DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Redatto ai sensi e per gli effetti dell'articolo 34, comma 1, lettera g) del Decreto Legislativo 196/2003 in materia di trattamento dei dati personali

EMESSO DA

Responsabile Trattamento Dati

Nome Cognome

VERIFICATO E APPROVATO DA

Titolare Trattamento Dati

Nome Cognome

2017

Sommario

ALLEGATI

Premessa

Il presente Documento Programmatico sulla Sicurezza (in seguito abbreviato in DPsS) è redatto in conformità alle disposizioni di cui all'art. 34 del Decreto Legislativo n. 196 del 30 giugno 2003 e relativo allegato B e s.m.i., per definire le politiche di sicurezza in materia di trattamento di dati personali nonché i criteri tecnico-organizzativi per la loro attuazione. Il DPsS viene tenuto aggiornato con periodo annuale a cura del responsabile del trattamento.

L'ambito di applicazione comprende tutte le attività del Consiglio di Bacino che prevedono la gestione di dati personali.

Il documento fornisce idonee informazioni relative alla tipologia di dati personali trattati e all'analisi dei rischi connessi all'utilizzo degli strumenti mediante i quali viene effettuato il trattamento.

Gli originali del DPsS sono custoditi presso la sede dell'Ente dai soggetti all'uopo incaricati, per funzione e grado, alle succitate problematiche.

Quadro normativo

Relativamente al tema della sicurezza nell'ambito informatico e del trattamento di dati personali nella pubblica amministrazione, affrontati nel presente documento, le principali disposizioni normative di riferimento sono le seguenti:

Del. 23/11/2000

Regole tecniche in materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni ai sensi dell'art. 18, comma 3, del D.P.R. 10 novembre 1997, n. 513. (Deliberazione n. 51/2000 pubblicata nella Gazz. Uff. 14 dicembre 2000, n. 291).

Dir. Min. 16/1/2002

Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni. (Pubblicata nella Gazz. Uff. 22 marzo 2002, n. 69).

D. Lgs. 30/6/2003 n. 196

Codice in materia di protezione dei dati personali.

D. Lgs. 7/3/2005 n. 82

Codice dell'amministrazione digitale.

Linee guida per il disaster recovery delle pubbliche amministrazioni

ai sensi del c. 3, lettera b) dell'art. 50bis del Codice dell'Amministrazione Digitale.

L. 4/4/2012 n. 35

Conversione in legge, con modificazioni, del decreto-legge 9 febbraio 2012, n. 5, recante disposizioni urgenti in materia di semplificazione e di sviluppo.

D. Lgs. 28/5/2012 n. 69

Modifiche al decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali in attuazione delle direttive 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche, e 2009/140/CE in materia di reti e servizi di comunicazione elettronica e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori.

DPCM 3/12/2013

Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis, 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005. (Pubblicato nella Gazz. Uff. 12 marzo 2014, n. 59).

Regolamento 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Principali definizioni tecniche e legali

Nel presente documento sono riportate molte definizioni, alcune delle quali introdotte dal contesto normativo, altre dalle definizioni tecniche della materia. Per chiarezza è bene soffermarsi su alcune delle principali definizioni:

- Banca dati: qualsiasi complesso di dati, ripartito in una o più unità dislocate in uno o più siti.
- Trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di mezzi 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 dati.
- Dato Personale: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati od identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

I dati personali sono poi classificati in quattro categorie:

1° Dati sensibili: i dati personali idonei a rilevare l'origine razziale ed etnica, le convenzioni 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 vita sessuale.

2° Dati del Casellario Giudiziario: i dati personali idonei a rilevare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. n° 213 del 14 novembre 2002, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

3° Dati identificativi: i dati personali che permettono l'identificazione diretta dell'interessato.

4° Dato anonimo: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

- 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 ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
- 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.
- Interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

- Incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
- Per Garante si intende l'autorità istituita ai sensi dell'articolo 153 del decreto legislativo 196/2003.
- Per Comunicazione si intende la trasmissione a qualunque titolo, ed in qualunque forma, compiuta attraverso un mezzo trasmissivo, di dati (nel senso più generale del termine). Il decreto recita: *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.*

Ad ulteriore precisazione si aggiunge che:

- I Dati "in chiaro" sono dati comprensibili da chiunque. Ne sono esempio, una conversazione tra persone, il testo di un libro, o le parole di questo documento.
- Per Codifica si intende l'operazione di traduzione di una o più informazioni in una o più stringhe di caratteri detta appunto codice; tale codice porta in se la stessa quantità d'informazione del testo originario ma è comprensibile solo se è noto il sistema di codifica stesso.
- Codifica Univoca: l'operazione di traduzione di una o più informazioni in una stringa (di solito) di caratteri unica nel contesto utilizzato. Ne è un esempio il codice fiscale di una persona.
- Dati "cifrati" sono dati comprensibili a pochi. La cifratura è un'operazione, applicata a dati in chiaro, per trasmettere l'informazione attraverso una codifica segreta (nota a pochi). In questo modo solo chi conosce la codifica può interpretare i dati trasmessi.
- Per User-ID si intende un codice binario che in modo univoco identifica l'utente nel sistema. Esso è generato a partire da due altri codici: il nome utente ("username" o "login") ed il codice segreto ("password"). Il nome utente è un codice univoco in chiaro, il codice segreto non è univoco (più utenti possono avere lo stesso codice) ed è sempre cifrato (incomprensibile alla lettura).

Ogni sistema informatico identifica i suoi utilizzatori attraverso l'uso di user-id appropriati. Il metodo di creazione, gestione, e memorizzazione di questi dati è uno dei cardini essenziali della sicurezza informatica.

Consiglio di Bacino Laguna di Venezia

Il Consiglio di Bacino Laguna di Venezia, istituito con L.R. 17/2012, è la pubblica amministrazione cui è demandato il governo del Servizio idrico integrato all'interno dei 36 comuni di propria competenza.

La sede sia amministrativa che operativa si trova in:

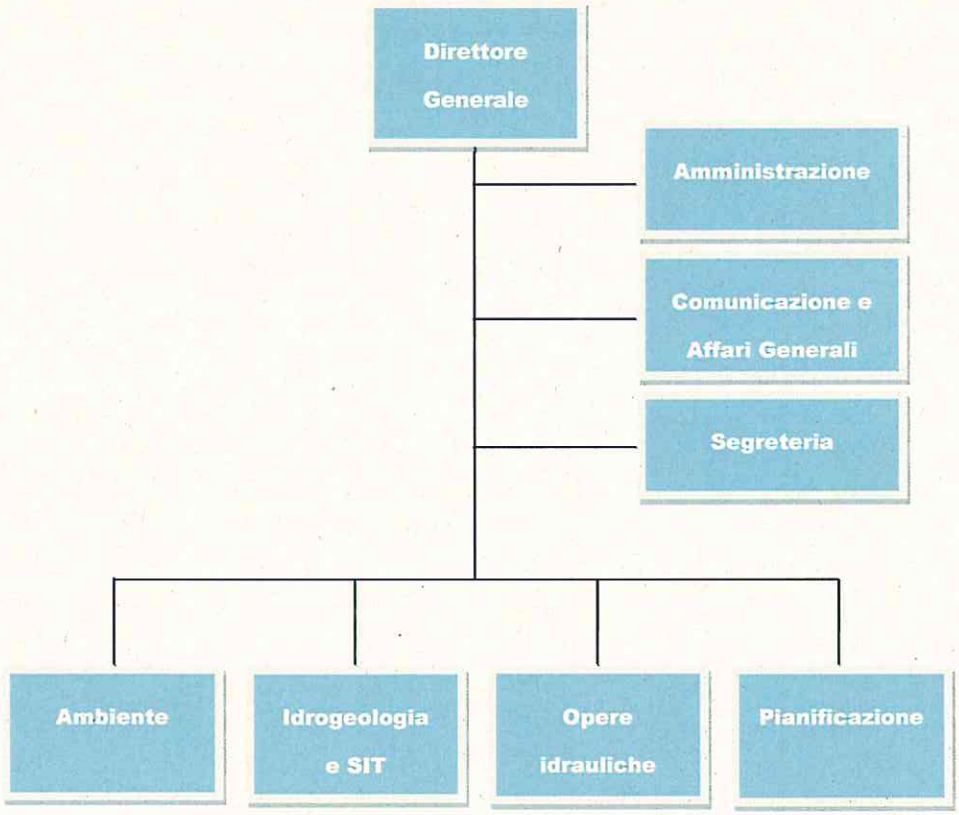
via G. Pepe, 102
30172 Mestre (VE)

I recapiti sono:

e-mail: info@consigliodibacinolv.gov.it
pec: consigliodibacinolv@pec.it
tel.: 041 5040793
fax: 041 3969123

L'amministrazione è dotata di sito internet istituzionale all'indirizzo: www.consigliodibacinolv.gov.it

Organigramma



I locali

I locali adibiti ad ufficio si trovano su due piani di un edificio su corte privata. L'accesso alla corte avviene attraverso un cancello aperto nelle sole ore diurne. L'accesso ai locali avviene attraverso porta blindata posta nella corte, normalmente chiusa e dotata di citofono collegato al centralino telefonico.

Per entrare negli uffici vi sono pertanto un cancello ed una porta di ingresso dotati di apertura elettrica. Non vi sono videocitofoni.

Il direttore ed ogni dipendente ha copia delle chiavi di ingresso. Il dipendente Marco Tabacchi custodisce in cassaforte le specifiche necessarie per la produzione di copie delle chiavi.

L'accesso ai locali per l'esecuzione delle pulizie è consentito all'impresa:

A.F. Multiservice Società cooperativa di Mestre (VE).

Il titolare dell'impresa ha copia delle chiavi che personalmente consegna ai dipendenti di volta in volta incaricati a svolgere il servizio richiesto. Al presente documento è allegata la relativa informativa.

Ruoli e responsabilità

All'interno dell'Ente i ruoli delle figure preposte al trattamento dei dati personali sono i seguenti:

RUOLO	NOME	ATTIVITA' DI COMPETENZA
Titolare del trattamento	Consiglio di Bacino Laguna di Venezia	Decisioni in merito alle finalità, modalità e strumenti del trattamento dati
Responsabile trattamento	Massimiliano Campanelli	Preposto al trattamento dei dati personali
Incaricati trattamento	Boscolo Federica Conchetto Enrico Marafatto Angela Micoli Chiara Tabacchi Marco	

Titolare del trattamento

Al Titolare del trattamento spetta l'onere di individuare e incaricare uno o più Responsabili del Trattamento. La nomina, sottoscritta per accettazione dal Responsabile, avviene per iscritto e contiene in dettaglio le mansioni assegnate. È cura del Titolare conservare in luogo sicuro una copia della lettera di incarico e istruire adeguatamente il Responsabile in merito agli incarichi assegnati.

Tra i compiti non delegabili assegnati al Titolare è prevista la vigilanza sul rispetto da parte del Responsabile degli incarichi a lui assegnati, nonché sulla diligente osservanza delle vigenti disposizioni in materia di trattamento, con particolare riguardo alle misure di sicurezza da adottare.

Il Titolare del trattamento provvederà ad agevolare l'accesso ai dati personali da parte dell'interessato, a fornirgli le informazioni richieste e a ridurre i tempi per il riscontro del richiedente.

Responsabile del trattamento

In ottemperanza all'articolo 29 del D.Lgs. 196/2003, il Titolare del Trattamento può nominare uno o più Responsabili del trattamento con apposita lettera di incarico. I Responsabili devono essere individuati fra soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, con particolare riguardo alla sicurezza dei dati. I Responsabili, pertanto, dovranno adottare tutte le misure idonee ad assicurare l'integrità dei dati oggetto del trattamento, a ridurre i rischi di diffusione o trattamento di dati non consentiti e mantenere in piena efficienza tutti gli strumenti e la struttura organizzativa al fine di perseguire gli scopi dettati dal presente DPsS.

Il Responsabile del trattamento ha il dovere di informare tempestivamente il Titolare di eventuali incidenti o della sopravvenuta mancanza dei requisiti minimi di sicurezza richiesti.

Al Responsabile è conferita possibilità di nominare uno o più Incaricati al trattamento e istruirli adeguatamente per renderli idonei a svolgere le mansioni assegnate.
La nomina del Responsabile si intende a tempo indeterminato e decade o per dimissioni o per revoca comunicata per iscritto o con idonei mezzi informatici dal Titolare del trattamento.

Incaricati del trattamento

Qualora la gestione delle banche dati richieda l'intervento operativo di altri soggetti, il Titolare o il Responsabile possono nominare uno o più Incaricati del trattamento con apposita comunicazione scritta. Sempre per iscritto devono essere specificati i compiti loro assegnati. La lettera di incarico deve essere sottoscritta dal soggetto interessato e sarà cura del Responsabile la sua conservazione o del Titolare (a seconda di chi ha conferito l'incarico) custodire copia della lettera in luogo sicuro.
Loro compito è quello di svolgere gli incarichi assegnati, dettagliatamente specificati nella lettera di incarico, sempre nel pieno rispetto del presente Documento Programmatico sulla Sicurezza. In caso di incidenti o di conoscenza di circostanze che possano far venir meno i requisiti minimi di sicurezza, gli Incaricati dovranno comunicare tempestivamente tale circostanza al Responsabile del trattamento o, in mancanza, al Titolare.
Se non diversamente previsto nella lettera di incarico, gli Incaricati del trattamento vengono nominati a tempo indeterminato e decadono per dimissioni o per revoca.

Nomina dell'amministratore di sistema

Il Responsabile del trattamento o il Titolare possono conferire a uno o più incaricati le mansioni di gestione delle soluzioni informatiche sia hardware che software adottate per la gestione e la tenuta in sicurezza dei dati. La nomina avviene per iscritto e nella lettera di incarico sono dettagliati i compiti assegnati, compreso quello di approntare i mezzi necessari per effettuare le copie di sicurezza dei dati e il loro ripristino in caso di accidentale distruzione.
A tal proposito l'Amministratore di Sistema è abilitato al trattamento (come definito dal Codice) dei dati personali:

- nell'ambito della gestione delle risorse della rete aziendale e dei DB: profili di rete, posta elettronica, fax informatici, file sharing, back-up di dati, monitoraggio traffico di rete, gestione accesso alle aree di rete, monitoraggio dei sistemi in genere;
- nell'ambito della gestione degli applicativi e dei DB: protocollo, contabilità, personale (cedolini stipendi, presenze), atti dell'Ente (delibere, determinazioni, firma digitale) e tutti gli altri applicativi di gestione settoriale;
- nell'ambito della gestione del web.

L'Amministratore di Sistema sovraintende alle risorse del sistema informatico dell'Ente. Opera personalmente e dà direttive in relazione alle operazioni di trattamento dei dati personali cercando di evitare i rischi di distruzione o perdita, anche accidentale dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta, come previsto dal D.Lgs. 196/03.

L'Amministratore di Sistema dovrà tra i suoi compiti:

- agire con profilo di superutente sui server con la finalità di monitorarne lo stato per l'individuazione di eventuali tentativi di accesso fraudolenti;
- disattivare i codici identificativi in caso di perdita della qualità degli stessi o di mancato utilizzo per un periodo superiore a sei mesi;
- proteggere gli elaboratori contro i rischi di intrusione, mediante l'utilizzo di appositi programmi;
- verificare l'efficacia e l'aggiornamento del software antivirus;
- collaborare con i responsabili del trattamento dei dati personali alla stesura e all'aggiornamento del presente documento;
- distruggere i supporti di memorizzazione nel caso non siano più riutilizzabili;
- vigilare sul buon utilizzo dell'hardware e del software dato in dotazione agli utenti;
- regolare le policy di accesso alle risorse della rete in base ai profili assegnati;
- individuare eventuali malfunzionamenti nelle procedure ed attuare le adeguate misure preservando l'integrità dei dati;
- regolare le policy di accesso alle procedure del sistema in base ai profili assegnati;
- gestire i profili di accesso agli applicativi;
- supervisionare i sistemi in modo da garantirne la funzionalità operativa;
- implementazione e integrazione dei flussi informativi;
- gestire il sistema di posta elettronica dell'Ente.

Nomina del custode delle credenziali di autenticazione

Il Responsabile, di concerto con il Titolare, può nominare un custode delle credenziali di autenticazione per l'accesso ai sistemi di elaborazione dati. L'incarico viene assegnato per iscritto e la lettera deve essere conservata in un luogo sicuro da parte del soggetto che conferisce l'incarico.
Le credenziali non dovranno essere divulgate e dovranno essere custodite in luogo sicuro. Spetta al custode definire le modalità di utilizzo delle credenziali di autenticazione in caso di impedimenti o prolungata assenza dell'incaricato alle quali sono state assegnate.

Responsabile della sicurezza

Il responsabile per la sicurezza è il direttore del Consiglio di Bacino.

Il sistema informatico

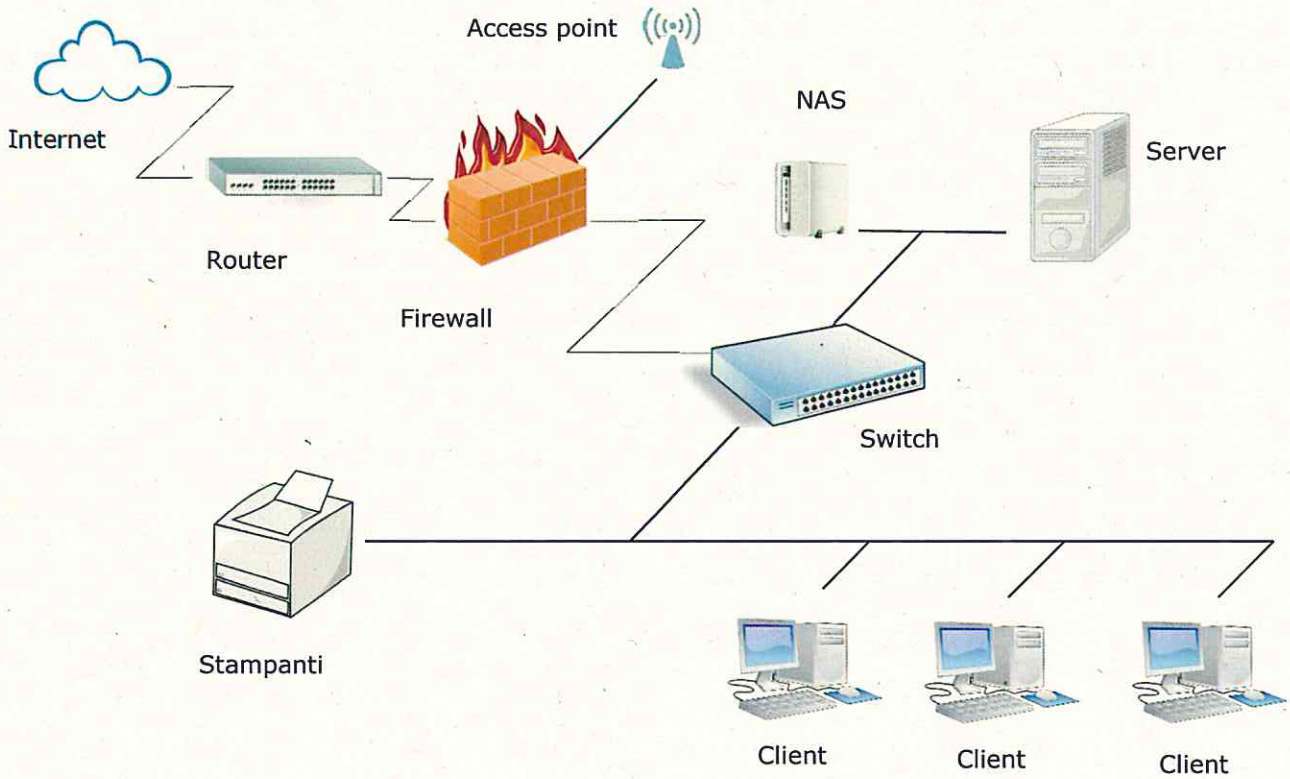
La rete

Il Consiglio di Bacino ha una dotazione informatica composta dalle seguenti apparecchiature:

- 1 server;
- 8 postazioni client fisse e 1 computer portatile;
- 2 stampanti multifunzione di rete ed un plotter di rete;
- NAS di rete per backup;
- access point.

Tutte le apparecchiature sono collegate alla rete ethernet, collegata alla rete internet tramite router in comodato d'uso. La rete informatica dell'Ente è protetta da apposito firewall hardware.

La struttura informatica può essere schematizzata come segue:



Il server fornisce il servizio di autenticazione di rete e i servizi di document server, DNS, DHCP, FTP, mentre il backup è garantito da Acronis che gestisce il salvataggio dei dati verso l'unità esterna NAS e verso cloud.

I sistemi operativi ed applicativi

I sistemi operativi caricati nei server e nelle postazioni di lavoro sono i seguenti: 1 server con Windows Server 2012; 7 clients con Windows 8.1; 1 clients con Windows XP utilizzato solo saltuariamente; 1 portatile con Windows 7. Tutte le apparecchiature sono dotate di software antivirus Symantec EndPoint Protection Small Business Cloud. I principali programmi applicativi installati sono: Microsoft Office, Adobe Acrobat, Autocad Map 3D, Geomedia Professional, Corel Draw.

Un'applicazione con interfaccia web, appositamente installata in remoto su server messi a disposizione dalla società Halley Informatica S.r.l., viene utilizzata per: protocollo, inventario beni, contabilità finanziaria, gestione del personale, gestione delle presenze, contratti, atti amministrativi, albo pretorio.

Il documento programmatico di sicurezza

In base a quanto indicato nell'art.34, il trattamento di dati personali è consentito solo se vengono adottate misure minime di sicurezza, tra cui la tenuta di un DPsS. Il DPsS deve contenere quanto indicato in modo specifico nell'allegato B punto 19 (ora abrogato dalla L. 35/2012).

