderà conoscenza in conseguenza dell'esercizio delle mansioni così assegnate dovranno essere trattati in modo lecito e secondo correttezza, nonché custoditi in maniera tale da ridurre al minimo, mediante l'adozione delle idonee misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, degli stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Qualora avesse dubbi in merito a quanto sopra, La invitiamo a chiedere chiarimenti al Suo Responsabile oppure al sottoscritto.

In particolare, Lei è tenuto ad utilizzare i dati di traffico di cui venga a conoscenza nell'esercizio delle su indicate mansioni solo ed esclusivamente ai fini del trattamento di cui è incaricato ed a comunicarli, diffonderli o trasmetterli solo in ambito aziendale e/o secondo le istruzioni che Le saranno come sopra impartite, nonché a rispettare, più in generale, il divieto di comunicazione e diffusione dei dati trattati nell'esercizio ditali mansioni.

Nell'assolvimento del compito in questione dovrà osservare scrupolosamente le seguenti istruzioni:

- può accedere esclusivamente alle banche dati delle aree e degli uffici in cui sono custoditi i dati di traffico per finalità di giustizia, incluse le aree ad accesso selezionato, previa autenticazione nelle forme di legge;
- senza preventiva autorizzazione, anche verbale, del Titolare, non è possibile creare nuove autonome banche dati;
- nessun dato può essere utilizzato o trasmesso all'esterno se non dietro autorizzazione del Titolare;

- è tenuto ad osservare tutte le misure di protezione e sicurezza atte ad evitare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito, già in atto o successivamente indicate dal Titolare;
- deve consegnare al Custode delle chiavi in busta chiusa la parola chiave da lei adottata e le eventuali modificazioni, nonché provvedere a fornire, secondo le istruzioni del Titolare, i dati necessari per la *strong authentication.*

Poiché la violazione degli obblighi sanciti dal Codice e dal Provvedimento è tale da determinare (anche a Suo carico) responsabilità civili e penali, la violazione delle disposizioni di cui sopra può esporLa alle conseguenti sanzioni disciplinari. In tal caso, Venis S.p.A. si riserva di attivare contro di Lei ogni ulteriore mezzo legale a salvaguardia propria e dei terzi interessati.

Le eventuali intervenute modifiche di cui sopra alle Sue mansioni, originate dall'entrata in vigore del Codice, lasciano intatta ed immodificata ogni ulteriore condizione economica e normativa del Suo attuale rapporto di lavoro.

Copia del Documento Programmatico sulla Sicurezza e del Codice e sono conservati e consultabili presso l'Ufficio del Direttore dei Sistemi e Servizi Tecnologici – Sicurezza Informatica.

Cordiali saluti.

Venis Spa

Il Titolate del Trattamento

## 15.5 STANDARD LETTERA INCARICATO DEL TRATTAMENTO DI DATI SENSIBILI PER DIPENDENTE

VENIS S.P.A.

MANSIONI DEI DIPENDENTI INCARICATI DEL TRATTAMENTO DI DATI PERSONALI E SENSIBILI

(ai sensi del Codice in materia di protezione dei dati personali)

Luogo, data

Egregio Signor, [indicare NOME COGNOME]

Con la presente La informiamo che le Sue mansioni includono anche, ai sensi del Decreto legislativo n. 196/03 (d'ora in poi il «Codice»), quella di Incaricato del Trattamento di dati personali (intendendosi per dato personale qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale, ai sensi dell'art. 4, c. 1, lett. b) del Codice), mansioni che deve svolgere secondo le procedure stabilite dalla competente funzione aziendale. In particolare, le Sue mansioni includono tutte le operazioni rientranti nella nozione di trattamento di cui all'art. 4, c. 1, lett. a) del Codice svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati.

I dati personali di cui Lei ha preso o prenderà conoscenza in conseguenza dell'esercizio delle mansioni così assegnate dovranno essere trattati in modo lecito e secondo correttezza, nonché custoditi in maniera tale da ridurre al minimo, mediante l'adozione delle idonee misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, degli stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Qualora avesse dubbi in merito a quanto sopra, La invitiamo a chiedere chiarimenti al Suo Responsabile oppure al sottoscritto.

In particolare, Lei è tenuto ad utilizzare i dati personali di cui venga a conoscenza nell'esercizio delle su indicate mansioni solo ed esclusivamente ai fini del trattamento di cui è incaricato ed a comunicarli, diffonderli o trasmetterli solo in ambito aziendale e/o secondo le istruzioni che Le saranno come sopra impartite, nonché a rispettare, più in generale, il divieto di comunicazione e diffusione dei dati trattati nell'esercizio ditali mansioni.