In dettaglio il Documento Programmatico sulla Sicurezza fornisce informazioni relative a:

a. l'elenco dei trattamenti di dati personali: tipologia di banche dati, tipologia di trattamenti previsti;
b. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
c. l'analisi dei rischi relativi al trattamento dati;
d. le modalità operative con cui si gestiscono le misure minime adottate;
e. un piano di formazione per rendere edotti gli incaricati del trattamento.

Il Documento Programmatico sulla Sicurezza deve essere divulgato e illustrato a tutti gli incaricati nominati con apposite lettere di incarico allegate al presente documento.

Il presente documento è valido per un anno. Trascorso tale termine, e non oltre il 31 Marzo di ogni anno, sarà oggetto di opportune revisioni per adeguarlo ad eventuali modifiche normative, al mutato livello di rischio a cui sono soggetti i dati trattati, ad eventuali assegnazioni o revoche di incarichi, all'utilizzo di nuovi strumenti informatici o in generale a un mutato assetto organizzativo.

Il DPsS è stato redatto e verificato dal Responsabile Trattamento Dati, ed approvato dal Titolare del Trattamento.

Principi per il corretto trattamento dei dati

In conformità a quanto previsto nel Codice, l'azienda si impegna e sensibilizza il proprio personale affinché:

- il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali (art. 2);
- sia ridotta al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità (art. 3);
- i dati personali oggetto di trattamento siano (art.11):
  a) trattati in modo lecito e secondo correttezza;
  b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
  c) esatti e, se necessario, aggiornati;
  d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
  e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.
- i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31).

I dati trattati

Nel presente paragrafo vengono identificati e descritti, nelle schede che seguono, i trattamenti di dati personali e le banche dati all'uopo utilizzate dall'amministrazione, al fine di permetterne una gestione in linea con quanto stabilito nel D.Lgs. 196/2003.

Ai fini della presente trattazione si ricorda che per "*banca dati*" si intende qualsiasi complesso organizzato di dati personali e non, ripartito in una o più unità dislocate in uno o più siti.

CdB_01	PROTOCOLLO

CARATTERISTICHE:
- dati su supporto cartaceo e informatico in formato MySQL
- registrazione e organizzazione di documenti
- dati personali identificativi, sensibili e giudiziari

TIPOLOGIA DI DATI INFORMATICI E CARTACEI:
- atti e documenti emanati dall'amministrazione
- atti e documenti ricevuti dall'amministrazione
- anagrafica soggetti pubblici e privati mittenti e destinatari della corrispondenza
- anagrafica fornitori

TRATTAMENTI:
- raccolta
- archiviazione
- consultazione

ACCESSO INCARICATI:	TRATTAMENTI:
- Campanelli Massimiliano	- Lettura; Scrittura; Cancellazione; Stampa
- Boscolo Federica	- Lettura; Scrittura; Cancellazione; Stampa
- Conchetto Enrico	- Lettura; Scrittura; Cancellazione; Stampa
- Marafatto Angela	- Lettura; Scrittura; Cancellazione; Stampa
- Micoli Chiara	- Lettura; Scrittura; Cancellazione; Stampa
- Tabacchi Marco	- Lettura; Scrittura; Cancellazione; Stampa

COLLOCAZIONE:
Informatica: Hosting su server Halley S.r.l. – Marcon (Ve)
Cartacea: armadi archivio del Consiglio di Bacino Laguna di Venezia

MISURE DI SICUREZZA:
Password: il software è accessibile mediante credenziali personali di accesso

<table>
<tr><th>CdB_02</th><th colspan="2">INVENTARIO BENI</th></tr>
<tr><td colspan="3">CARATTERISTICHE:
- dati su supporto informatico in formato MySQL
- gestione operazioni finanziarie e bilanci
- dati personali identificativi</td></tr>
<tr><td colspan="3">TIPOLOGIA DI DATI INFORMATICI:
- dati relativi ai beni inventariabili</td></tr>
<tr><td colspan="3">TRATTAMENTI:
- gestione contabile dei cespiti</td></tr>
<tr><td colspan="2">ACCESSO INCARICATI:
- Marafatto Angela
- Tabacchi Marco</td><td>TRATTAMENTI:
- Lettura; Scrittura; Cancellazione; Stampa
- Lettura; Scrittura; Cancellazione; Stampa</td></tr>
<tr><td colspan="3">COLLOCAZIONE:
Hosting su server Halley S.r.l. – Marcon (Ve)</td></tr>
<tr><td colspan="3">MISURE DI SICUREZZA:
Password: il software è accessibile, mediante credenziali personali di accesso, solo a:
- Marafatto Angela
- Tabacchi Marco</td></tr>
</table>

CdB_03	CONTABILITÀ FINANZIARIA

CARATTERISTICHE:
- dati su supporto informatico in formato MySQL
- gestione operazioni finanziarie e bilanci
- dati personali identificativi

TIPOLOGIA DI DATI INFORMATICI:
- bilancio
- rendiconto di gestione
- incassi e spese
- gestione beneficiari
- anagrafica fornitori
- cassa economale

TRATTAMENTI:
- elaborazione contabilità finanziaria

ACCESSO INCARICATI:	TRATTAMENTI:
- Campanelli Massimiliano	- Lettura; Scrittura; Cancellazione; Stampa
- Marafatto Angela	- Lettura; Scrittura; Cancellazione; Stampa
- Tabacchi Marco	- Lettura; Scrittura; Cancellazione; Stampa

COLLOCAZIONE:
Hosting su server Halley S.r.l. – Marcon (Ve)

MISURE DI SICUREZZA:
Password: il software è accessibile, mediante credenziali personali di accesso, solo a:
- Campanelli Massimiliano
- Marafatto Angela
- Tabacchi Marco

CdB_04	GESTIONE DEL PERSONALE

CARATTERISTICHE:
- dati su supporto informatico in formato MySQL
- gestione dell'aspetto economico-previdenziale e giuridico del personale
- dati personali identificativi e sensibili

TIPOLOGIA DI DATI INFORMATICI:
- anagrafica del personale
- aspetti contrattuali
- stipendi
- previdenza

TRATTAMENTI:
- registrazione anagrafica personale
- registrazione dati contrattuali
- elaborazione stipendi

ACCESSO INCARICATI:	TRATTAMENTI:
- Tabacchi Marco	- Lettura; Stampa

COLLOCAZIONE:
Hosting su server Halley S.r.l. – Marcon (Ve)

MISURE DI SICUREZZA:
Password: il software è accessibile, mediante credenziali personali di accesso, solo a:
- Tabacchi Marco

CdB_05	GESTIONE PRESENZE

CARATTERISTICHE:

- dati su supporto informatico in formato MySQL
- gestione presenze del personale
- dati personali identificativi

TIPOLOGIA DI DATI INFORMATICI:

- presenze del personale
- assenze e relativi giustificativi

TRATTAMENTI:

- elaborazione presenze

ACCESSO INCARICATI:	TRATTAMENTI:
- Campanelli Massimiliano	- Lettura; Scrittura; Cancellazione; Stampa
- Marafatto Angela	- Lettura; Scrittura; Cancellazione; Stampa
- Tabacchi Marco	- Lettura; Scrittura; Cancellazione; Stampa

COLLOCAZIONE:
Timbrature presenze: server LAN del Consiglio di Bacino Laguna di Venezia
Tutti gli altri dati: hosting su server Halley S.r.l. – Marcon (Ve)

MISURE DI SICUREZZA:
Backup timbrature presenze: ogni giorno su unità NAS
Backup offsite timbrature presenze: backup in cloud
Password: il software è accessibile tramite password solo a:

- Campanelli Massimiliano
- Marafatto Angela
- Tabacchi Marco

<table>
<tr><td>CdB_06</td><td colspan="2">MESSI COMUNALI</td></tr>
<tr><td colspan="3">CARATTERISTICHE:
- dati su supporto informatico in formato MySQL
- registrazione e organizzazione di documenti
- dati personali identificativi, sensibili e giudiziari</td></tr>
<tr><td colspan="3">TIPOLOGIA DI DATI INFORMATICI:
- Dati e/o atti soggetti a pubblicazione all'Albo Pretorio on line</td></tr>
<tr><td colspan="3">TRATTAMENTI:
- archiviazione
- consultazione</td></tr>
<tr><td>ACCESSO INCARICATI:
- Marafatto Angela
- Tabacchi Marco</td><td colspan="2">TRATTAMENTI:
- Lettura; Scrittura; Cancellazione; Stampa
- Lettura; Scrittura; Cancellazione; Stampa</td></tr>
<tr><td colspan="3">COLLOCAZIONE:
Hosting su server Halley S.r.l. – Marcon (Ve)</td></tr>
<tr><td colspan="3">MISURE DI SICUREZZA:
Password: il software è accessibile, mediante credenziali di accesso, a:
- Marafatto Angela
- Tabacchi Marco</td></tr>
</table>

<table>
<tr><td>CdB_07</td><td colspan="2">CONTRATTI</td></tr>
<tr><td colspan="3">CARATTERISTICHE:
- dati su supporto cartaceo e informatico in formato MySQL
- registrazione e organizzazione di documenti
- dati personali identificativi e sensibili</td></tr>
<tr><td colspan="3">TIPOLOGIA DI DATI INFORMATICI E CARTACEI:
- contratti attivati dall'amministrazione</td></tr>
<tr><td colspan="3">TRATTAMENTI:
- raccolta documentazione
- archiviazione
- consultazione</td></tr>
<tr><td>ACCESSO INCARICATI:
- Campanelli Massimiliano
- Marafatto Angela
- Tabacchi Marco</td><td colspan="2">TRATTAMENTI:
- Lettura; Scrittura; Cancellazione; Stampa
- Lettura; Scrittura; Cancellazione; Stampa
- Lettura; Scrittura; Cancellazione; Stampa</td></tr>
<tr><td colspan="3">COLLOCAZIONE:
Informatica: hosting su server Halley S.r.l. – Marcon (Ve).
Cartacea: armadi archivio del Consiglio di Bacino Laguna di Venezia.</td></tr>
<tr><td colspan="3">MISURE DI SICUREZZA:
Password: il software è accessibile, mediante credenziali di accesso, a:
- Campanelli Massimiliano
- Marafatto Angela
- Tabacchi Marco</td></tr>
</table>

CdB_08	**ATTI AMMINISTRATIVI**

CARATTERISTICHE:

- dati su supporto cartaceo e informatico in formato MySQL
- registrazione e organizzazione di documenti
- dati personali identificativi, sensibili e giudiziari

TIPOLOGIA DI DATI INFORMATICI E CARTACEI:

- atti amministrativi emanati dall'amministrazione

TRATTAMENTI:

- redazione documentazione
- archiviazione
- consultazione

ACCESSO INCARICATI:	TRATTAMENTI:
- Campanelli Massimiliano	- Lettura; Scrittura; Cancellazione; Stampa
- Boscolo Federica	- Lettura; Scrittura; Cancellazione; Stampa
- Conchetto Enrico	- Lettura; Scrittura; Cancellazione; Stampa
- Marafatto Angela	- Lettura; Scrittura; Cancellazione; Stampa
- Micoli Chiara	- Lettura; Scrittura; Cancellazione; Stampa
- Tabacchi Marco	- Lettura; Scrittura; Cancellazione; Stampa

COLLOCAZIONE:

Informatica: hosting su server Halley S.r.l. – Marcon (Ve)

Cartacea: armadi archivio del Consiglio di Bacino Laguna di Venezia

MISURE DI SICUREZZA:

Password: il software è accessibile, mediante credenziali di accesso, a:

- Campanelli Massimiliano
- Boscolo Federica
- Conchetto Enrico
- Marafatto Angela
- Micoli Chiara
- Tabacchi Marco

CdB_09	PROCEDIMENTI

CARATTERISTICHE:
- dati su supporto cartaceo e informatico
- registrazione e organizzazione di documenti
- dati personali identificativi, sensibili e giudiziari

TIPOLOGIA DI DATI INFORMATICI E CARTACEI:
- atti e documenti emanati dall'amministrazione
- atti e documenti ricevuti dall'amministrazione
- procedimenti disciplinari
- autorizzazioni allo scarico in fognatura
- progetti del SII relativi a specifiche utenze o ad espropri
- pratiche del Genio Civile per autorizzazioni alla terebrazione di pozzi

TRATTAMENTI:
- raccolta documentazione in ingresso
- elaborazione documenti del procedimento
- archiviazione
- consultazione

ACCESSO INCARICATI:	TRATTAMENTI:
- Campanelli Massimiliano	- Lettura; Scrittura; Cancellazione; Stampa
- Boscolo Federica	- Lettura; Scrittura; Cancellazione; Stampa
- Conchetto Enrico	- Lettura; Scrittura; Cancellazione; Stampa
- Marafatto Angela	- Lettura; Scrittura; Cancellazione; Stampa
- Micoli Chiara	- Lettura; Scrittura; Cancellazione; Stampa
- Tabacchi Marco	- Lettura; Scrittura; Cancellazione; Stampa

COLLOCAZIONE:
Informatica: server LAN del Consiglio di Bacino Laguna di Venezia
Cartacea: armadi archivio del Consiglio di Bacino Laguna di Venezia

MISURE DI SICUREZZA:
Backup: ogni giorno su unità NAS
Backup offsite: backup in cloud
Password: credenziali personali di accesso alla rete

Analisi dei rischi relativi al trattamento dei dati

E' necessario individuare i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutandone le possibili conseguenze e la gravità e ponendoli in correlazione con le misure previste.

Nella Tabella di rischio è individuato l'elenco degli eventi che possono essere causa di danni e che comportano quindi rischi per la sicurezza ed integrità dei dati personali.

In relazione a ciascun evento viene individuata una contromisura da adottare in relazione alla valutazione della gravità dell'evento stesso e alla probabilità stimata che esso si verifichi.

Le componenti di rischio possono essere idealmente suddivise in:

1. rischio legato ad atti di sabotaggio e ad errori umani, da parte del personale appartenente all'organizzazione del Titolare, o di persone che con essa hanno stretti contatti;
2. rischio di guasti tecnici delle apparecchiature, che interessa in particolare gli strumenti elettronici (risorse hardware, software e supporti) e rischio di penetrazione logica nelle reti di comunicazione;
3. rischio di area, che dipende dal luogo dove gli strumenti sono ubicati. Tale rischio è legato sostanzialmente:
   - al verificarsi di eventi distruttivi o alla perdita di dati (incendi, allagamenti, corto circuiti, smarrimento documenti);
   - alla possibilità che terzi malintenzionati accedano nei locali dove si svolge il trattamento (rapine, furti, danneggiamenti da atti vandalici).

TABELLA DI RISCHIO

Evento		Gravità stimata	Probab. stimata	Coeff. di rischio	Misure d'azione per sventurare il rischio e per garantire l'integrità e la disponibilità dei dati
Comportamenti degli operatori	carenza di consapevolezza disattenzione o incuria	8	8	64	Formazione specifica sulle conseguenze di atteggiamenti sbagliati rispetto alle norme di tutela dei dati personali contenute nel codice e rispetto alla corretta custodia dei dati trattati e delle credenziali di autenticazione assegnate.
	comportamenti sleali o fraudolenti	8	1	8	Sottoscrizione della lettera di incarico al trattamento dei dati personali contenente norme di comportamento nell'utilizzo delle risorse informatiche.
	errore materiale	8	6	48	Verifica e controllo da parte dei responsabili dei trattamenti sui comportamenti degli incaricati interni ed esterni. Formazione specifica sull'utilizzo delle risorse informatiche.
Eventi relativi agli strumenti	azione di virus informatici o di codici malefici	8	8	64	Aggiornamento giornaliero dell'antivirus. Corretta gestione dei firewall e adeguato sistema di autenticazione e autorizzazione all'accesso da parte degli incaricati e dei responsabili del trattamento ai dati presenti nella rete interna.
	spamming o altre tecniche di sabotaggio	8	10	80	Adeguato sistema antispam e antivirus su server dedicati di posta elettronica.
	malfunzionamento, indisponibilità o degrado degli strumenti	6	8	48	Periodica verifica dello stato di obsolescenza delle attrezzature informatiche assegnate agli incaricati e conseguente rinnovo o implementazione delle stesse.
	accessi esterni non autorizzati	10	2	20	Aggiornamento mensile dei sistemi operativi dei server e dei PC.

	intercettazione di informazioni in rete	5	2	10	Esecuzione di opportuni backup periodici (giornalieri, settimanali) del server.
Eventi relativi al contesto	accessi non autorizzati a locali/reparti ad accesso ristretto	10	5	50	Formazione specifica sui comportamenti di tutela dei dati quali: chiusura a chiave degli armadi contenenti dati personali, chiusura dei cassetti, chiusura delle porte degli uffici al di fuori del normale orario di lavoro.
	asportazione e furto di strumenti contenenti dati	8	1	8	Installazione porte di ingresso blindate.
	eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	8	1	8	Delocalizzazione dei dati di backup in cloud.
	guasto ai sistemi complementari (impianto elettrico, climatizzazione, ...)	2	7	14	Verifica del corretto funzionamento dei gruppi di continuità a supporto dei server. Periodiche verifiche delle procedure di ripristino dei dati.

La gravità dell'evento viene stimata in ordine di gravità crescente da 1 a 10 punti.
La probabilità che l'evento si verifichi viene stimata in ordine di probabilità crescente da 1 a 10 punti.
Il coefficiente di rischio di ciascun evento si ottiene moltiplicando fra loro i due indici di gravità e probabilità. La scala del coefficiente di rischio va da 1 a 100.

Il grado di rischio più alto, o addirittura elevatissimo, è collegato al trattamento dei dati, sensibili e giudiziari, alla tutela dei quali devono quindi essere dedicate particolari attenzioni, come ad esempio la stesura degli atti utilizzando codici.

Misure Minime adottate per garantire l'integrità e la disponibilità dei dati

Tutti i posti di lavoro del Consiglio di Bacino sono collegati in rete locale e l'accesso agli stessi è consentito previa sottoscrizione della lettera di incarico al trattamento dei dati personali contenente norme di comportamento nell'utilizzo delle risorse informatiche. L'accesso agli applicativi per il trattamento dei dati è preceduto da apposita formazione da parte dell'azienda fornitrice e abilita anche la consultazione della guida di utilizzo del software. La sottoscrizione della lettera di incarico corrisponde all'assunzione di responsabilità civile e penale sull'utilizzo di hardware, software e dati da parte del soggetto utilizzatore.
Come prescritto all'art. 33 del D.Lgs. 196/2003, il CdB Laguna di Venezia si dota delle misure minime di sicurezza, descritte nel dettaglio nel presente paragrafo, atte a garantire:

- la protezione delle aree e dei locali (Misure Minime Fisiche), nei quali si svolge il trattamento dei dati personali;
- la corretta archiviazione e custodia di atti, documenti e supporti contenenti dati personali, sensibili e giudiziari;

- la sicurezza logica, nell'ambito dell'utilizzo degli strumenti elettronici.

La protezione di aree e locali

Per quanto concerne il rischio d'area, legato ad eventi di carattere distruttivo, gli edifici ed i locali nei quali si svolge il trattamento sono protetti come risulta dalla seguente tabella:

Descrizione misura	Note ed indicazioni per la corretta applicazione
Custodia degli archivi cartacei in armadi chiusi a chiave	Tutti i documenti cartacei contenenti dati personali di tipo sensibile e giudiziario sono conservati in armadi dotati di serratura. Sarà compito dell'incaricato che preleva i documenti garantire che i documenti siano riposti, sotto chiave al termine delle operazioni di trattamento.
Dispositivi antincendio	Gli uffici, sono dotati di estintori regolarmente revisionati.
Controllo di operatori esterni addetti alle manutenzioni	Gli addetti alle manutenzioni sono sempre accompagnati dal personale dipendente del Consiglio di Bacino con la finalità di controllarne l'operato.

Custodia e archiviazione di atti, documenti e supporti

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti diversi (ad esempio, CD, fotografie, filmati ecc.), si è provveduto ad istruire gli incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.

Le misure logiche di sicurezza adottate

Sistema di autenticazione

Il sistema di autenticazione informatica viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici, presenti nell'organizzazione del Titolare.

E' impostata e gestita una procedura di autenticazione, che permette di verificare l'identità della persona, e quindi di accertare che la stessa sia in possesso delle credenziali di autenticazione per accedere ad un determinato strumento elettronico.

Per realizzare le credenziali di autenticazione si utilizza il seguente metodo: si associa un codice per l'identificazione dell'incaricato (username), ad una parola chiave riservata (password), conosciuta solamente dall'incaricato, che provvederà ad elaborarla, mantenerla riservata e modificarla trimestralmente.

Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizzano i seguenti criteri:

- ad ogni incaricato esse vengono assegnate e associate individualmente, per cui non è ammesso che due o più incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale;
- è invece ammesso, qualora sia necessario o comunque opportuno, che ad una persona venga assegnata più di una credenziale di autenticazione.

Agli incaricati vengono impartite precise istruzioni in merito ai seguenti punti:

- obbligo di non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza;
- dovere di elaborare in modo appropriato la password, e di conservare la segretezza sulla stessa. Agli incaricati è imposto l'obbligo di provvedere a modificare la password, con la seguente tempistica:
  - immediatamente, non appena viene consegnata loro da chi amministra il sistema;
  - successivamente trimestralmente. Il cambio della password di accesso alla rete e di tutte le applicazioni integrate è imposto ogni tre mesi dal sistema di autenticazione tramite policy. L'utente viene avvisato all'avvicinarsi della scadenza attraverso warning del Sistema Operativo.

Le password sono composte da almeno otto caratteri numerici e alfanumerici oppure, nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri pari al massimo consentito dallo strumento stesso.

- Le password, per maggiore sicurezza, non devono contenere riferimenti agevolmente riconducibili all'interessato, quali date di nascita o nomi dei figli.

La password non deve essere comunicata a nessuno. Nei casi di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe rendersi necessario disporre della password dell'incaricato, per accedere agli strumenti ed ai dati. A tale fine i responsabili chiedono all'amministratore di sistema di sostituire la password dell'incaricato assente, assumendo l'obbligo di comunicare tempestivamente al medesimo l'operazione effettuata e gli accessi avvenuti. L'incaricato, rientrando in servizio, provvederà tempestivamente alla modifica della propria password.

Sistema di autorizzazione

Per quanto concerne le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, si osserva che: si è impostato un sistema di autorizzazione, al fine di circoscrivere le tipologie di dati ai quali gli incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative. L'unica eccezione si ha nei casi in cui il trattamento riguardi solo dati personali destinati alla diffusione: in questo caso non è necessario predisporre alcun sistema di autorizzazione, poiché i dati trattati sono, per definizione, conoscibili da chiunque.

Le autorizzazioni all'accesso vengono rilasciate e revocate dal responsabile del trattamento, ovvero da soggetti da questi appositamente incaricati (amministratore di sistema). Il profilo di autorizzazione può essere studiato per ogni singolo incaricato ovvero per classi omogenee di incaricati.

Periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione: ciò per quanto riguarda l'ambito di trattamento consentito sia ai singoli incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.

Sistema antivirus e antispam

Per quanto riguarda la protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus), vengono adottate le misure sotto descritte.

Il primo aspetto riguarda la protezione dei dati dal rischio di intrusione e dall'azione di programmi di cui all'articolo 615-quinquies del codice penale, aventi per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento (comunemente conosciuti come virus).

A tale fine, l'Ente si è dotato di idoneo software che, in relazione al continuo evolversi dei virus, è sottoposto ad aggiornamento giornaliero. Ulteriore accorgimento di difesa perimetrale è l'impiego di filtri antispam da parte del mailserver esterno alla rete del Consiglio di Bacino.

I messaggi in arrivo sono soggetti ai filtri antispam che reindirizzano automaticamente i messaggi rilevati come spam in apposita cartella. I filtri antispam possono essere personalizzati come segue:

- attivazione di un filtro antispam restrittivo per controllare in modo più rigoroso la posta in blocco.
- creazione di un elenco di mittenti approvati per aggirare il filtro antispam. Si possono approvare mittenti specifici in base all'indirizzo email o al dominio.

Tutti gli incaricati sono stati istruiti, in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere, per minimizzare il rischio di essere contagiati.

Sistema di controllo dei flussi di navigazione internet

Nel rispetto della delibera del Garante n. 13 del 1 marzo 2007 recante le linea guida per posta elettronica e internet, gli accessi degli utenti ad internet sono filtrati da un sistema di controllo centralizzato che consente di inibire l'accesso a determinati siti web che possono essere bloccati singolarmente oppure per categoria di appartenenza. Il sistema permette di attribuire autorizzazioni diverse ad ogni singolo utente delle rete o a gruppi di utenti.

Sistema di monitoraggio del server e dei clients

L'attivazione di un servizio di assistenza esterno per la manutenzione della dotazione software e hardware dell'Ente consente di avere abilitato un servizio da remoto di monitoraggio dello stato del server e delle postazioni di lavoro che permette di effettuare molti controlli; i più interessanti sono:

- patch management;
- manutenzione con accesso remoto;
- reportistica sullo stato di salute dei PC e server;
- controllo della salute dei dischi del server;
- controllo dell'uso dello spazio disco;

- controllo prestazioni;
- controllo accessi falliti (solo server);
- controllo stato dei backup (solo server);
- controllo stato antivirus;
- controllo stato dei servizi;
- controllo delle vulnerabilità dei software.

Sistema di backup dei dati

Il server di rete del Consiglio di Bacino è dotato di un sistema che esegue il salvataggio di tutti i dati in esso presenti con cadenza giornaliera. I salvataggi vengono conservati su unità disco esterna appositamente predisposta.

Per fronteggiare le ipotesi in cui i dati siano colpiti da eventi che possano danneggiarli, o addirittura distruggerli, vengono previsti criteri e modalità tali, da garantire il loro ripristino in termini ragionevoli.

I sistemi e le modalità con cui vengono realizzati i salvataggi sono meglio descritti nel documento allegato "ANALISI DEI RISCHI RELATIVI ALLA CONSERVAZIONE DATI INFORMATICI".

Il sistema adottato si basa su Acronis che fornisce backup e disaster recovery di livello superiore per server Windows e consente di ripristinare in pochi minuti dati e sistemi dopo interruzioni operative o emergenze. Grazie all'esclusiva tecnologia impiegata, l'amministratore di sistema è in grado di ripristinare esattamente il necessario, quando e dove occorre, compresi interi sistemi virtuali e fisici su hardware nuovo o diverso oltre a file, cartelle e oggetti di applicazione granulari.

Il salvataggio dei dati avviene come segue:

- ogni giorno lavorativo viene eseguito il backup incrementale giornaliero.

Il salvataggio appena descritto viene effettuato sia su unità NAS esterna che in cloud per garantire la delocalizzazione dei salvataggi.

Sistema di protezione perimetrale

La protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo 615-ter del codice penale, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, è garantita da misure di sicurezza che impediscono tali accessi ed avviene tramite l'impiego di idonei strumenti elettronici, comunemente ricompresi tra i firewall e i sistemi di autenticazione.

Misure di sicurezza adottate nel trattamento di dati cartacei

Al fine di un corretto trattamento dei dati, tutti i trattamenti su supporto cartaceo devono essere effettuati, sotto la responsabilità del responsabile del trattamento, nel rispetto delle seguenti istruzioni operative:

1. il riciclaggio della carta usata nelle stampe è consentito solo se nella prima stampa non sono contenuti dati personali;
2. la carta stampata che contiene dati personali, prima dello smaltimento, deve essere resa illeggibile, per esempio utilizzando un distruggi-documenti;
3. è fondamentale che i documenti da distruggere siano chiaramente identificati;
4. non devono essere affissi post-it con scritti numeri di telefono o indirizzi con il nome della persona di riferimento;
5. le cartelle cartacee che contengono dati personali non devono essere trasparenti, e non devono consentire la facile identificazione dei dati contenuti legati ad una persona: pertanto utilizzare, quando è possibile, codici al posto di nomi che identifichino le persone di riferimento;
6. documenti che contengono dati personali sensibili e/o giudiziari devono essere tenuti in armadi chiusi a chiave, con individuazione dei soggetti incaricati e che sono in possesso della chiave;
7. non tenere documenti contenenti dati personali incustoditi sulle scrivanie, ma riporli nelle cartelle apposte alla fine del lavoro o in occasione di pause;
8. evitare quando possibile di portare documenti cartacei contenenti dati personali fuori dagli uffici: nel caso adottare tutte le precauzioni opportune per proteggere i dati.

Trattamenti affidati all'esterno della struttura

Qualora il trattamento dei dati venisse affidato anche in parte a soggetti esterni alla struttura, la nomina di tali soggetti avverrà per iscritto mediante apposita lettera di incarico. Sarà cura del Titolare conservare in luogo sicuro copia di tale lettera.

La scelta dei Responsabili del trattamento dati in esterno deve ricadere su soggetti che forniscano i requisiti di affidabilità previsti dal D. Lgs. 196/2003 (art. 29 comma 2).

Sarà compito del Responsabile esterno nominare gli incaricati e impartire loro la dovuta istruzione per garantire il trattamento e la conservazione dei dati in modo puntuale, lecito e sicuro.

Ogni trattamento di dati affidato a terzi è descritto nella relativa scheda dei Dati Trattati, ove viene riportato anche il luogo in cui vengono trattati e conservati i dati. Al Titolare del trattamento spetta il compito di vigilare sull'operato del Responsabile esterno affinché non vengano mai meno le misure minime di sicurezza dei dati.

Dismissione di Pc e Server

In ottemperanza a quanto previsto dal provvedimento del Garante sulla Privacy "Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali" del 13 ottobre 2008 G.U. n. 287

del 9 Dicembre 2008, in occasione del periodico svecchiamento delle postazioni di lavoro le misure idonee a garantire la corretta distruzione dei dati presenti nei dischi dei PC e dei Server non più utilizzabili sono le seguenti:

- qualora i PC/Server vengano riutilizzati donandoli ad associazioni o ad enti che ne facciano richiesta, prima di procedere con la consegna dei dispositivi si procede alla cancellazione sicura dei dati contenuti nei dischi utilizzando un opportuno software che riscrive sequenze di bit annullando di fatto la possibilità di recuperare il contenuto precedentemente memorizzato;
- nel caso in cui il PC/Server venga dismesso in quanto non più efficacemente riutilizzabile, si procede alla distruzione fisica dei dischi.

Controllo generale sullo stato della sicurezza

Al responsabile per la sicurezza, ovvero al Direttore del Consiglio di Bacino, è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

Al fine di verificare l'efficacia delle misure di sicurezza adottate, i responsabili e le persone da questi appositamente incaricati provvedono, anche con controlli a campione, ad effettuare una o più delle seguenti attività:

- verificare l'accesso fisico ai locali dove si svolge il trattamento;
- verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici, mediante l'analisi dei log file, nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni o le operazioni svolte dagli incaricati per il loro tramite. Attraverso questa analisi, che viene effettuata adottando strumenti automatici di reportistica e di sintesi, è possibile individuare i tentativi, riusciti o meno, di accesso al sistema e l'esecuzione di operazioni non corrette, o sospette;
- verificare l'integrità dei dati e delle loro copie di back up;
- verificare la sicurezza delle trasmissioni in rete;
- verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti;
- verificare il livello di formazione degli incaricati.

Almeno ogni tre mesi, si procede ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati in sei mesi.

Dichiarazioni d'impegno e firma

L'originale del presente documento viene custodito presso la sede dell'Ente, per essere esibito in caso di controlli; inoltre sarà pubblicato nel portale del Consiglio di Bacino Laguna di Venezia.
Una sua copia verrà consegnata a chiunque ne faccia richiesta, in relazione all'instaurarsi di un rapporto che implichi un trattamento congiunto di dati personali.

ALLEGATO 1

ANALISI DEI RISCHI RELATIVI ALLA CONSERVAZIONE DEI DATI INFORMATICI

ANALISI DEI RISCHI RELATIVI ALLA CONSERVAZIONE DEI DATI INFORMATICI

Sommario

Il Data Center del CdB Laguna di Venezia

Gli spazi del Consiglio di Bacino adibiti a Data Center sono classificabili come "Server Cabinet" di superficie inferiore a 10 m^2 che ospita server, gruppi di continuità, apparati elettronici per l'immagazzinamento dei dati (storage) e per le comunicazioni (network). Il server cabinet è privo di specifico impianto di raffreddamento, tuttavia il locale è separato solo parzialmente, tramite armadio divisorio, dalla sala dotata di impianto di climatizzazione. La temperatura dell'ambiente rimane normalmente tra i 20 °C e i 25 °C durante tutto l'anno. Il sistema di illuminazione consiste in una lampada, dotata di due tubi al neon da 35 w ciascuno, utilizzata all'occorrenza.

La potenza complessiva utilizzata è nell'ordine dei 2 kW.

Un sistema di generazione e distribuzione dell'energia ridondato, a supporto del sistema di alimentazione elettrica principale, è costituito da due unità UPS che alimentano indipendentemente la doppia alimentazione del server. Il software di controllo dell'UPS gestisce lo spegnimento del server dopo trenta minuti che l'alimentazione della rete elettrica è venuta meno o quando il livello di carica della batteria dell'UPS è inferiore al 20%. Ciò garantisce dal rischio di perdita di dati e dal danneggiamento dei dischi rigidi.

Il locale adibito a DC è conforme a quanto previsto dalle attuali norme sulla sicurezza e salute sul luogo di lavoro dei lavoratori, di cui al d.lgs. n. 81/2008 e successive modificazioni.

Procedure di salvataggio e ripristino dei dati

A fine di conseguire uno standard di sicurezza adeguato nell'elaborazione dei dati sono state adottate delle misure minime tra cui la realizzazione di un sistema di backup dei dati in formato elettronico, efficace e funzionale, in grado di offrire reali garanzie nella gestione di situazioni critiche che potrebbero sorgere in concomitanza di crash di sistemi con conseguenti perdite di dati. Tra le misure adottate per ottenere risultati concreti ed efficaci in termini di sicurezza dei dati, possono essere menzionati:

- l'utilizzo di dischi SAS su server in configurazione RAID 1 e RAID 5 più disco hot-spare;
- l'utilizzo di unità NAS di rete per il backup con dischi in configurazione RAID 1;
- l'adozione di un sistema di backup del server di rete;
- l'adozione di software per il controllo dell'esecuzione dei salvataggi;
- l'impiego di crittografia AES integrata nel sistema di backup garantisce la sicurezza dei dati critici in transito e a destinazione.

Strategie di Backup

Al fine di garantire una maggiore affidabilità dei sistemi di backup, il Consiglio di bacino ha diversificato le strategie di salvataggio differenziandole in base alla specificità dei sistemi. In particolare i backup sono effettuati secondo i seguenti modelli procedurali:

Backup server su NAS: Il backup prevede il salvataggio dei dischi locali del sistema e la tecnologia adottata garantisce anche il ripristino completo del sistema.

Backup off-site: una copia speculare dei dati di backup su NAS viene eseguita in cloud per garantire funzionalità di disaster recovery avanzate.

Backup database: I dati gestiti dalle procedure fornite da Halley per la gestione del protocollo informatico dell'Ente, dell'inventario dei beni, degli atti amministrativi ecc., sono in formato MySQL. Tali databases sono in hosting su server Halley S.r.l. e da quest'ultima società sono garantiti servizi di backup sui dati.
Altri tipi di dati, gestiti attraverso databases sul server locale, vengono posti su disco in appositi files e quindi salvati su unità NAS ed in cloud con le procedure di backup su NAS e off-site.

Server di posta: Il Consiglio di Bacino usufruisce per la posta elettronica dei servizi GMail offerti da Google. Ciascun utente, durante la normale attività lavorativa quotidiana, gestisce attraverso un browser di posta i messaggi relativi agli account che ha in gestione. I databases di posta presenti in ciascuna delle postazioni di lavoro rappresentano una replica dei databases presenti nel mailserver di Google, in cui i messaggi non vengono cancellati una volta che sono stati scaricati dal browser.
I dati sono memorizzati in una rete di data center di Google dislocati geograficamente. Google gestisce i suoi data center utilizzando hardware personalizzato su cui sono in esecuzione un sistema operativo e un file system personalizzati. Ciascuno di questi sistemi è stato ottimizzato per la sicurezza e le prestazioni.
I cluster di calcolo di Google sono progettati pensando alla resilienza e alla ridondanza, eliminando tutti i single point of failure (SPF) e riducendo al minimo l'impatto dei comuni guasti dell'apparecchiatura e i rischi ambientali. L'architettura delle applicazioni e della rete gestita da Google è stata progettata per la massima affidabilità e disponibilità. La piattaforma di calcolo di Google è in grado di reggere il carico presunto di guasti hardware ricorrenti, mentre un affidabile meccanismo di failover del software consente di resistere a queste interruzioni. Tutti i sistemi di Google sono progettati per essere intrinsecamente ridondanti e l'operatività continua dei singoli sottosistemi non dipende da alcun server fisico o logico. I dati vengono replicati più volte sui server attivi in cluster di Google. In questo modo, in caso di malfunzionamento di un computer, i dati restano accessibili su un altro sistema. I dati vengono replicati inoltre in data center secondari per garantire la sicurezza in caso di guasti dei data center (vedere il Libro Bianco sulla Sicurezza

https://static.googleusercontent.com/media/apps.google.com/en/US/files/google-apps-security-and-compliance-whitepaper.pdf e il Certificato sicurezza ISO 27001 allegato).
In merito alla privacy, Google ha certificato la propria adesione ai princìpi di tutela della privacy del "Safe Harbor" in vigore tra Stati Uniti e Unione Europea, come stabilito dal Dipartimento del Commercio degli Stati Uniti in relazione alla raccolta, all'utilizzo e alla conservazione di dati personali dei Paesi dell'Unione europea.

Pianificazione dei salvataggi

Il salvataggio dei dati viene effettuato con il criterio del "minor utilizzo delle risorse da parte dell'utente" e viene concentrato durante le ore notturne (alle ore 23:00 salvataggio su NAS e alle ore 23:02 salvataggio in cloud) dal lunedì al venerdì.

Schedulazione backup server su disco: la strategia di backup adottata prevede che sia effettuato alle ore 23:00 di ogni giorno dal lunedì al venerdì il salvataggio di un'immagine completa del server su un dispositivo esterno locale (NAS).

Schedulazione backup off-site: per quanto riguarda il salvataggio dei dati delocalizzato in cloud viene adottata la stessa pianificazione dei backup del server su disco, ma con orario diverso (23:02).

Verifica dell'esito dei salvataggi

Le operazioni di backup vengono monitorate quotidianamente. Il Sistema di backup è in grado di fornire eventuali warning nel momento in cui il processo di backup locale o in cloud per qualche motivo fallisca.

Conservazione dei dati

L'unità NAS contenente i salvataggi completi ed incrementali viene sempre tenuta in linea. I salvataggi incrementali giornalieri vengono consolidati per rispondere ad un piano di conservazione che consente di recuperare tutti i dati:

- di ogni giorno fino a 7 giorni prima;
- di ogni settimana fino a 4 settimane prima;
- di ogni mese fino a 6 mesi prima.

Il medesimo criterio di conservazione è applicato anche ai dati salvati in data center Acronis Cloud ubicato in Germania.

Ripristino dei dati

Il ripristino dei dati può essere condotto con modalità differenti a seconda della gravità della predita riscontrata. In ogni caso, le procedure di backup adottate, consentono il ripristino dei dati al giorno precedente la perdita degli stessi (Recovery Point Object); il tempo di ripristino dei dati (Recovery Time Object) è invece dell'ordine di qualche ora nel caso si richieda il recupero dei dati infrasettimanali e di un giorno nel caso si richieda il ripristino dei dati risalenti sino al mese precedente. Di seguito vengono descritte le procedure di ripristino da utilizzare nelle diverse situazioni che si possono presentare.

Ripristino di files o cartelle

Il ripristino di file o cartelle di rete accidentalmente cancellati o persi in seguito ad un crash del sistema possono essere recuperati utilizzando il software Acronis e selezionando lo storage contenente i backups nell'apposita sezione "Backup", quindi:

- selezionare la data ed il punto di ripristino cui quale fare riferimento;
- selezionare il tasto "ripristina file/cartelle";
- sfogliare e selezionare i files o le cartelle da recuperare;
- avviare il ripristino.

Ripristino di Database

La procedura di ripristino dei databases prevede il recupero o la messa in linea di dati presenti nei dischi locali del sistema. Per recuperare i dati dai databases di SQL Server occorre accedere alla console "SQL Management" e lanciare la procedura guidata di "Ripristino database" che guiderà l'operatore nella procedura di ripristino. All'operatore verrà richiesto di impostare il set di backup da utilizzare per il ripristino e la data alla quale recuperare i dati.

Ripristino di Posta elettronica

Considerato che il mail server è impostato per conservare tutti i messaggi, compresi quelli già scaricati dal browser mail di ciascun utente, in caso di eliminazione accidentale o perdita di messaggi nel database di posta locale è possibile accede alla casella di posta online per la consultazione dei messaggi persi o per un loro puntuale ripristino ottenibile con un reinoltro degli stessi al medesimo account. In caso di perdita massiva di messaggi è possibile abilitare tra le impostazioni l'opzione "Attiva POP per tutti i messaggi (anche i messaggi già scaricati)" per riscaricare l'intero database presente online.

Disaster Recovery

In caso di danneggiamento irreparabile del sistema è necessario procedere con la ricostruzione dello stesso. In tal caso occorre procedere con la riparazione dell'hardware o alla creazione di una Virtual machine su hardware agnostico e quindi con il ripristino del software.

Il ripristino dell'hardware può rientrare nella procedura di acquisto d'urgenza attraverso MePA inclusa nel regolamento degli acquisti in economia. Per quanto riguarda la parte software la procedura di Disaster Recovery prevede l'utilizzo del software Acronis, attracerso cui:

- selezionare lo storage contenente i backups, nell'apposita sezione "Backup";
- selezionare la data ed il punto di ripristino cui quale fare riferimento;
- selezionare il tasto "ripristina intera macchina";
- il software seleziona automaticamente la macchina originale come macchina di destinazione;

Per il ripristino in un'altra macchina virtuale, fare clic su Macchina di destinazione e procedere nel seguente modo:

- selezionare l'hypervisor (Hyper-V);
- selezionare se eseguire il ripristino di una macchina nuova o una già esistente;
- selezionare l'host e specificare il nome della nuova macchina oppure selezionare una macchina di destinazione esistente;
- fare clic su OK.

Minimizzazione di rischi specifici

Localizzazione

In merito alla possibilità che il sito possa essere colpito da potenziali eventi di allagamento, come avvenuto il 26 settembre 2007, è consigliabile attrezzare il Server Cabinet in modo che tutto l'IT equipment sia sollevato da terra e posizionato su tavolo.

Sistemi di raffreddamento e climatizzazione

Il Server Cabinet, soprattutto durante le giornate estive in cui si manifestano temperature particolarmente elevate, potrebbe essere sottoposto, in coincidenza con gli orari di chiusura degli uffici, a temperature superiori a quelle consigliabili per norma. Si può abbassare il livello di rischio programmando l'azionamento del climatizzatore durante i giorni di chiusura degli uffici che ricadono nei periodi di maggior calura estiva.