Nell'assolvimento del compito in questione deve osservare scrupolosamente le seguenti istruzioni:

- può accedere esclusivamente alle banche dati (informatiche e/o cartacee) delle aree e degli uffici di sua competenza;
- senza preventiva autorizzazione del Titolare, anche verbale, non è possibile creare nuove autonome banche dati;
- nessun dato può essere utilizzato o trasmesso all'esterno se non dietro autorizzazione del Titolare;
- è tenuto ad osservare tutte le misure di protezione e sicurezza atte ad evitare rischi di distruzione, perdita, accesso non autorizzato o trattamento non consentito, già in atto o successivamente indicate dal Titolare;

- deve consegnare al Custode delle chiavi in busta chiusa la parola chiave da lei adottata e le eventuali modificazioni, nonché provvedere a fornire, secondo le istruzioni del Titolare, i dati necessari per la *strong authentication.*

Poiché la violazione degli obblighi sanciti dal Codice è tale da determinare (anche a Suo carico) responsabilità civili e penali, la violazione delle disposizioni di cui sopra può esporLa alle conseguenti sanzioni disciplinari. In tal caso, Venis S.p.A. si riserva di attivare contro di Lei ogni ulteriore mezzo legale a salvaguardia propria e dei terzi interessati.

Lei ha inoltre accesso, ai fini del trattamento ed in conformità alle disposizioni del Codice e del Documento Programmatico sulla sicurezza, in ragione dei compiti che Le sono stati assegnati, anche a dati definiti sensibili, cioè a dati personali «idonei a rivelare l'origine razziale od etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute o la vita sessuale». Vista la particolare delicatezza di tali dati, sottolineiamo l'esigenza di una particolare attenzione e diligenza da parte Sua nell'osservanza delle disposizioni di cui sopra.

Le eventuali intervenute modifiche di cui sopra alle Sue mansioni, originate dall'entrata in vigore del Codice, lasciano intatta ed immodificata ogni ulteriore condizione economica e normativa del Suo rapporto di lavoro.

Copia del Documento Programmatico sulla Sicurezza e del Codice e sono conservati e consultabili presso l'Ufficio del Direttore dei Sistemi e Servizi Tecnologici – Sicurezza Informatica.

Cordiali saluti.

Venis Spa

Il Titolate del Trattamento

## 15.6 STANDARD LETTERA DI NOMINA AD AMMINISTRATORE DI SISTEMA ED ISTRUZIONI

Luogo, data

Egregio e/o Spett.le

_____

via_____

_____

Consegnata a mano

Oggetto: Lettera di comunicazione della nomina di Amministratore del Sistema Informatico della società.

Egregio Sig. _____,

con la presente, si comunica che - in conformità del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 recante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" – Lei è stato nominato Amministratore del Sistema Informatico della società Venis S.p.A..

Lei, con la sottoscrizione della presente, accetta la nomina, e conferma la diretta ed approfondita conoscenza della normativa in materia di protezione dei dati personali nonché degli obblighi in essa previsti.

Con la presente, in considerazione delle caratteristiche di esperienza, capacità ed affidabilità richieste dalle vigenti disposizioni in materia di sicurezza del trattamento dei dati, si affidano le seguenti incombenze e responsabilità:

- operare il sistema informativo nel quale risiedono le banche dati personali in osservanza al Documento Programmatico sulla Sicurezza ed alle misure minime previste dal Codice in materia di protezione dei dati personali ( di seguito anche il "Codice"), attenendosi alle disposizioni del Responsabile del Trattamento dei dati in tema di sicurezza;
- collaborare per l'implementazione ed operare le misure prescritte dal Provvedimento del 17 gennaio 2008 sulla "Sicurezza dei dati di traffico telefonico e telematico" adottato dal Garante per la protezione dei dati personali;
- collaborare in generale per l'attuazione delle prescrizioni impartite dal Garante per la protezione dei dati personali;
- collaborare al coordinamento delle attività operative degli Incaricati del Trattamento nello svolgimento delle mansioni loro affidate per garantire un corretto, lecito e sicuro trattamento;
- collaborare alla predisposizione ed aggiornamento del sistema di sicurezza idoneo a rispettare le prescrizioni di cui al Codice, nonché collaborare all'adeguamento del sistema alle future norme regolamentari in materia di sicurezza in osservanza alle disposizioni del Responsabile del Trattamento dei dati personali e in coordinamento con esso;
- comunicare al Responsabile del Trattamento dei dati personali qualsiasi elemento oggettivo o soggettivo che possa compromettere il corretto trattamento dei dati stessi;

- assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso in azienda;
- predisporre e rendere funzionanti le copie di sicurezza (operazioni di backup e recovery) dei dati e delle applicazioni;
- adottare ogni e qualsiasi misura necessaria per garantire il rispetto della Legge 18 marzo 2008, n. 48 - Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, firmata a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno.