Sistemi antincendio

In linea con quanto previsto dalle leggi e normative vigenti, i sistemi antincendio devono poter garantire la sicurezza negli ambienti a uso tecnologico e non. Pertanto, oltre al piano antincendio con mezzi estinguenti

mobili e idranti, è opportuno che il Data Center sia provvisto di una centrale del sistema di rilevazione incendi in grado di coordinare e gestire automaticamente la sensoristica di rilevazione fumi e spegnimento. L'abbassamento del livello di rischio di incendio può essere ottenuto evitando lo stoccaggio di carta e cartone all'interno del Server Cabinet.

Protezione del Data Center

Per aumentare il livello di sicurezza fornito dalle normali procedure adottate per evitare l'accesso indesiderato di persone entro il perimetro di sicurezza esterno ed interno può essere installato un sistema antifurto a protezione del perimetro di sicurezza interno.

Custodia backup dei dati

L'aumento del livello di sicurezza contro la perdita di dati, al fine di fronteggiare l'effetto di possibili eventi calamitosi simultanei nel Data Center e negli eventuali locali destinati alla conservazione delle copie di backup, è stata ottenuta attivando apposito servizio di backup in cloud.

Manutenzione programmata

La riduzione del rischio di interruzione della continuità operativa per malfunzionamento degli apparati elettronici utilizzati per l'elaborazione dei dati è possibile programmando una pulizia periodica (annuale) del server.

ALLEGATO

Certificato sicurezza ISO 27001 Google

MGMT. SYS.
RvA C 466

Certificate

Certificate number: 2012-001
Certified by EY CertifyPoint since:
May 11, 2012

Based on certification examination in conformity with defined requirements in ISO/IEC 17021:2011 and ISO/IEC 27006:2011, the Information Security Management System as defined and implemented by

Google, Inc.*

located in Mountain View, California, United States of America, is compliant with the requirements as stated in the standard:

ISO/IEC 27001:2013

Issue date of certificate: April 15, 2015
Expiration date of certificate: April 14, 2018

EY CertifyPoint will, according to the certification agreement dated February 13, 2015, perform surveillance audits and acknowledge the certificate until the expiration date of the certificate.

**This certificate is applicable for the assets, services and locations as described in the scoping section on the back of this certificate, with regard to the specific requirements for information security as stated in the Statement of Applicability, dated March 5, 2015.*

drs. R. Toppen RA
Director EY CertifyPoint

DIGITAL COPY

MGMT. SYS.
RvA C 466

Google, Inc.
Scope for certificate 2012-001

The scope of this ISO/IEC 27001:2013 certification is bounded by the Google Apps for Work and Google Apps for Education, Google Cloud Platform, Google+, Google Life Sciences, Google Now, Google Analytics and Google Analytics Premium offerings and the data contained or collected by those offerings and specified facilities. The Information Security Management System (ISMS) is centrally managed out of the Google, Inc. headquarters in Mountain View, California, United States of America.

The in-scope applications, systems, people and processes are globally implemented and operated by teams out of an explicit set of offices and data centers that comprise the functional scope as specifically defined in the 'Google ISO 27001 Implementation Manual.' The listing below indicates which offerings by product are included in the scope of the ISMS.

- **Google Apps for Work and Google Apps for Education:** Gmail, Calendar, Drive, Docs, Sheets (including Forms), Slides, Talk, Hangouts, Vault, Sites, Groups, Tasks, Contacts, Admin console, Directory API, Reports API, SAML-based SSO API, Apps Script, Classroom, Inbox by Gmail;
- **Google Cloud Platform:** Compute Engine, App Engine, Cloud SQL, Cloud Storage, Cloud Datastore, BigQuery, Genomics;
- **Google+;**
- **Google Life Sciences:** Baseline Study, BioQuery, Google Life Sciences Study Kit;
- **Google Now;** and
- **Google Analytics and Google Analytics Premium.**

The ISMS mentioned in the above scope is restricted as defined in the 'Google ISO 27001 Implementation Manual', version 2.8, signed on March 5, 2015, by the Senior Manager of Engineering Compliance, as well as the 'Google ISO 27001 Scope and Bounds Assertion' (formal ISMS location listing document), version 1.2, signed on January 23, 2015, by the Senior Manager of Engineering Compliance.

This scope (edition: **March 5, 2015***) is only valid in connection with certificate 2012-001.*

ALLEGATO 2

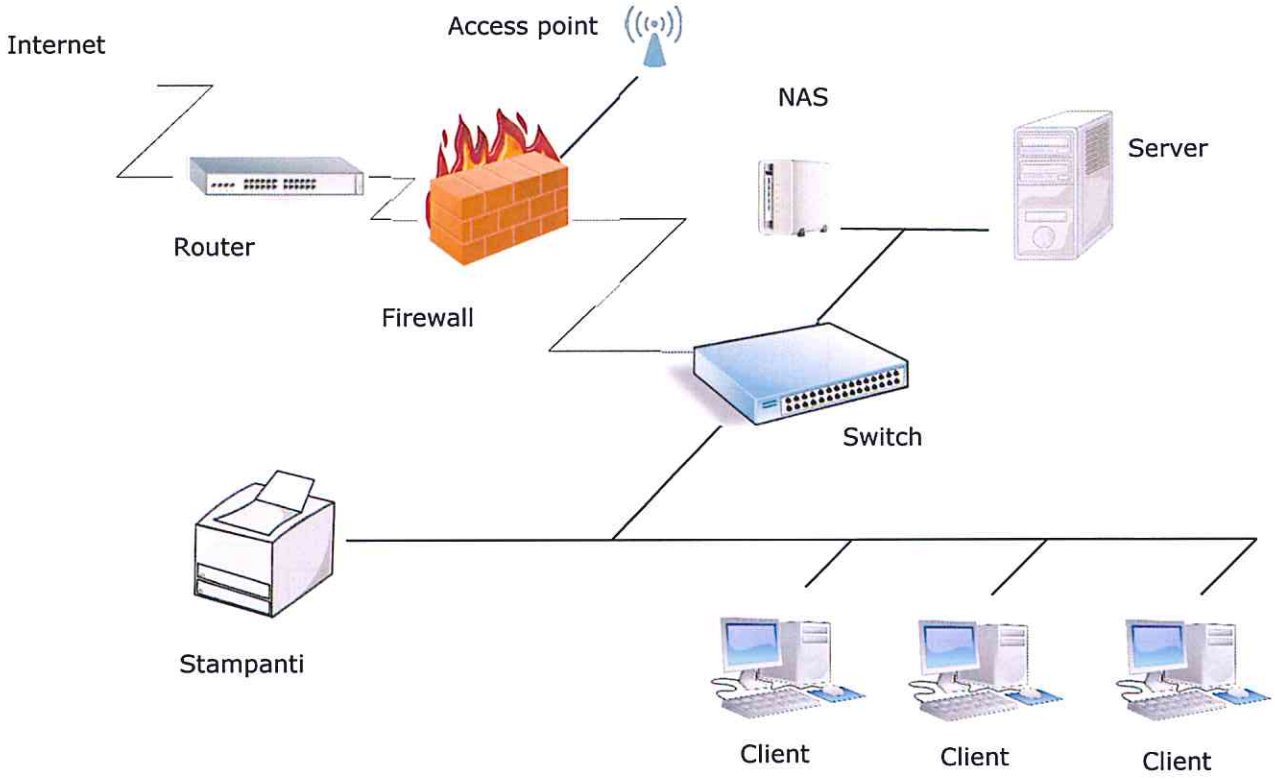
PROCEDURE DI PRIMO INTERVENTO INFORMATICO

PROCEDURE DI PRIMO INTERVENTO INFORMATICO

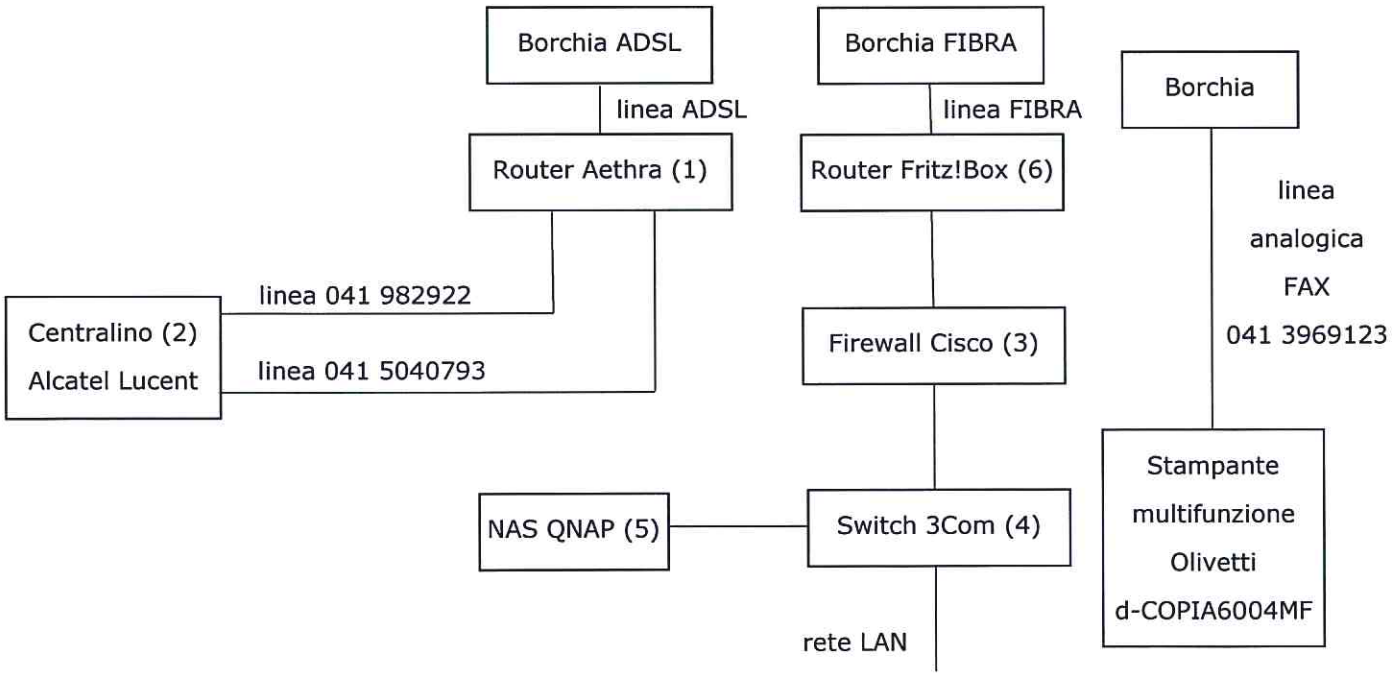
Sommario

COMPONENTI HARDWARE E SCHEMI DI CONNESSIONE

Schema generale rete intranet

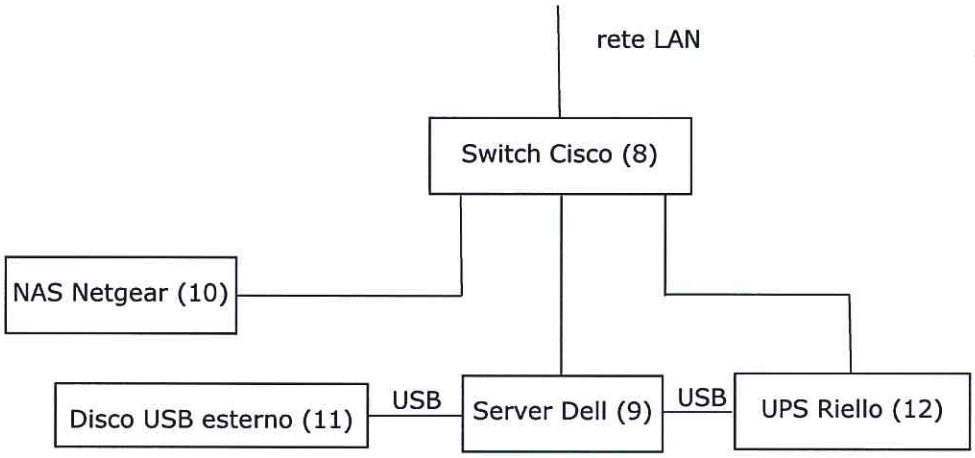


Schema connessioni armadietto primo piano



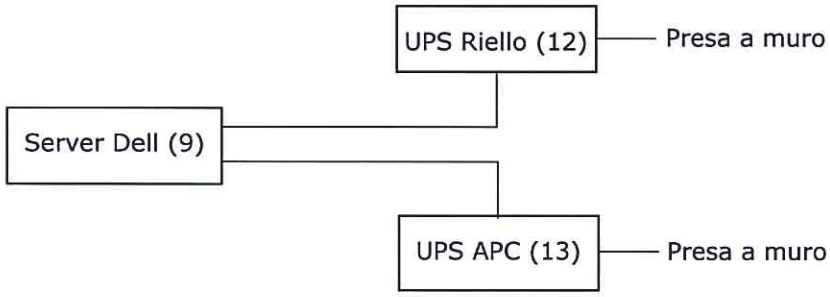
ID	Apparato	Modello	IP WAN	IP LAN
1	Router	Aethra (Fastweb)	93.42.228.127	192.168.179.1
2	Centralino	Alcatel Lucent		192.168.0.246
3	Firewall	Cisco Meraki MX60W	31.197.22.74	192.168.0.250
4	Switch	3Com Baseline 3824		
5	NAS	QNAP		192.168.0.100
6	Router	Fritz!Box (MC-LINK)		192.168.178.1

Schema connessioni del Server Cabinet al piano terra



ID	Apparato	Modello	IP LAN
8	Switch	Cisco SG200-18	192.168.0.30
9	Server	Dell T620	192.168.0.2 - fisico (srvvirt01) 192.168.0.3 - virtuale (srvcdb)
10	NAS	Netgear	192.168.0.4
11	Disco USB esterno	Buffalo HD-LXU3	
12	UPS	Riello MSR3000EVO	192.168.0.29

Schema di alimentazione del Server

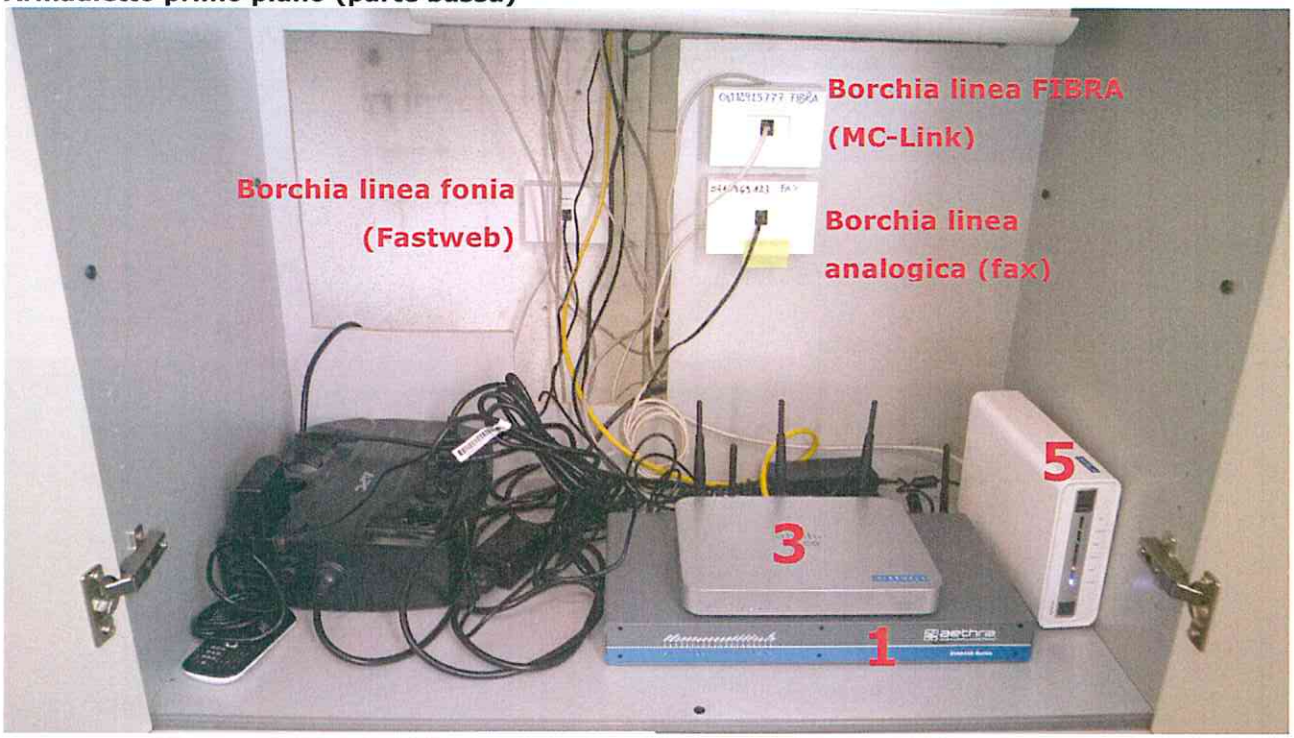


ID	Apparato	Modello	IP LAN
9	Server	Dell T620	192.168.0.2 - fisico (srvvirt01) 192.168.0.3 - virtuale (srvcdb)
12	UPS	Riello MSR3000EVO	192.168.0.29
13	UPS	APC RS 1500	

Identificazione apparecchiature

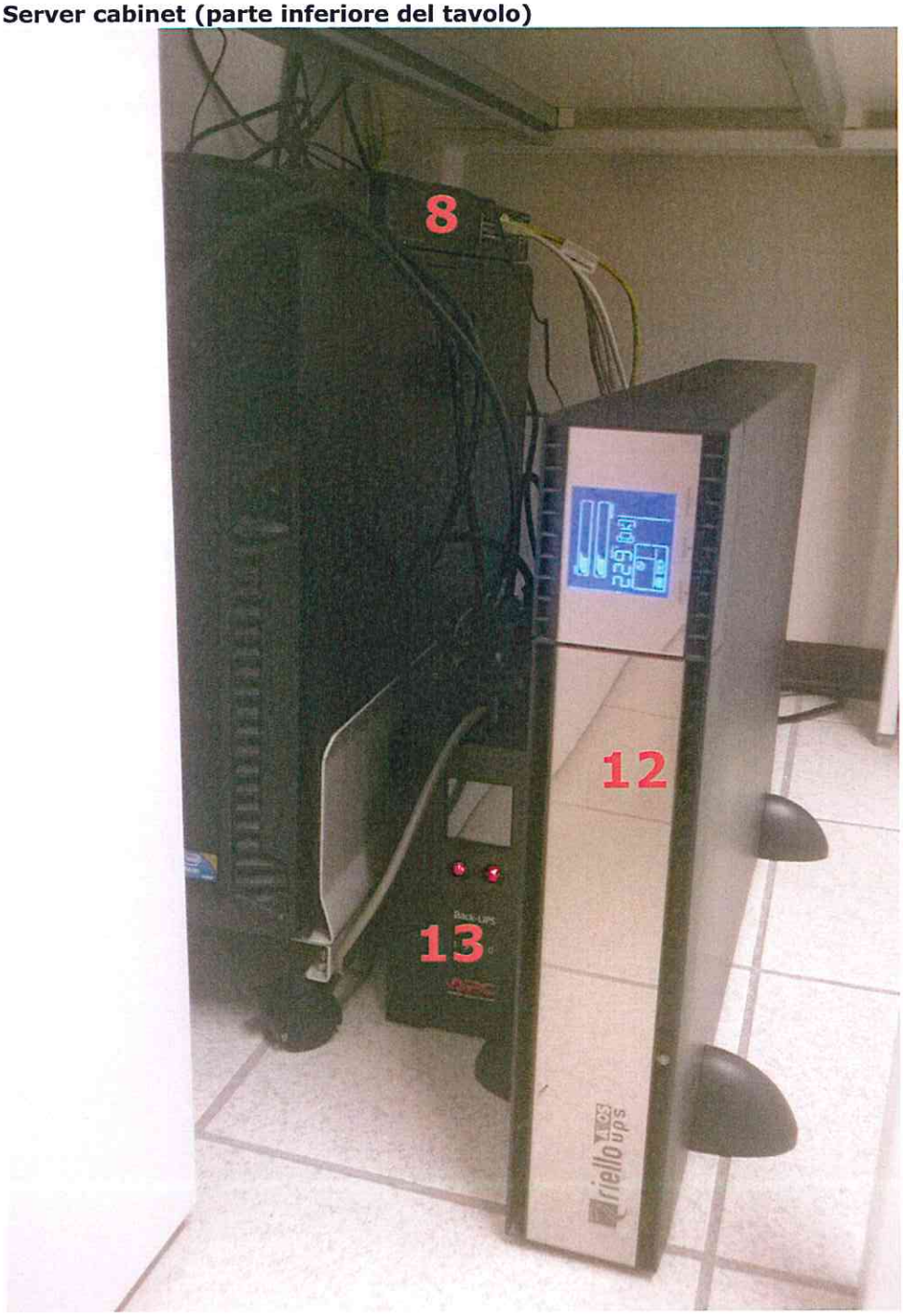
Armadietto primo piano (parte alta)

Armadietto primo piano (parte bassa)



Server cabinet (parte superiore del tavolo)

Server cabinet (parte inferiore del tavolo)



ELENCO DELLE PROCEDURE DI PRIMO INTERVENTO INFORMATICO

Procedure di Primo Intervento informatico (PPI) da attuare in caso di anomalie nel funzionamento dei sistemi informatici o in caso di assenza dell'amministratore di sistema.

PROCEDURA	ANOMALIA
PPI1	Interruzione dei servizi telefonici
PPI2	Interruzione dei servizi internet
PPI3	Interruzione dei servizi di rete o della connessione con il server
PPI4	Verifica dei backup
PPI5	Interruzione del servizio di scarico timbrature
PPI6	Aggiornamento antivirus

PROCEDURA PPI1 - INTERRUZIONE DEI SERVIZI TELEFONICI

Riferimenti contrattuali

Contratto Fastweb	Unlimited Business – ADSL 20/1 - 4 linee

	N. Servizio Clienti	Servizio	Numero linea telefonica	Serial number
Assistenza Fastweb	192 194	ADSL	041 5040793 041 982922	
		Router (comodato)		SV6044EMV2W

	Contatto	Telefono	e-mail
Assistenza Medialink	Antonio Vaccaro	0444 1496106	antonio.vaccaro@medialink.vi.it
	Alvise De Paoli		alvise@medialink.vi.it

Verifiche preliminari

In caso di anomalia nel funzionamento dei servizi telefonici, in primo luogo verificare:

- quadro elettrico al piano terra: tutti gli interruttori dei differenziali devono essere *alzati*;
- router AETHRA dentro l'armadietto al primo piano (unità 1 degli schemi di connessione): deve essere acceso con luci verdi sul frontale; verificare anche il corretto innesto del cavo ADSL (nero proveniente dalla borchia a muro) e BRI1 e BRI2 (cavo voce grigio e cavo voce nero);
- centralino Alcatel Lucent dentro l'armadietto al primo piano (unità 2 degli schemi di connessione): deve essere acceso con luce POWER verde.

Nel caso le verifiche precedenti rilevino delle situazioni non conformi, provvedere a rimediare l'anomalia: sollevare il differenziale staccato, accendere gli apparecchi spenti, innestare correttamente i cavi; nel caso in cui tutto sia regolare, provvedere comunque a riavviare prima il router (staccare l'alimentazione e lasciarlo spento per un minuto) e poi il centralino (tenere premuto per alcuni secondi il tasto di accensione fino allo spegnimento e lasciarlo spento per un minuto). Riaccendere prima il router e dopo un paio di minuti riaccendere anche il centralino.

Attivazione assistenza Fastweb

Se i servizi telefonici non sono stati ripristinati nei passaggi precedenti, chiamare il N. Servizio Clienti con il cellulare di servizio e fornire il numero della linea telefonica per la quale si chiama (041 5040793).

ATTENZIONE: *durante la telefonata a Fastweb segnare il n° operatore ed il n° ticket.*

L'operatore di Fastweb eseguirà una verifica speditiva da remoto per la risoluzione del problema segnalato. Nel caso ciò non fosse sufficiente, chiederà un nominativo ed un numero di telefono di riferimento che potrebbe essere utilizzato dal tecnico che nelle 24 ore successive interviene fisicamente in loco.

Attivazione assistenza Medialink

Se i servizi telefonici non sono stati ripristinati nei passaggi precedenti e l'assistenza Fastweb verifichi che il problema non deriva né dalla linea ADSL né dal Router, è necessario attivare l'assistenza Medialink per far verificare il corretto funzionamento del centralino.

Per consentire l'assistenza sul centralino, è necessario attivare una sessione di assistenza da remoto utilizzando il terminale IDROGEOLOGIA e avviare l'applicazione OmniPCX (icona OMC 921 sul desktop) per la connessione al centralino.

PROCEDURA PPI2 - INTERRUZIONE DEI SERVIZI INTERNET

Riferimenti contrattuali

Contratto MC-Link	Corporate Ultra Broadband NGA Bmg 20/6 Mb/s

	N. verde Clienti Top	N. Impianto	Codice/SN
Assistenza MC-Link	800 969896 (n. verde da fisso) 06 41892434 (da fisso e mobile) CODICE ASSISTENZA: 73304	Codice tecnico	XD257150
		Codice utente	MR7150
		Router	H354.590.30.020.584

	Contatto	Telefono	e-mail
Assistenza Chip Computers su firewall	Enzo Bastianello	041 5950465	support@chipcomputers.it
	Attilio Rifici		
	Nicola Simionato		

Verifiche preliminari

In caso di anomalia nel funzionamento dei servizi internet, in primo luogo verificare:

- quadro elettrico al piano terra: tutti gli interruttori dei differenziali devono essere *alzati*;
- router Fritz!Box dentro l'armadietto al primo piano (unità 6 degli schemi di connessione): deve essere acceso con luce verde fissa sul frontale (LED Power); verificare anche il corretto innesto del cavo LAN (cavo giallo);
- firewall CISCO dentro l'armadietto al primo piano (unità 3 degli schemi di connessione): deve essere acceso con luce POWER verde; verificare anche il corretto innesto del cavi LAN giallo e LAN bianco.

Procedura

Nel caso le verifiche precedenti rilevino delle situazioni non conformi, provvedere a rimediare l'anomalia: sollevare il differenziale staccato, accendere gli apparecchi spenti, innestare correttamente i cavi; nel caso in cui tutto sia regolare, provvedere comunque a riavviare prima il router (staccare l'alimentazione e lasciarlo spento per un minuto) e poi il firewall (staccare l'alimentazione e lasciarlo spento per un minuto).

Attivazione assistenza MC-LinK

Se i servizi internet non sono stati ripristinati nei passaggi precedenti, chiamare il N. verde MC-Link e fornire il codice utente ed il codice assistenza.

ATTENZIONE: *durante la telefonata a MC-Link segnare il n° operatore ed il n° ticket.*

L'operatore di MC-Link eseguirà una verifica speditiva da remoto per la risoluzione del problema segnalato. Nel caso ciò non fosse sufficiente, chiederà un nominativo ed un numero di telefono di riferimento per i successivi contatti.

Attivazione assistenza Chip Computers

Nel caso in cui a seguito della chiamata all'assistenza MC-Link non sia ancora chiara l'origine del problema e comunque non sia sicuramente riconducibile ai servizi offerti da MC-Link (linea in Fibra ottica e/o Router), è consigliabile contattare Chip Computers per far fare una verifica da remoto sul firewall.

PROCEDURA PPI3 - INTERRUZIONE DEI SERVIZI DI RETE O DELLA CONNESSIONE CON IL SERVER

Riferimenti contrattuali

	Contatto	Telefono	e-mail
Assistenza Fastweb (convenzione CONSIP – contratto non ancora avviato)			

Verifiche preliminari

In caso di anomalia nel funzionamento dei servizi di rete LAN (non sono visibili in rete i documenti del server, le stampanti di rete, ecc) in primo luogo verificare se il problema si manifesta solamente da una postazione o da tutte. Se il problema riguarda una sola postazione verificarne il corretto collegamento del cavo LAN e, se necessario, provare a riavviarla; nel caso in cui il problema riguardi tutte le postazioni verificare:

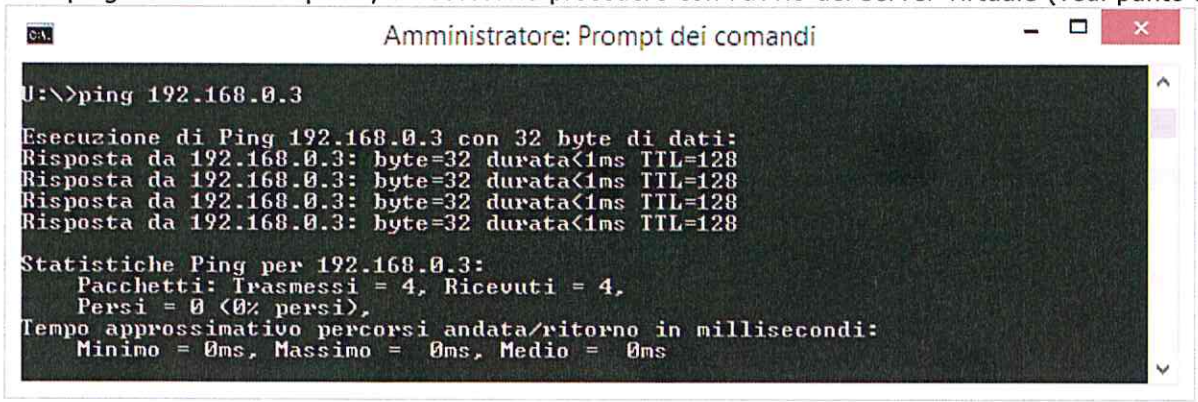
- quadro elettrico al piano terra: tutti gli interruttori dei differenziali devono essere *alzati*;
- gruppi di continuità (unità 12 e 13 degli schemi di connessione): devono essere accesi entrambe;
- server (unità 9 degli schemi di connessione): deve essere acceso sia il server fisico che il server virtuale (vedi punti B, C, D);
- switch: sia lo switch dentro l'armadietto del primo piano (unità 4 degli schemi di connessione) sia lo switch sotto al tavolo del server al piano terra (unità 8 degli schemi di connessione) devono essere accesi (nel primo caso deve essere verde il led "power", nel secondo caso deve essere verde il led "system").

Procedura

A) Nel caso le verifiche precedenti rilevino delle situazioni non conformi, provvedere a rimediare l'anomalia: sollevare il differenziale staccato, accendere gli apparecchi spenti, innestare correttamente i cavi;

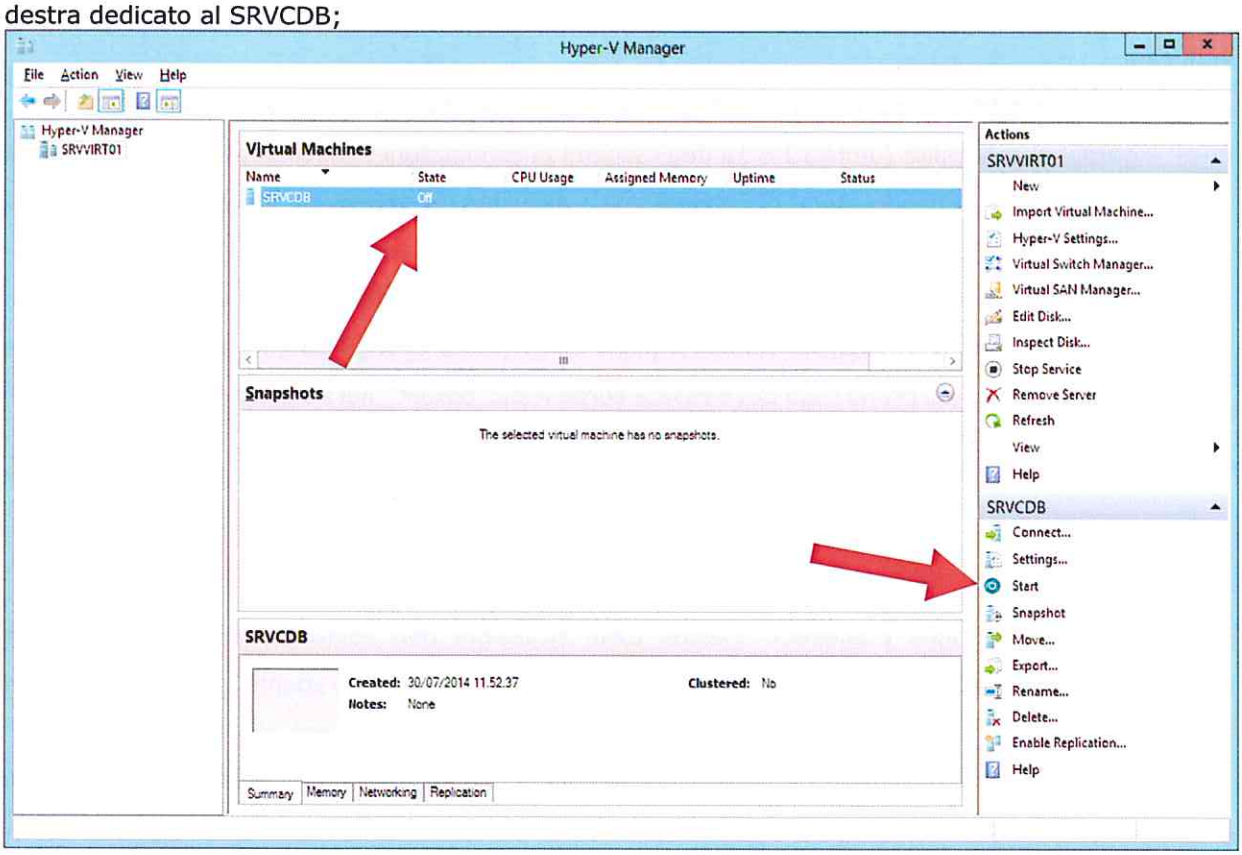
B) nel caso in cui il server fisico sia acceso, per verificare che anche il server virtuale sia acceso, da una qualsiasi postazione avviare Prompt dei comandi ed effettuare il ping digitando: ping 192.168.0.3

Se il ping non ottiene risposta, è necessario procedere con l'avvio del server virtuale (vedi punto D).



C) nel caso in cui il server fisico sia spento, procedere con l'accensione della macchina premendo il tasto power in alto a sinistra del frontale, dopo aver estratto la griglia di protezione (l'avvio del server richiede alcuni minuti di attesa);

D) dopo aver avviato il server fisico è necessario effettuare il login premendo la combinazione di tasti CTRL+ALT+CANC ed inserendo le credenziali. Dopo il login, chiudere l'applicazione Server Manager e avviare Hyper-V Manager dalla barra delle applicazioni, selezionare con un click SRVCDB dal riquadro delle Virtual Machines e, nel caso in cui lo State sia off, premere il tasto Start dal riquadro in basso a destra dedicato al SRVCDB;



E) Chiudere Hyper-V Manager, attivare il riquadro Start a scomparsa in basso a sinistra del Desktop, cliccare Administrator in alto a destra e selezionare Sign Out per uscire. Spegnere il monitor utilizzando il tasto Power;

F) se gli interventi di cui sopra non portano alla risoluzione del problema, provvedere a riavviare prima lo switch (unità 4 degli schemi di connessione) dentro l'armadietto del primo piano (staccare

l'alimentazione e lasciarlo spento per un minuto) e poi lo switch (unità 8 degli schemi di connessione) sotto al tavolo del server al piano terra (staccare l'alimentazione e lasciarlo spento per un minuto).

Attivazione assistenza

Se il problema persiste, contattare Fastweb per far fare una verifica da remoto sul server e sulla rete.

PROCEDURA PPI4 – VERIFICA DEI BACKUP

Almeno una volta a settimana deve essere verificato che il sistema di backup su NAS (unità 10 degli schemi di connessione) ed in cloud sia in esecuzione correttamente.

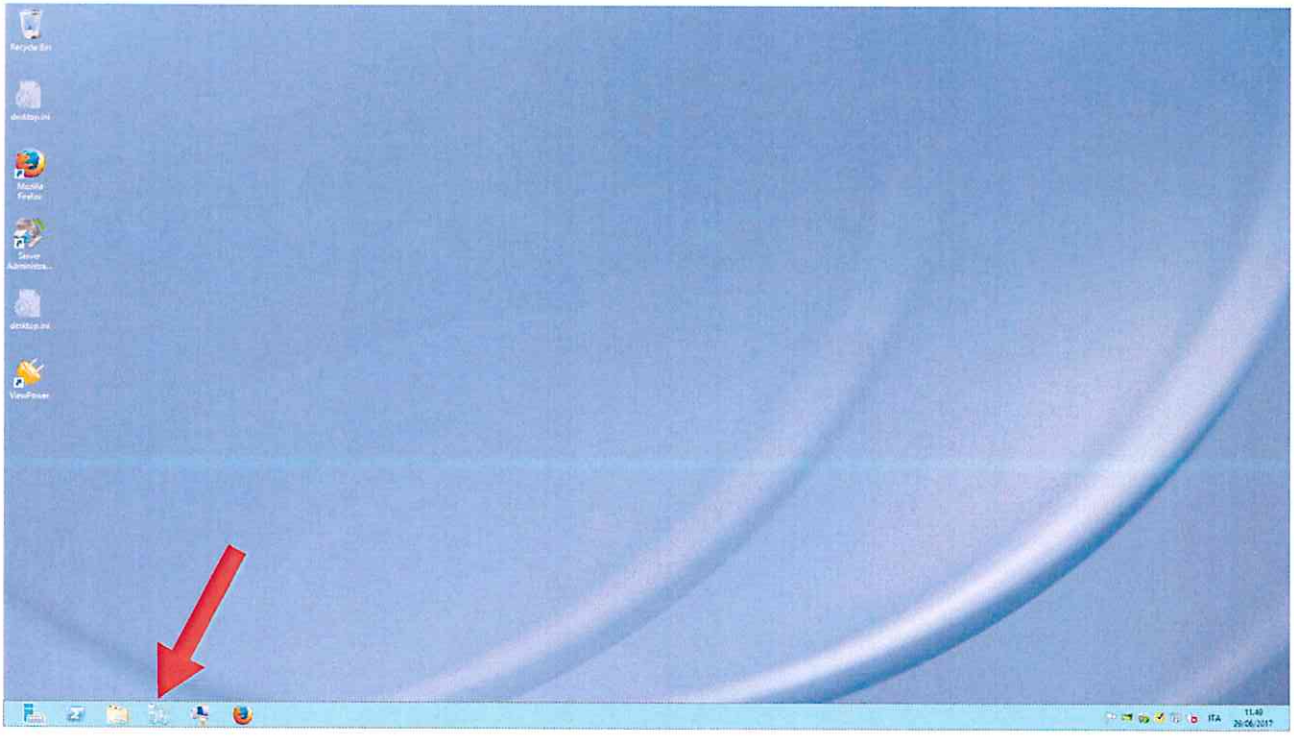
Riferimenti contrattuali

	Contatto	Telefono	e-mail
Assistenza Chip Computers su Acronis	Enzo Bastianello	041 5950465	support@chipcomputers.it
	Attilio Rifici		
	Nicola Simionato		

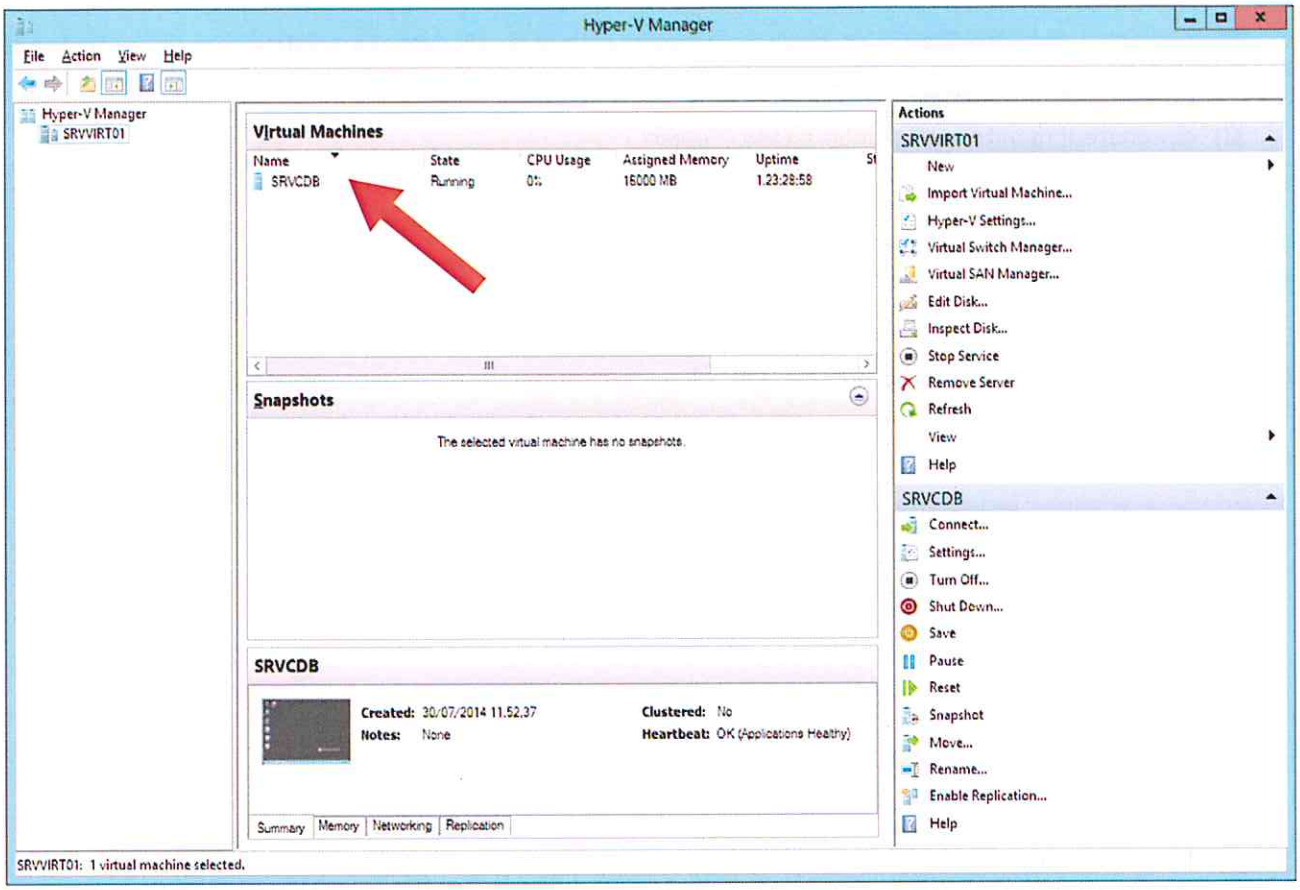
Procedura

A) effettuare il login direttamente sul server fisico premendo la combinazione di tasti CTRL+ALT+CANC ed inserendo le credenziali. Chiudere l'applicazione Server Manager;

B) dalla barra delle applicazioni nel Desktop in basso a sinistra avviare Hyper-V Manager;