Con la presente, si ricorda che il Suo operato sarà oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dello scrivente Responsabile del Trattamento dei dati personali, allo scopo di controllare la rispondenza dello stesso alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

Infine, si significa che Venis S.p.A. applica sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) degli Amministratori di Sistema ai sistemi di elaborazione e agli archivi elettronici, che assicurano che le registrazioni (*access log*) abbiano le caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste, e comprendano i riferimenti temporali e la descrizione dell'evento che le ha generate, assicurando che siano conservate per un congruo periodo, non inferiore a sei mesi.

Cordiali Saluti.

Venis Spa

Il Titolate del Trattamento

## 15.7 STANDARD LETTERA DI NOMINA DEL CUSTODE DELLE PAROLE CHIAVE

Luogo, data

Egregio
Sig._____
Via_____
_____

Consegnata a mano

Oggetto: Lettera di incarico al Custode delle parole chiave

Con la presente, conformemente a quanto stabilito dal Codice in materia di protezione dei dati personali, Le affidiamo l'incarico di Custode delle parole chiave.

Il Custode delle parole chiave dichiara di essere a conoscenza di quanto stabilito dal Codice e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

In particolare dovrà:

- predisporre, per ogni Incaricato del Trattamento, una busta sulla quale è indicato lo USER-ID utilizzato:
- all'interno della busta deve essere indicata la password;
- conservare le buste con le password in un luogo chiuso e protetto;
- revocare tutte le password non utilizzate per un periodo superiore a 6 (sei) mesi;
- modificare la parola chiave almeno ogni sei mesi e, in caso di trattamento di dati sensibili e di dati giudiziari, almeno ogni 3 (tre) mesi;
- revocare tempestivamente tutte le password assegnate a soggetti che su comunicazione scritta del Titolare del Trattamento non sono più autorizzati ad accedere ai dati;
- provvedere al rilevamento ed alla registrazione dei dati per l'accesso secondo tecniche di *strong authentication* ai dati di traffico.

Nel caso in cui l'Incaricato del Trattamento possa modificare autonomamente la propria Password di accesso, quest'ultimo deve consegnare, per ogni variazione, al Custode delle Password una busta chiusa sulla quale è indicato il proprio USER-ID che contiene la Password in vigore. Il Custode delle Password provvederà a sostituire la precedente busta con quest'ultima.

Cordiali Saluti

Venis Spa

Il Titolate del Trattamento

Modulo comunicazione Password

Nome incaricato del trattamento .

Password di accensione:

Password di accesso alla rete:

Area di appartenenza:

Data

Firma dell'incaricato del trattamento

N.B. Questo modulo è da consegnare al Custode delle Password, in busta chiusa che dovrà recare all'esterno il nome dell'Incaricato del Trattamento autorizzato alla modifica della propria Password.

Sarà cura dell'Incaricato del Trattamento comunicare immediatamente al Custode delle Password ed in mancanza al Responsabile di Area, la variazione delle proprie password di accesso, utilizzando sempre il presente modulo.

## 15.8 STANDARD LETTERA DI RICHIESTA DEI NOMINATIVI DELLE PERSONE CHE LA DITTA DI VIGILANZA HA ASSEGNATO AL CONTROLLO DEI LOCALI DI VENIS S.P.A.

Luogo, data

Spettabile

_____

Via _____

_____ - _____

Raccomandata A/R

Con riferimento agli obblighi di identificazione e registrazione dei soggetti ammessi agli archivi prima dell'orario di apertura e dopo l'orario di chiusura, si fa presente che la protezione delle archiviazioni è estesa alla custodia e conservazione di ogni atto e documento cartaceo contenente dati personali particolari riferiti a persone fisiche e giuridiche.

In ottemperanza alle suddette necessità di legge, vogliate cortesemente fornirci i nominativi delle persone che la Vostra ditta ha assegnato alla vigilanza dei locali di Venis S.p.A., in Venezia Sestiere Castello n. 2838 e Marghera (Venezia) Via delle Industrie 27/B. In caso di assenza o impedimento delle persone che ci indicherete, sarà Vostra cura, ed obbligo, comunicarci i nominativi dei sostituti.

Ai fini dei controlli e delle responsabilità civili e penali connessi alla violazione delle norme contenute nel decreto sarà opportuno che la Vostra ditta organizzi un registro delle persone autorizzate ad accedere nei nostri locali.

Le persone autorizzate dovranno limitarsi alle sole attività di vigilanza. Tale condotta dovrà essere rispettata dal Vostro personale che, allo scopo, sarà da Voi informato.

Cordiali Saluti

Venis Spa

Il Titolate del Trattamento

## 15.9 STANDARD LETTERA DI RICHIESTA DEI NOMINATIVI DELLE PERSONE CHE LA DITTA DI PULIZIE ASSEGNA AI LOCALI DI VENIS S.P.A.