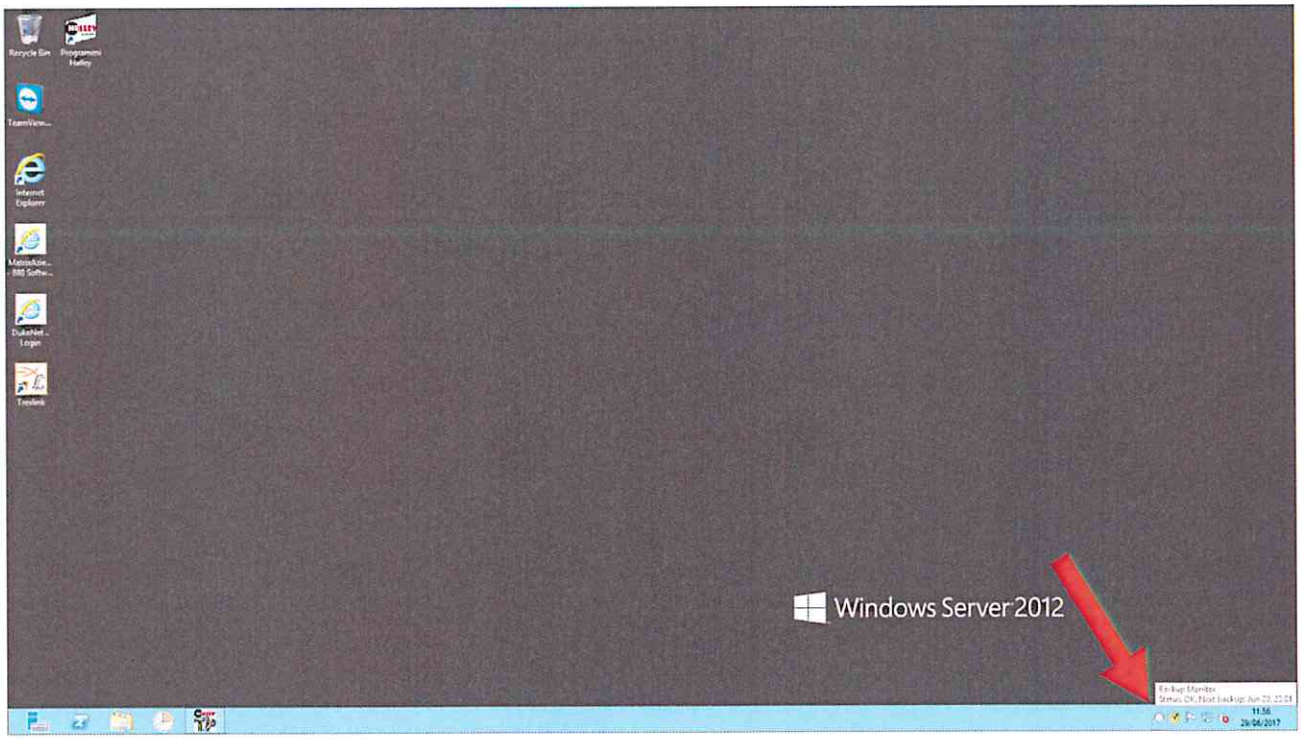


C) avviare con doppio click il server virtuale SRVCDB dal riquadro delle Virtual Machines;



D) passare con il mouse sull'icona di Acronis in basso a destra (la prima a sinistra del gruppo) e verificare che lo stato del backup sia "OK";

E) chiudere la finestra del server virtuale e la finestra di Hyper-V Manager;



F) cliccare il riquadro Start a scomparsa in basso a sinistra, cliccare Administrator in alto a destra e selezionare Sign Out per uscire;

G) spegnere il monitor utilizzando il tasto Power.

Attivazione assistenza

Nel caso in cui lo stato del backup non sia "OK", è necessario attivare l'assistenza di Chip Computers.

PROCEDURA PPI5 - INTERRUZIONE DEL SERVIZIO DI SCARICO TIMBRATURE

Riferimenti contrattuali

	Contatto	Telefono	e-mail
Assistenza Halley Veneto	Nicola Marton	800 400256	

	Contatto	Telefono	e-mail
Assistenza Fastweb (convenzione CONSIP – contratto non ancora avviato)			

Verifiche preliminari

Qualora le timbrature giornaliere non vengano più caricate nell'applicativo delle presenze, in primo luogo bisogna verificare:

- il dispositivo per la lettura del badge: deve essere acceso;
- il quadro elettrico al piano terra: tutti gli interruttori dei differenziali devono essere *alzati*.

Procedura

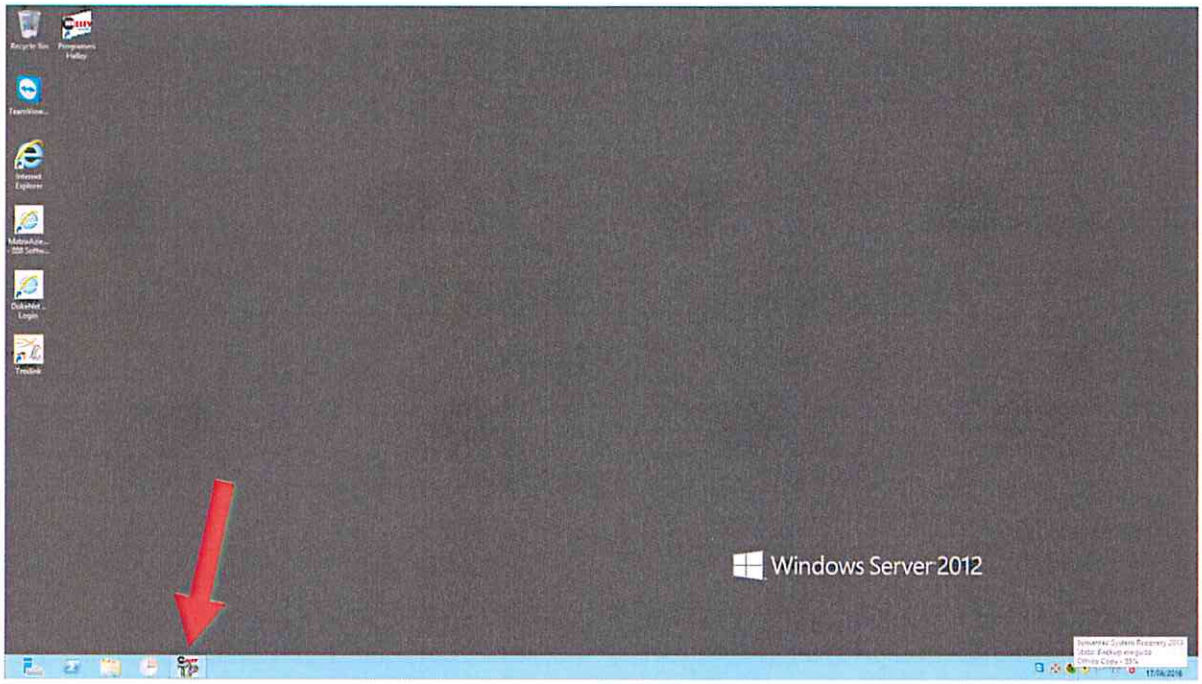
A) Nel caso in cui le verifiche precedenti rilevino delle situazioni non conformi, provvedere a rimediare l'anomalia: sollevare il differenziale staccato, far sostituire la batteria del lettore di badge attivando l'assistenza Halley Veneto;

B) nel caso in cui il problema non sia risolto, avviare da una qualsiasi postazione il Prompt dei comandi ed effettuare il ping al lettore di badge digitando: ping 192.168.0.90

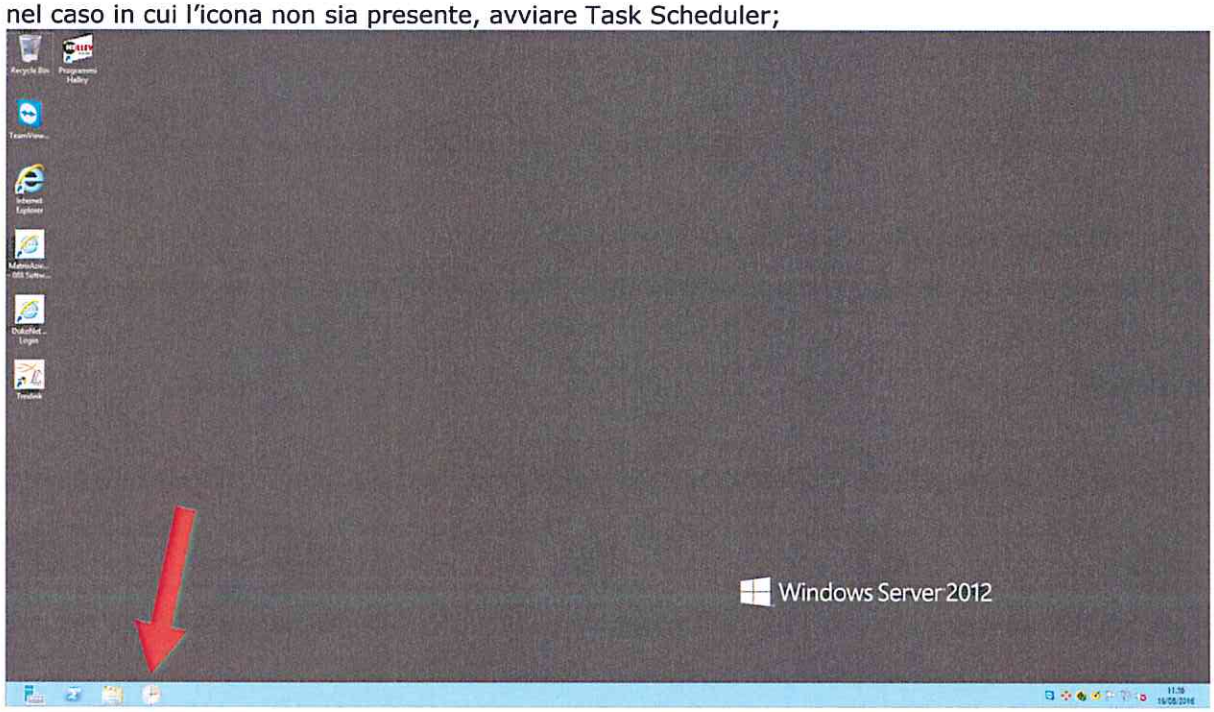
C) se il ping non ottiene risposta, è necessario riavviare lo switch (unità 4 degli schemi di connessione) dentro l'armadietto del primo piano (staccare l'alimentazione e lasciarlo spento per un minuto). Se il problema non si risolve è necessario attivare l'assistenza Chip Computers per fare una verifica da remoto sulla rete;

D) se il ping ottiene risposta, da una qualsiasi postazione avviare Desktop Remoto ed effettuare il login al server SRVCDB;

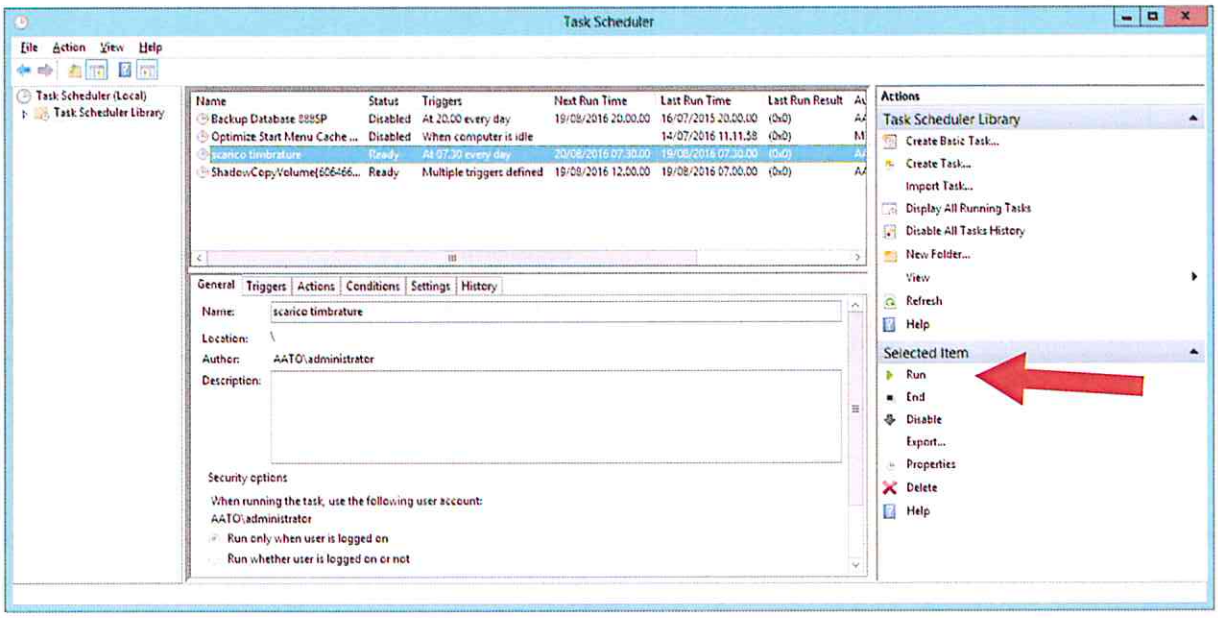
E) verificare la presenza dell'icona Halley nella barra delle applicazioni;



F) nel caso in cui l'icona non sia presente, avviare Task Scheduler;



G) Selezionare Task Scheduler Library e poi selezionare Scarico timbrature, infine cliccare su Run;



H) aspettare circa un minuto affinché avvenga lo scarico delle timbrature e si avvii l'applicativo Halley, quindi ridurre l'applicativo a icona, chiudere Task Scheduler e chiudere la finestra della connessione a SRVCDB.

Attivazione assistenza

Se il problema persiste, contattare Halley Veneto e, nel caso in cui il problema non dipenda dall'applicativo Trexlink o dal lettore di Badge, attivare l'assistenza Fastweb.

PROCEDURA PPI6 – AGGIORNAMENTO ANTIVIRUS

Riferimenti contrattuali

	Contatto	Telefono	e-mail
Assistenza Chip Computers su Symantec antivirus	Enzo Bastianello	041 5950465	support@chipcomputers.it
	Attilio Rifici		
	Nicola Simionato		

Verifiche preliminari

Verificare quotidianamente l'icona di stato del Symantec Endpoint Protection, presente nella barra in basso a destra del desktop, che può assumere 3 diversi aspetti:

1 – stato "protetto" ;

2 – stato di "attenzione" ;

3 – stato di "rischio" .

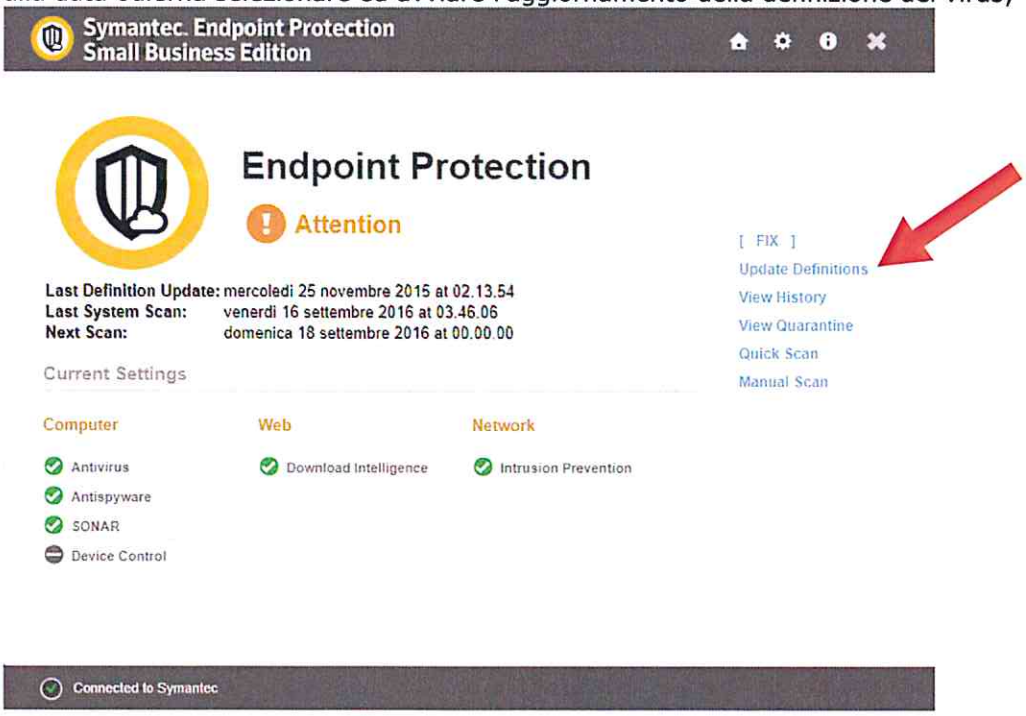
Di norma l'antivirus deve essere nello stato "protetto". Nel caso in cui sia nello stato "attenzione" o "rischio", rifarsi alle procedure sotto riportate.

Procedura

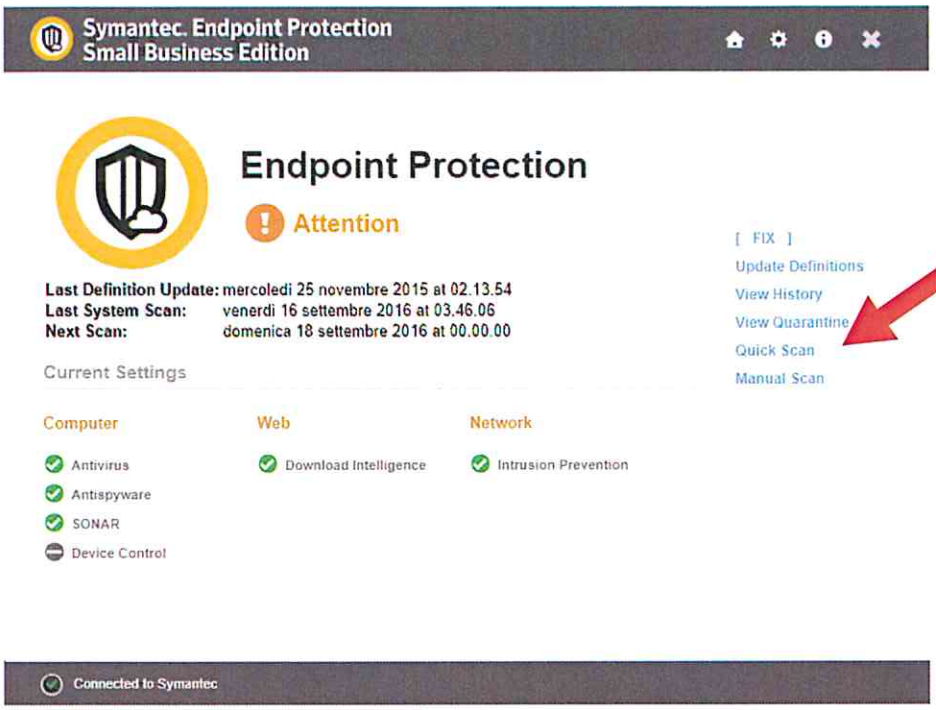
Stato di "attenzione":

A) avviare Symantec Endpoint Protection cliccando due volte l'icona;

B) verificare la data dell'ultimo aggiornamento della definizione dei virus. Nel caso in cui non corrisponda alla data odierna selezionare ed avviare l'aggiornamento della definizione dei virus;



C) selezionare ed avviare una scansione rapida;

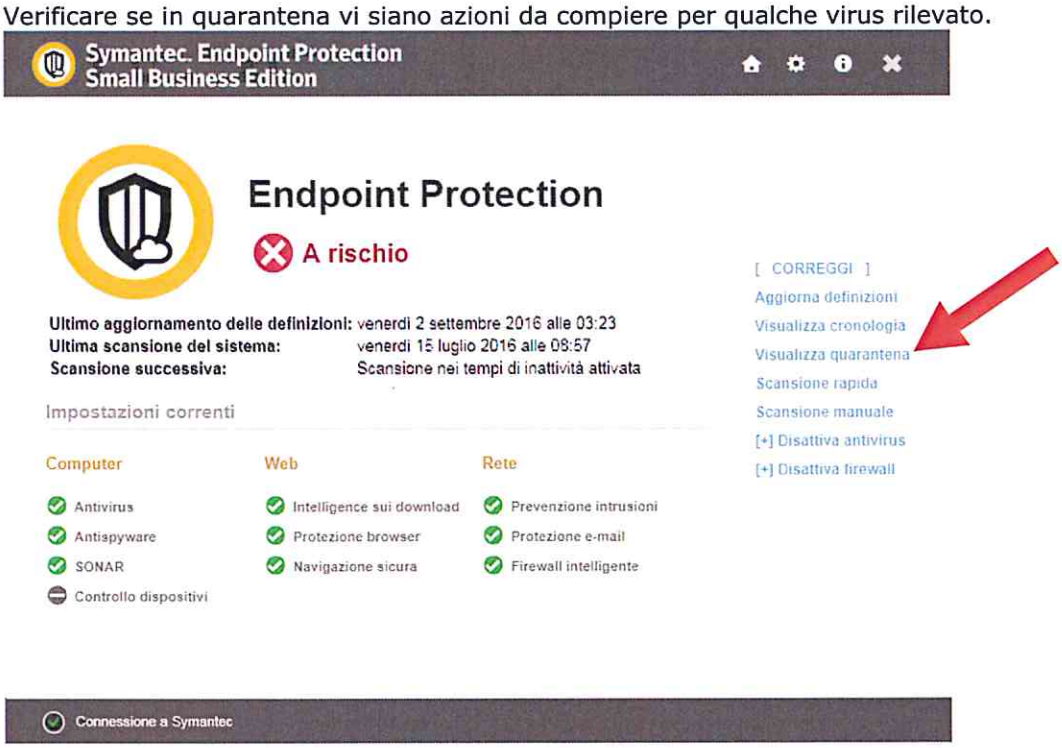


D) selezionare FIX.