Luogo, data

Spettabile

_____

Via _____

_____ - _____

Raccomandata A/R

Conformemente a quanto stabilito dal Codice in materia di protezione dei dati personali e dal Documento Programmatico sulla sicurezza dell'azienda, tra i nuovi obblighi previsti vi è anche quello:

- in determinate circostanze, della identificazione e registrazione dei soggetti ammessi agli archivi prima dell'orario di apertura e dopo l'orario di chiusura. Infatti, la protezione delle archiviazioni è estesa alla custodia e conservazione di ogni atto e documento cartaceo contenente dati personali particolari riferiti a soggetti fisici e giuridici;
- in ottemperanza alle suddette previsioni di legge, vogliate cortesemente fornirci i nominativi delle persone che la Vostra ditta ha assegnato alle pulizie dei locali di Venis S.p.A., in Venezia Sestiere Castello n. 2838 e Marghera (Venezia) Via delle Industrie 27/B, e ciò anche al fine di poter considerare tali persone autorizzate all'accesso nei nostri locali. In caso di assenza o impedimento delle persone che ci indicherete, sarà vostra cura ed obbligo comunicarci i nominativi dei sostituti.

Ai fine dei controlli e delle responsabilità civili e penali connesse alla violazione delle norme contenute nel decreto sarà opportuno che la Vostra ditta organizzi un registro delle persone autorizzate ad accedere nei nostri locali.

Le persone autorizzate dovranno limitarsi alle sole attività di pulizia. Il materiale cartaceo asportato destinato allo smaltimento dei rifiuti, dovrà essere riposto con cura negli appositi sacchi di plastica e, tali sacchi dovranno essere chiusi in maniera che gli atti e i documenti in essi contenuti non possano, nemmeno accidentalmente, fuoriuscire. Tale condotta dovrà essere rispettata dal Vostro personale che, allo scopo, sarà da Voi informato.

Cordiali Saluti

Venis Spa

Il Titolate del Trattamento

## 15.10 FORMAZIONE E VERBALE DI PARTECIPAZIONE AI CORSI DI FORMAZIONE

Gli incaricati dovranno essere edotti sui rischi individuati e sui modi per prevenire i danni.
La formazione ha i seguenti contenuti:

- Una analisi dettagliata ed aggiornata delle vigenti disposizioni di legge, con riferimenti anche alle normative europee.
- Analisi dettagliata del Decreto Legislativo 196/2003.
- Analisi e spiegazione dei ruoli: titolare, responsabile, incaricato, amministratore di sistema, custode delle password, interessato.
- Panoramica sugli adempimenti: notificazione, rapporti con gli interessati, rapporti con il Garante.
- Misure minime ed appropriate di sicurezza con particolare riferimento a:
  - criteri logici, fisici ed organizzativi per la protezione dei sistemi informativi.
  - prevenzione e contenimento del danno.
  - strumenti di protezione hardware e software (in particolare antivirus e misure antihacker), contenitori di sicurezza, sistemi anti intrusione.
  - importanza e modalità di realizzazione delle operazioni di backup.

Coerentemente con l'evoluzione degli strumenti tecnici adottati da VENIS S.p.A. e/o dall'insorgere di nuove disposizioni legislative in materia, verranno istituiti incontri formativi. In ogni caso, almeno una volta l'anno, verrà comunque istituito un incontro per risensibilizzare gli incaricati sull'importanza di adottare le norme di sicurezza predisposte e per recepire eventuali suggerimenti in materia derivanti dalla constatazione della presenza di minacce o vulnerabilità riscontrate.

| **Dati del corso formativo** | |
|---|---|
| Relatore | |
| Argomenti trattati:<br>Codice in materia di protezione dei dati personali<br>Misure di sicurezza<br>Analisi della situazione aziendale: rischi individuati e possibili soluzioni | |
| Documentazione | |

| **Elenco dei partecipanti** |
|---|

| Nominativo | Dipartimento | Firma |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Luogo e data

Venis S.p.A.

## 16. DICHIARAZIONE D'IMPEGNO E FIRMA

Il presente documento redatto in data 15 Luglio 2011 viene firmato in calce da Venis S.p.A. in qualità di Titolare del trattamento dei dati, nella persona di Presidente e Legale rappresentante, il quale verrà aggiornato periodicamente entro il 31 marzo di ogni anno.
L'originale del presente documento è custodito presso la sede di Venis S.p.A. per essere esibito in caso di controllo.
Una copia verrà consegnata ai responsabili di determinati trattamenti di dati appositamente nominati.

Venezia,

Venis S.p.A

L'Amministratore Unico
Paolo Bettio