Stato di "rischio":

A) Oltre ad espletare la procedura precedente verificare che il client sia connesso alla rete. Nel caso in cui il client non sia connesso alla rete attenersi alla procedura PPI3;

B) Verificare se in quarantena vi siano azioni da compiere per qualche virus rilevato.



Attivazione assistenza

Se il problema persiste, contattare l'assistenza Chip Computers.

ALLEGATO 3

NOMINA DEL RESPONSABILE DEL TRATTAMENTO

CONSIGLIO di BACINO
LAGUNA DI VENEZIA
Ambito Territoriale Ottimale per il servizio idrico integrato

Prot. n. /17 Venezia, 30/06/2017
Resp. Procedimento: Ing. Massimiliano Campanelli
Resp. Istruttoria: Dott. Enrico Conchetto

Oggetto: Lettera di incarico al Responsabile del Trattamento (Art. 29 D.Lgs. 196/03).

In qualità di "Titolare del Trattamento" dei dati personali, conformemente a quanto stabilito dal D.Lgs. n. 196 del 30/06/2003, il Consiglio di Bacino Laguna di Venezia, nella persona del Presidente e legale rappresentante, affida al signor Massimiliano Campanelli l'incarico di Responsabile del Trattamento per la sicurezza dei dati.

In particolare, sono compiti del Responsabile del Trattamento:

- individuare, nominare e incaricare per iscritto gli incaricati del trattamento impartendo loro le idonee istruzioni e vigilandone sul rispetto;
- individuare, nominare e incaricare per iscritto, un "Custode delle Password" qualora vi siano più incaricati del trattamento effettuato con mezzi informatici;
- individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, gli "Amministratori di Sistema";
- redigere ed aggiornare, ad ogni variazione, l'elenco dei sistemi di elaborazione connessi in rete pubblica, nonché l'elenco delle tipologie dei trattamenti effettuati;
- con l'ausilio degli "Amministratori di Sistema" attribuire ad ogni "Utente" (USER) o incaricato un "Codice identificativo personale" (USER–ID) per l'utilizzazione dell'elaboratore, che deve essere individuabile e non riutilizzabile;
- autorizzare i singoli incaricati del trattamento e della manutenzione, nel caso di trattamento di dati sensibili, qualora si utilizzino elaboratori accessibili in rete; per gli stessi dati, qualora il trattamento sia effettuato tramite elaboratori accessibili in rete disponibili al pubblico, saranno oggetto di autorizzazione anche gli strumenti da utilizzare;
- verificare, con l'ausilio degli "Amministratori di Sistema", con cadenza almeno semestrale, l'efficacia dei programmi di protezione antivirus, nonché definire le modalità di accesso ai locali;
- organizzare uno o più incontri formativi per gli incaricati;

Consiglio di Bacino Laguna di Venezia
Via Pepe, 102 - 30172 Mestre – VENEZIA
Tel. 041 5040 793 – Fax 041 3969 123
e-mail: info@consigliodibacinolv.gov.it
pec: consigliodibacinolv@pec.it
website: www.consigliodibacinolv.gov.it
cod. fiscale: 94049070272

- predisporre il Documento Programmatico sulla Sicurezza, in caso ci sia l'obbligo, e portarlo all'approvazione del Comitato Istituzionale e aggiornarlo con frequenza annuale;
- garantire che tutte le misure di sicurezza riguardanti i dati detenuti dall'Ente siano applicate all'interno dello stesso ed eventualmente al di fuori dello stesso, qualora siano cedute a terzi quali Responsabili del Trattamento, tutte o parte delle attività di trattamento;
- informare il titolare nella eventualità che si siano rilevati dei rischi;
- rispondere tempestivamente alle richieste ed eventuali reclami degli interessati, nonché interagire con soggetti che per legge compiono verifiche, controlli o ispezioni sugli adempimenti della privacy.

Il Responsabile del Trattamento dichiara di essere a conoscenza di quanto stabilito dal D.Lgs. n. 196 del 30/06/2003 e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Titolare del Trattamento

Il Responsabile del Trattamento per accettazione

Consiglio di Bacino Laguna di Venezia
Via Pepe, 102 - 30172 Mestre – VENEZIA
Tel. 041 5040 793 – Fax 041 3969 123
e-mail: info@consigliodibacinolv.gov.it
pec: consigliodibacinolv@pec.it
website: www.consigliodibacinolv.gov.it
cod. fiscale: 94049070272

ALLEGATO 4

NOMINA DELL'AMMINISTRATORE DI SISTEMA

CONSIGLIO di BACINO
LAGUNA DI VENEZIA
Ambito Territoriale Ottimale per il servizio idrico integrato

Prot. n. /17 Venezia, 30/06/2017
Resp. Procedimento: Ing. Massimiliano Campanelli
Resp. Istruttoria: Dott. Enrico Conchetto

Oggetto: lettera di incarico di Amministratore di Sistema (D.Lgs. 196/03).

In qualità di "Titolare del Trattamento" dei dati personali, conformemente a quanto stabilito dal D.Lgs. n. 196 del 30/06/2003, il Consiglio di Bacino Laguna di Venezia, nella persona del Presidente e legale rappresentante, affida al signor Massimiliano Campanelli l'incarico di Amministratore di Sistema per i server e PC in uso presso il Consiglio di Bacino Laguna di Venezia.

Le funzioni ad esso attribuite sono:

- definizione delle strategie per la manutenzione ordinaria e straordinaria dei sistemi informatici;
- definizione delle strategie per l'attuazione di adeguati livelli di sicurezza informatica;
- definizione delle strategie di backup;
- gestione e verifica dei backup;
    - messa in sicurezza dei supporti di backup;
    - verifica dei log di backup;
- gestione autorizzazioni accessi alle banche dati ed agli applicativi.
- gestione ordinaria dei Sistemi informatici;
- verifica periodica stato di funzionamento antivirus;
- gestione credenziali utenti (cambio password o blocco utenti).

All'Amministratore di Sistema è consentito l'accesso ai dati personali contenuti nelle banche dati esclusivamente e solo per il tempo necessario per garantire il buon funzionamento.

L'Amministratore di Sistema dichiara di essere a conoscenza di quanto stabilito dal D.Lgs. n. 196 del 30/06/2003 e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.

Il Titolare del trattamento

L'Amministratore di Sistema per accettazione

Consiglio di Bacino Laguna di Venezia
Via Pepe, 102 - 30172 Mestre – VENEZIA
Tel. 041 5040 793 – Fax 041 3969 123
e-mail: info@consigliodibacinolv.gov.it
pec: consigliodibacinolv@pec.it
website: www.consigliodibacinolv.gov.it
cod. fiscale: 94049070272

ALLEGATO 5

ATTI DI DELEGA AL TRATTAMENTO DEI DATI

CONSIGLIO di BACINO
LAGUNA DI VENEZIA
Ambito Territoriale Ottimale per il servizio idrico integrato

Prot. n. /17 Venezia, 30/06/2017
Resp. Procedimento: Ing. Massimiliano Campanelli

Alla Sig.ra Federica Boscolo

Oggetto: Lettera di incarico per il trattamento dei dati personali

Il sottoscritto Massimiliano Campanelli, in qualità di Responsabile del trattamento dei dati personali ex art.29 del D.Lgs. 196/2003, per il Consiglio di Bacino Laguna di Venezia,

- visto il D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali", di seguito definito "Codice";
- premesso che il Consiglio di Bacino Laguna di Venezia è Titolare del trattamento dei dati personali, ai sensi dell'art. 28 del Codice;
- preso atto che l'art. 4, comma 1, lettera h) del Codice definisce "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- atteso che l'art. 30 del Codice, dispone che:
  - le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.
  - la designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito.

in applicazione del Codice, con la presente nomina Federica Boscolo quale Incaricato del trattamento dei dati personali relativamente a quanto di seguito indicato:

TRATTAMENTO	INFORMATIZZATO	CARTACEO
Protocollo	si	si
Atti amministrativi	si	si
Procedimenti	si	si

In qualità dipendente del CdB Laguna di Venezia incaricato del trattamento dei dati, nello svolgimento dei compiti che Le vengono assegnati dovrà:

1. adottare ogni accorgimento necessario ad assicurare l'integrità e riservatezza dei dati dei quali comunque venga a conoscenza;
2. curare che il trattamento avvenga in modo lecito e secondo correttezza, riguardi dati esatti, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati, provvedendo, se necessario, al loro aggiornamento e che la loro raccolta e registrazione avvenga per scopi determinati, espliciti e legittimi;
3. trattare i soli dati sensibili e giudiziari la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati, conservarli fino alla loro restituzione in contenitori muniti di serratura, adottare misure di sicurezza a protezione delle aree e dei locali ove i dati in oggetto vengono trattati e controllare l'accesso delle persone ai locali medesimi dopo l'orario di chiusura degli archivi, provvedendo alla loro identificazione e registrazione;

4. curare l'adozione di accorgimenti necessari alla tutela della riservatezza di dati diversi da quelli sensibili e giudiziari che presentino rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

5. svolgere le attività previste dai trattamenti di cui al punto 1 in conformità ai sistemi di autenticazione e di autorizzazione assegnati.

In ordine alla richieste di accesso agli atti e documenti contenenti dati sensibili, nell'osservanza dei principi, delle misure, modalità e accorgimenti sovra indicati, si rammenta la necessità di procedere alla previa verifica dei requisiti di cui alla L. 241/90.

Si ricordano, di seguito, alcune cautele alle quali dovrà porre particolare attenzione qualora si trovasse ad operare a contatto con il pubblico.

1) nei rapporti di front-office:

- rispetto della **distanza di sicurezza:** per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia;

- **identificazione dell'interessato**: in alcuni casi può essere necessario dover identificare il soggetto interessato per esigenze di garanzia di correttezza del dato da raccogliere, ossia può essere necessario richiedere ed ottenere un documento di identità o di riconoscimento ove si abbia un dubbio sulle modalità di scrittura del nome e cognome dell'interessato o si voglia avere garanzia dell'effettiva identità del soggetto interessato;

- **controllo dell'esattezza del dato:** fare attenzione alla digitazione ed all'inserimento dei dati identificativi dell'interessato, al fine di evitare errori di battitura, che potrebbero creare problemi nella gestione dell'anagrafica e nel prosieguo del processo;

- **obbligo di riservatezza e segretezza:** l'incaricato del trattamento deve mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni del trattamento e deve evitare qualunque diffusione delle informazioni stesse. Si ricorda che l'eventuale violazione dell'obbligo ivi considerato può comportare l'applicazione di sanzioni di natura disciplinare ed una responsabilità civile e penale, secondo quanto previsto dal codice della privacy;

2) cautele da seguire per la corretta comunicazione di dati a soggetti terzi o comunque con strumenti impersonali o che non consentono un controllo effettivo dell'identità del chiamante:

- **controllo dell'identità del richiedente:** nel caso di richieste di comunicazione di dati propri personali (presentate per telefono o per fax) occorre verificare l'identità del soggetto richiedente, attraverso la richiesta di invio, anche via fax, della fotocopia del suo documento di identità; successivamente alla verifica può essere utile comunicare all'interessato un codice personale identificativo, da comunicare al personale per ogni comunicazione impersonale (ad esempio a mezzo telefonico);

- **verifica dell'esattezza dei dati comunicati:** nell'accogliere una richiesta di comunicazione di dati personali, da parte dell'interessato ovvero di un terzo a ciò delegato, occorre fare attenzione che il dato comunicato sia esatto, pertinente, completo e non eccedente rispetto all'attività che si deve espletare, in particolare quando la richiesta viene soddisfatta telefonicamente o attraverso trascrizione da parte dell'operatore, di quanto visualizzato sul monitor; qualora si riscontri che i dati già in proprio possesso non sono aggiornati rispetto ad i dati comunicati dall'interessato, è necessario procedere all'aggiornamento dei

medesimi, previo espletamento delle formalità (richiesta, anche via fax, della fotocopia di un documento di identità) di cui al punto precedente.

3) istruzioni per l'uso degli strumenti del trattamento

- **telefono**: nel caso di richieste di informazioni da parte di organi di amministrazioni pubbliche, o di autorità giudiziarie, può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:
  - chiedere l'identità del chiamante e la motivazione della richiesta;
  - richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;
  - verificare che il numero di telefono dichiarato corrisponda effettivamente a quello del chiamante;
  - procedere immediatamente a richiamare la persona che ha richiesto le informazioni, con ciò accertandosi della identità dichiarata in precedenza;
- **fax**: nell'utilizzare questo strumento occorre prestare attenzione a:
  - digitare correttamente il numero di telefono, cui inviare la comunicazione;
  - controllare l'esattezza del numero digitato prima di inviare il documento;
  - attendere la stampa del rapporto di trasmissione, verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate;
  - qualora vengano trasmessi dati idonei a rivelare lo stato di salute, è necessario inviarli mediante raccomandata A/R al destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati, possano conoscere il contenuto della documentazione inviata;
  - in alcuni casi, può essere opportuno richiedere una telefonata che confermi da parte del destinatario la circostanza della corretta ricezione e leggibilità del contenuto del fax;
- **scanner**: i soggetti che provvedano all'acquisizione in formato digitale della documentazione cartacea (utilizzando ad esempio uno scanner) devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile; qualora vi siano errori di acquisizione ovvero si verifichino anomalie di processo, occorrerà procedere alla ripetizione delle operazioni;
- **distruzione delle copie cartacee**: coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero alla sostituzione della documentazione cartacea con registrazione ottica devono procedere alla distruzione controllata dei supporti cartacei non più occorrenti ovvero che presentino una forma non corretta. Occorre evitare di gettare la documentazione nel cestino della carta straccia senza aver previamente provveduto a rendere inintelligibile il contenuto: si potranno utilizzare apparati distruggi documenti o altri sistemi atti a ciò;
- **riutilizzo dei supporti di memorizzazione contenenti dati sensibili o giudiziari:** i supporti rimovibili (ad esempio pendrive, cd-rom, dvd) che contengano dati sensibili o giudiziari possono essere

riutilizzati solo se i dati precedentemente memorizzati non siano più visionabili da parte di terzi che procedano al riutilizzo del supporto medesimo; in caso contrario, occorrerà distruggere il supporto.

4) istruzioni in tema di sicurezza

a) password o componente riservata d'accesso alla rete:
- la password non deve contenere riferimenti agevolmente riconducibile all'incaricato e dovrebbe essere generata preferibilmente senza un significato compiuto;
- deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;
- l'incaricato è responsabile di ogni utilizzo indebito o non consentito della password di cui sia titolare;

b) back-up:
salvo che non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato, occorre procedere con cadenza almeno settimanale alla effettuazione di copie di sicurezza dei dati personali oggetto di trattamento, utilizzando gli apparati che siano messi a disposizione dell'incaricato e riporre le copie in un contenitore al quale possano accedere solamente soggetti autorizzati;

c) antivirus:
a meno che non siano adottati sistemi automatici di aggiornamento dei sistemi di protezione da programmi antivirus, gli incaricati del trattamento devono procedere all'effettuazione delle operazioni di aggiornamento dei programmi ivi considerati, almeno con cadenza settimanale o quando venga segnalata dal sistema tale esigenza, secondo le istruzioni visualizzate sullo schermo; una volta scaricato l'aggiornamento occorre procedere alla scansione dell'intero sistema per verificare la presenza sull'elaboratore in dotazione di virus;

d) stampanti:
Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento. La stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato;

e) protezione degli strumenti di lavoro:
in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (cd. screen-saver) dotato di password, ovvero, in alternativa, occorrerà porre la machina in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando.

Distinti saluti.

Direttore del CdB
Responsabile del trattamento
.....

Firma per accettazione
Incaricato del trattamento
.....

CONSIGLIO di BACINO
LAGUNA DI VENEZIA
Ambito Territoriale Ottimale per il servizio idrico integrato

Prot. n. /17 Venezia, 30/06/2017
Resp. Procedimento: Ing. Massimiliano Campanelli

Al Sig. Massimiliano Campanelli

Oggetto: Lettera di incarico per il trattamento dei dati personali

In qualità di "Titolare del Trattamento" dei dati personali, il Consiglio di Bacino Laguna di Venezia, nella persona del Presidente e legale rappresentante,

- visto il D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali", di seguito definito "Codice";
- premesso che il Consiglio di Bacino Laguna di Venezia è Titolare del trattamento dei dati personali, ai sensi dell'art. 28 del Codice;
- preso atto che l'art. 4, comma 1, lettera h) del Codice definisce "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- atteso che l'art. 30 del Codice, dispone che:
  - le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.
  - la designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito.

in applicazione del Codice, con la presente nomina il signor Massimiliano Campanelli quale Incaricato del trattamento dei dati personali relativamente a quanto di seguito indicato:

TRATTAMENTO	INFORMATIZZATO	CARTACEO
Protocollo	si	si
Contabilità finanziaria	si	no
Gestione presenze	si	no
Contratti	si	si
Atti amministrativi	si	si
Procedimenti	si	si

In qualità di direttore del CdB Laguna di Venezia incaricato del trattamento dei dati, nello svolgimento dei compiti che Le vengono assegnati dovrà:

1. adottare ogni accorgimento necessario ad assicurare l'integrità e riservatezza dei dati dei quali comunque venga a conoscenza;
2. curare che il trattamento avvenga in modo lecito e secondo correttezza, riguardi dati esatti, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati, provvedendo, se necessario, al loro aggiornamento e che la loro raccolta e registrazione avvenga per scopi determinati, espliciti e legittimi;
3. trattare i soli dati sensibili e giudiziari la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati, conservarli fino alla loro restituzione in contenitori muniti di serratura, adottare misure di sicurezza a protezione delle aree e dei locali ove i dati in oggetto vengono trattati e controllare l'accesso delle persone ai locali medesimi dopo l'orario di chiusura degli archivi, provvedendo alla loro identificazione e registrazione;

4. curare l'adozione di accorgimenti necessari alla tutela della riservatezza di dati diversi da quelli sensibili e giudiziari che presentino rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

5. svolgere le attività previste dai trattamenti di cui al punto 1 in conformità ai sistemi di autenticazione e di autorizzazione assegnati.

In ordine alla richieste di accesso agli atti e documenti contenenti dati sensibili, nell'osservanza dei principi, delle misure, modalità e accorgimenti sovra indicati, si rammenta la necessità di procedere alla previa verifica dei requisiti di cui alla L. 241/90.

Si ricordano, di seguito, alcune cautele alle quali dovrà porre particolare attenzione qualora si trovasse ad operare a contatto con il pubblico.

1) nei rapporti di front-office:

- rispetto della **distanza di sicurezza:** per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia;

- **identificazione dell'interessato**: in alcuni casi può essere necessario dover identificare il soggetto interessato per esigenze di garanzia di correttezza del dato da raccogliere, ossia può essere necessario richiedere ed ottenere un documento di identità o di riconoscimento ove si abbia un dubbio sulle modalità di scrittura del nome e cognome dell'interessato o si voglia avere garanzia dell'effettiva identità del soggetto interessato;

- **controllo dell'esattezza del dato:** fare attenzione alla digitazione ed all'inserimento dei dati identificativi dell'interessato, al fine di evitare errori di battitura, che potrebbero creare problemi nella gestione dell'anagrafica e nel prosieguo del processo;

- **obbligo di riservatezza e segretezza:** l'incaricato del trattamento deve mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni del trattamento e deve evitare qualunque diffusione delle informazioni stesse. Si ricorda che l'eventuale violazione dell'obbligo ivi considerato può comportare l'applicazione di sanzioni di natura disciplinare ed una responsabilità civile e penale, secondo quanto previsto dal codice della privacy;

2) cautele da seguire per la corretta comunicazione di dati a soggetti terzi o comunque con strumenti impersonali o che non consentono un controllo effettivo dell'identità del chiamante:

- **controllo dell'identità del richiedente:** nel caso di richieste di comunicazione di dati propri personali (presentate per telefono o per fax) occorre verificare l'identità del soggetto richiedente, attraverso la richiesta di invio, anche via fax, della fotocopia del suo documento di identità; successivamente alla verifica può essere utile comunicare all'interessato un codice personale identificativo, da comunicare al personale per ogni comunicazione impersonale (ad esempio a mezzo telefonico);

- **verifica dell'esattezza dei dati comunicati:** nell'accogliere una richiesta di comunicazione di dati personali, da parte dell'interessato ovvero di un terzo a ciò delegato, occorre fare attenzione che il dato comunicato sia esatto, pertinente, completo e non eccedente rispetto all'attività che si deve espletare, in particolare quando la richiesta viene soddisfatta telefonicamente o attraverso trascrizione da parte dell'operatore, di quanto visualizzato sul monitor; qualora si riscontri che i dati già in proprio possesso non sono aggiornati rispetto ad i dati comunicati dall'interessato, è necessario procedere all'aggiornamento dei

medesimi, previo espletamento delle formalità (richiesta, anche via fax, della fotocopia di un documento di identità) di cui al punto precedente.

3) istruzioni per l'uso degli strumenti del trattamento

- **telefono**: nel caso di richieste di informazioni da parte di organi di amministrazioni pubbliche, o di autorità giudiziarie, può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:
  - chiedere l'identità del chiamante e la motivazione della richiesta;
  - richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;
  - verificare che il numero di telefono dichiarato corrisponda effettivamente a quello del chiamante;
  - procedere immediatamente a richiamare la persona che ha richiesto le informazioni, con ciò accertandosi della identità dichiarata in precedenza;
- **fax**: nell'utilizzare questo strumento occorre prestare attenzione a:
  - digitare correttamente il numero di telefono, cui inviare la comunicazione;
  - controllare l'esattezza del numero digitato prima di inviare il documento;
  - attendere la stampa del rapporto di trasmissione, verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate;
  - qualora vengano trasmessi dati idonei a rivelare lo stato di salute, è necessario inviarli mediante raccomandata A/R al destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati, possano conoscere il contenuto della documentazione inviata;
  - in alcuni casi, può essere opportuno richiedere una telefonata che confermi da parte del destinatario la circostanza della corretta ricezione e leggibilità del contenuto del fax;
- **scanner**: i soggetti che provvedano all'acquisizione in formato digitale della documentazione cartacea (utilizzando ad esempio uno scanner) devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile; qualora vi siano errori di acquisizione ovvero si verifichino anomalie di processo, occorrerà procedere alla ripetizione delle operazioni;
- **distruzione delle copie cartacee**: coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero alla sostituzione della documentazione cartacea con registrazione ottica devono procedere alla distruzione controllata dei supporti cartacei non più occorrenti ovvero che presentino una forma non corretta. Occorre evitare di gettare la documentazione nel cestino della carta straccia senza aver previamente provveduto a rendere inintelligibile il contenuto: si potranno utilizzare apparati distruggi documenti o altri sistemi atti a ciò;
- **riutilizzo dei supporti di memorizzazione contenenti dati sensibili o giudiziari:** i supporti rimovibili (ad esempio pendrive, cd-rom, dvd) che contengano dati sensibili o giudiziari possono essere

riutilizzati solo se i dati precedentemente memorizzati non siano più visionabili da parte di terzi che procedano al riutilizzo del supporto medesimo; in caso contrario, occorrerà distruggere il supporto.

4) istruzioni in tema di sicurezza

a) password o componente riservata d'accesso alla rete:
- la password non deve contenere riferimenti agevolmente riconducibile all'incaricato e dovrebbe essere generata preferibilmente senza un significato compiuto;
- deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;
- l'incaricato è responsabile di ogni utilizzo indebito o non consentito della password di cui sia titolare;

b) back-up:
salvo che non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato, occorre procedere con cadenza almeno settimanale alla effettuazione di copie di sicurezza dei dati personali oggetto di trattamento, utilizzando gli apparati che siano messi a disposizione dell'incaricato e riporre le copie in un contenitore al quale possano accedere solamente soggetti autorizzati;

c) antivirus:
a meno che non siano adottati sistemi automatici di aggiornamento dei sistemi di protezione da programmi antivirus, gli incaricati del trattamento devono procedere all'effettuazione delle operazioni di aggiornamento dei programmi ivi considerati, almeno con cadenza settimanale o quando venga segnalata dal sistema tale esigenza, secondo le istruzioni visualizzate sullo schermo; una volta scaricato l'aggiornamento occorre procedere alla scansione dell'intero sistema per verificare la presenza sull'elaboratore in dotazione di virus;

d) stampanti:
Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento. La stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato;

e) protezione degli strumenti di lavoro:
in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (cd. screen-saver) dotato di password, ovvero, in alternativa, occorrerà porre la machina in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando.

Distinti saluti.

Presidente del CdB
Titolare del trattamento
.....

Firma per accettazione
Responsabile del trattamento
.....

CONSIGLIO di BACINO
LAGUNA DI VENEZIA
Ambito Territoriale Ottimale per il servizio idrico integrato

Prot. n. /17 Venezia, 30/06/2017
Resp. Procedimento: Ing. Massimiliano Campanelli

Al Sig. Enrico Conchetto

Oggetto: Lettera di incarico per il trattamento dei dati personali

Il sottoscritto Massimiliano Campanelli, in qualità di Responsabile del trattamento dei dati personali ex art.29 del D.Lgs. 196/2003, per il Consiglio di Bacino Laguna di Venezia,

- visto il D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali", di seguito definito "Codice";
- premesso che il Consiglio di Bacino Laguna di Venezia è Titolare del trattamento dei dati personali, ai sensi dell'art. 28 del Codice;
- preso atto che l'art. 4, comma 1, lettera h) del Codice definisce "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- atteso che l'art. 30 del Codice, dispone che:
  - le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.
  - la designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito.

in applicazione del Codice, con la presente nomina Enrico Conchetto quale Incaricato del trattamento dei dati personali relativamente a quanto di seguito indicato:

TRATTAMENTO	INFORMATIZZATO	CARTACEO
Protocollo	si	si
Atti amministrativi	si	si
Procedimenti	si	si

In qualità dipendente del CdB Laguna di Venezia incaricato del trattamento dei dati, nello svolgimento dei compiti che Le vengono assegnati dovrà:

1. adottare ogni accorgimento necessario ad assicurare l'integrità e riservatezza dei dati dei quali comunque venga a conoscenza;
2. curare che il trattamento avvenga in modo lecito e secondo correttezza, riguardi dati esatti, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati, provvedendo, se necessario, al loro aggiornamento e che la loro raccolta e registrazione avvenga per scopi determinati, espliciti e legittimi;
3. trattare i soli dati sensibili e giudiziari la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati, conservarli fino alla loro restituzione in contenitori muniti di serratura, adottare misure di sicurezza a protezione delle aree e dei locali ove i dati in oggetto vengono trattati e controllare l'accesso delle persone ai locali medesimi dopo l'orario di chiusura degli archivi, provvedendo alla loro identificazione e registrazione;

4. curare l'adozione di accorgimenti necessari alla tutela della riservatezza di dati diversi da quelli sensibili e giudiziari che presentino rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

5. svolgere le attività previste dai trattamenti di cui al punto 1 in conformità ai sistemi di autenticazione e di autorizzazione assegnati.

In ordine alla richieste di accesso agli atti e documenti contenenti dati sensibili, nell'osservanza dei principi, delle misure, modalità e accorgimenti sovra indicati, si rammenta la necessità di procedere alla previa verifica dei requisiti di cui alla L. 241/90.

Si ricordano, di seguito, alcune cautele alle quali dovrà porre particolare attenzione qualora si trovasse ad operare a contatto con il pubblico.

1) nei rapporti di front-office:

- rispetto della **distanza di sicurezza:** per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia;

- **identificazione dell'interessato**: in alcuni casi può essere necessario dover identificare il soggetto interessato per esigenze di garanzia di correttezza del dato da raccogliere, ossia può essere necessario richiedere ed ottenere un documento di identità o di riconoscimento ove si abbia un dubbio sulle modalità di scrittura del nome e cognome dell'interessato o si voglia avere garanzia dell'effettiva identità del soggetto interessato;

- **controllo dell'esattezza del dato:** fare attenzione alla digitazione ed all'inserimento dei dati identificativi dell'interessato, al fine di evitare errori di battitura, che potrebbero creare problemi nella gestione dell'anagrafica e nel prosieguo del processo;

- **obbligo di riservatezza e segretezza:** l'incaricato del trattamento deve mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni del trattamento e deve evitare qualunque diffusione delle informazioni stesse. Si ricorda che l'eventuale violazione dell'obbligo ivi considerato può comportare l'applicazione di sanzioni di natura disciplinare ed una responsabilità civile e penale, secondo quanto previsto dal codice della privacy;

2) cautele da seguire per la corretta comunicazione di dati a soggetti terzi o comunque con strumenti impersonali o che non consentono un controllo effettivo dell'identità del chiamante:

- **controllo dell'identità del richiedente:** nel caso di richieste di comunicazione di dati propri personali (presentate per telefono o per fax) occorre verificare l'identità del soggetto richiedente, attraverso la richiesta di invio, anche via fax, della fotocopia del suo documento di identità; successivamente alla verifica può essere utile comunicare all'interessato un codice personale identificativo, da comunicare al personale per ogni comunicazione impersonale (ad esempio a mezzo telefonico);

- **verifica dell'esattezza dei dati comunicati:** nell'accogliere una richiesta di comunicazione di dati personali, da parte dell'interessato ovvero di un terzo a ciò delegato, occorre fare attenzione che il dato comunicato sia esatto, pertinente, completo e non eccedente rispetto all'attività che si deve espletare, in particolare quando la richiesta viene soddisfatta telefonicamente o attraverso trascrizione da parte dell'operatore, di quanto visualizzato sul monitor; qualora si riscontri che i dati già in proprio possesso non sono aggiornati rispetto ad i dati comunicati dall'interessato, è necessario procedere all'aggiornamento dei

medesimi, previo espletamento delle formalità (richiesta, anche via fax, della fotocopia di un documento di identità) di cui al punto precedente.

3) istruzioni per l'uso degli strumenti del trattamento

- **telefono**: nel caso di richieste di informazioni da parte di organi di amministrazioni pubbliche, o di autorità giudiziarie, può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:
  - chiedere l'identità del chiamante e la motivazione della richiesta;
  - richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;
  - verificare che il numero di telefono dichiarato corrisponda effettivamente a quello del chiamante;
  - procedere immediatamente a richiamare la persona che ha richiesto le informazioni, con ciò accertandosi della identità dichiarata in precedenza;
- **fax**: nell'utilizzare questo strumento occorre prestare attenzione a:
  - digitare correttamente il numero di telefono, cui inviare la comunicazione;
  - controllare l'esattezza del numero digitato prima di inviare il documento;
  - attendere la stampa del rapporto di trasmissione, verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate;
  - qualora vengano trasmessi dati idonei a rivelare lo stato di salute, è necessario inviarli mediante raccomandata A/R al destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati, possano conoscere il contenuto della documentazione inviata;
  - in alcuni casi, può essere opportuno richiedere una telefonata che confermi da parte del destinatario la circostanza della corretta ricezione e leggibilità del contenuto del fax;
- **scanner**: i soggetti che provvedano all'acquisizione in formato digitale della documentazione cartacea (utilizzando ad esempio uno scanner) devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile; qualora vi siano errori di acquisizione ovvero si verifichino anomalie di processo, occorrerà procedere alla ripetizione delle operazioni;
- **distruzione delle copie cartacee**: coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero alla sostituzione della documentazione cartacea con registrazione ottica devono procedere alla distruzione controllata dei supporti cartacei non più occorrenti ovvero che presentino una forma non corretta. Occorre evitare di gettare la documentazione nel cestino della carta straccia senza aver previamente provveduto a rendere inintelligibile il contenuto: si potranno utilizzare apparati distruggi documenti o altri sistemi atti a ciò;
- **riutilizzo dei supporti di memorizzazione contenenti dati sensibili o giudiziari:** i supporti rimovibili (ad esempio pendrive, cd-rom, dvd) che contengano dati sensibili o giudiziari possono essere

riutilizzati solo se i dati precedentemente memorizzati non siano più visionabili da parte di terzi che procedano al riutilizzo del supporto medesimo; in caso contrario, occorrerà distruggere il supporto.

4) istruzioni in tema di sicurezza

a) password o componente riservata d'accesso alla rete:
- la password non deve contenere riferimenti agevolmente riconducibile all'incaricato e dovrebbe essere generata preferibilmente senza un significato compiuto;
- deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;
- l'incaricato è responsabile di ogni utilizzo indebito o non consentito della password di cui sia titolare;

b) back-up:
salvo che non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato, occorre procedere con cadenza almeno settimanale alla effettuazione di copie di sicurezza dei dati personali oggetto di trattamento, utilizzando gli apparati che siano messi a disposizione dell'incaricato e riporre le copie in un contenitore al quale possano accedere solamente soggetti autorizzati;

c) antivirus:
a meno che non siano adottati sistemi automatici di aggiornamento dei sistemi di protezione da programmi antivirus, gli incaricati del trattamento devono procedere all'effettuazione delle operazioni di aggiornamento dei programmi ivi considerati, almeno con cadenza settimanale o quando venga segnalata dal sistema tale esigenza, secondo le istruzioni visualizzate sullo schermo; una volta scaricato l'aggiornamento occorre procedere alla scansione dell'intero sistema per verificare la presenza sull'elaboratore in dotazione di virus;

d) stampanti:
Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento. La stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato;

e) protezione degli strumenti di lavoro:
in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (cd. screen-saver) dotato di password, ovvero, in alternativa, occorrerà porre la machina in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando.

Distinti saluti.

Direttore del CdB
Responsabile del trattamento
.....

Firma per accettazione
Incaricato del trattamento
.....

CONSIGLIO di BACINO
LAGUNA DI VENEZIA
Ambito Territoriale Ottimale per il servizio idrico integrato

Prot. n. /17 Venezia, 30/06/2017
Resp. Procedimento: Ing. Massimiliano Campanelli

Alla Sig.ra Angela Marafatto

Oggetto: Lettera di incarico per il trattamento dei dati personali

Il sottoscritto Massimiliano Campanelli, in qualità di Responsabile del trattamento dei dati personali ex art.29 del D.Lgs. 196/2003, per il Consiglio di Bacino Laguna di Venezia,

- visto il D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali", di seguito definito "Codice";
- premesso che il Consiglio di Bacino Laguna di Venezia è Titolare del trattamento dei dati personali, ai sensi dell'art. 28 del Codice;
- preso atto che l'art. 4, comma 1, lettera h) del Codice definisce "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- atteso che l'art. 30 del Codice, dispone che:
  - le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.
  - la designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito.

in applicazione del Codice, con la presente nomina Angela Marafatto quale Incaricato del trattamento dei dati personali relativamente a quanto di seguito indicato:

TRATTAMENTO	INFORMATIZZATO	CARTACEO
Protocollo	si	si
Inventario beni	si	no
Contabilità finanziaria	si	no
Gestione presenze	si	no
Messi comunali	si	no
Contratti	si	si
Atti amministrativi	si	si
Procedimenti	si	si

In qualità dipendente del CdB Laguna di Venezia incaricato del trattamento dei dati, nello svolgimento dei compiti che Le vengono assegnati dovrà:

1. adottare ogni accorgimento necessario ad assicurare l'integrità e riservatezza dei dati dei quali comunque venga a conoscenza;
2. curare che il trattamento avvenga in modo lecito e secondo correttezza, riguardi dati esatti, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati, provvedendo, se necessario, al loro aggiornamento e che la loro raccolta e registrazione avvenga per scopi determinati, espliciti e legittimi;
3. trattare i soli dati sensibili e giudiziari la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati, conservarli fino alla loro restituzione in contenitori muniti di serratura, adottare misure di sicurezza a protezione delle aree e dei locali ove i dati in oggetto vengono trattati e controllare l'accesso delle persone ai locali medesimi dopo l'orario di chiusura degli archivi, provvedendo alla loro identificazione e registrazione;

4. curare l'adozione di accorgimenti necessari alla tutela della riservatezza di dati diversi da quelli sensibili e giudiziari che presentino rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

5. svolgere le attività previste dai trattamenti di cui al punto 1 in conformità ai sistemi di autenticazione e di autorizzazione assegnati.

In ordine alla richieste di accesso agli atti e documenti contenenti dati sensibili, nell'osservanza dei principi, delle misure, modalità e accorgimenti sovra indicati, si rammenta la necessità di procedere alla previa verifica dei requisiti di cui alla L. 241/90.

Si ricordano, di seguito, alcune cautele alle quali dovrà porre particolare attenzione qualora si trovasse ad operare a contatto con il pubblico.

1) nei rapporti di front-office:

- rispetto della **distanza di sicurezza:** per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia;

- **identificazione dell'interessato**: in alcuni casi può essere necessario dover identificare il soggetto interessato per esigenze di garanzia di correttezza del dato da raccogliere, ossia può essere necessario richiedere ed ottenere un documento di identità o di riconoscimento ove si abbia un dubbio sulle modalità di scrittura del nome e cognome dell'interessato o si voglia avere garanzia dell'effettiva identità del soggetto interessato;

- **controllo dell'esattezza del dato:** fare attenzione alla digitazione ed all'inserimento dei dati identificativi dell'interessato, al fine di evitare errori di battitura, che potrebbero creare problemi nella gestione dell'anagrafica e nel prosieguo del processo;

- **obbligo di riservatezza e segretezza:** l'incaricato del trattamento deve mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni del trattamento e deve evitare qualunque diffusione delle informazioni stesse. Si ricorda che l'eventuale violazione dell'obbligo ivi considerato può comportare l'applicazione di sanzioni di natura disciplinare ed una responsabilità civile e penale, secondo quanto previsto dal codice della privacy;

2) cautele da seguire per la corretta comunicazione di dati a soggetti terzi o comunque con strumenti impersonali o che non consentono un controllo effettivo dell'identità del chiamante:

- **controllo dell'identità del richiedente:** nel caso di richieste di comunicazione di dati propri personali (presentate per telefono o per fax) occorre verificare l'identità del soggetto richiedente, attraverso la richiesta di invio, anche via fax, della fotocopia del suo documento di identità; successivamente alla verifica può essere utile comunicare all'interessato un codice personale identificativo, da comunicare al personale per ogni comunicazione impersonale (ad esempio a mezzo telefonico);

- **verifica dell'esattezza dei dati comunicati:** nell'accogliere una richiesta di comunicazione di dati personali, da parte dell'interessato ovvero di un terzo a ciò delegato, occorre fare attenzione che il dato comunicato sia esatto, pertinente, completo e non eccedente rispetto all'attività che si deve espletare, in particolare quando la richiesta viene soddisfatta telefonicamente o attraverso trascrizione da parte dell'operatore, di quanto visualizzato sul monitor; qualora si riscontri che i dati già in proprio possesso non sono aggiornati rispetto ad i dati comunicati dall'interessato, è necessario procedere all'aggiornamento dei

medesimi, previo espletamento delle formalità (richiesta, anche via fax, della fotocopia di un documento di identità) di cui al punto precedente.

3) istruzioni per l'uso degli strumenti del trattamento

- **telefono**: nel caso di richieste di informazioni da parte di organi di amministrazioni pubbliche, o di autorità giudiziarie, può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:
  - chiedere l'identità del chiamante e la motivazione della richiesta;
  - richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;
  - verificare che il numero di telefono dichiarato corrisponda effettivamente a quello del chiamante;
  - procedere immediatamente a richiamare la persona che ha richiesto le informazioni, con ciò accertandosi della identità dichiarata in precedenza;
- **fax**: nell'utilizzare questo strumento occorre prestare attenzione a:
  - digitare correttamente il numero di telefono, cui inviare la comunicazione;
  - controllare l'esattezza del numero digitato prima di inviare il documento;
  - attendere la stampa del rapporto di trasmissione, verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate;
  - qualora vengano trasmessi dati idonei a rivelare lo stato di salute, è necessario inviarli mediante raccomandata A/R al destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati, possano conoscere il contenuto della documentazione inviata;
  - in alcuni casi, può essere opportuno richiedere una telefonata che confermi da parte del destinatario la circostanza della corretta ricezione e leggibilità del contenuto del fax;
- **scanner**: i soggetti che provvedano all'acquisizione in formato digitale della documentazione cartacea (utilizzando ad esempio uno scanner) devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile; qualora vi siano errori di acquisizione ovvero si verifichino anomalie di processo, occorrerà procedere alla ripetizione delle operazioni;
- **distruzione delle copie cartacee**: coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero alla sostituzione della documentazione cartacea con registrazione ottica devono procedere alla distruzione controllata dei supporti cartacei non più occorrenti ovvero che presentino una forma non corretta. Occorre evitare di gettare la documentazione nel cestino della carta straccia senza aver previamente provveduto a rendere inintelligibile il contenuto: si potranno utilizzare apparati distruggi documenti o altri sistemi atti a ciò;
- **riutilizzo dei supporti di memorizzazione contenenti dati sensibili o giudiziari:** i supporti rimovibili (ad esempio pendrive, cd-rom, dvd) che contengano dati sensibili o giudiziari possono essere

riutilizzati solo se i dati precedentemente memorizzati non siano più visionabili da parte di terzi che procedano al riutilizzo del supporto medesimo; in caso contrario, occorrerà distruggere il supporto.

4) istruzioni in tema di sicurezza

a) password o componente riservata d'accesso alla rete:
- la password non deve contenere riferimenti agevolmente riconducibile all'incaricato e dovrebbe essere generata preferibilmente senza un significato compiuto;
- deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;
- l'incaricato è responsabile di ogni utilizzo indebito o non consentito della password di cui sia titolare;

b) back-up:
salvo che non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato, occorre procedere con cadenza almeno settimanale alla effettuazione di copie di sicurezza dei dati personali oggetto di trattamento, utilizzando gli apparati che siano messi a disposizione dell'incaricato e riporre le copie in un contenitore al quale possano accedere solamente soggetti autorizzati;

c) antivirus:
a meno che non siano adottati sistemi automatici di aggiornamento dei sistemi di protezione da programmi antivirus, gli incaricati del trattamento devono procedere all'effettuazione delle operazioni di aggiornamento dei programmi ivi considerati, almeno con cadenza settimanale o quando venga segnalata dal sistema tale esigenza, secondo le istruzioni visualizzate sullo schermo; una volta scaricato l'aggiornamento occorre procedere alla scansione dell'intero sistema per verificare la presenza sull'elaboratore in dotazione di virus;

d) stampanti:
Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento. La stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato;

e) protezione degli strumenti di lavoro:
in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (cd. screen-saver) dotato di password, ovvero, in alternativa, occorrerà porre la machina in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando.

Distinti saluti.

Direttore del CdB
Responsabile del trattamento
.....

Firma per accettazione
Incaricato del trattamento
Angela Moraldo.....

CONSIGLIO di BACINO
LAGUNA DI VENEZIA
Ambito Territoriale Ottimale per il servizio idrico integrato

Prot. n. /17 Venezia, 30/06/2017
Resp. Procedimento: Ing. Massimiliano Campanelli

Alla Sig.ra Chiara Micoli

Oggetto: Lettera di incarico per il trattamento dei dati personali

Il sottoscritto Massimiliano Campanelli, in qualità di Responsabile del trattamento dei dati personali ex art.29 del D.Lgs. 196/2003, per il Consiglio di Bacino Laguna di Venezia,

- visto il D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali", di seguito definito "Codice";
- premesso che il Consiglio di Bacino Laguna di Venezia è Titolare del trattamento dei dati personali, ai sensi dell'art. 28 del Codice;
- preso atto che l'art. 4, comma 1, lettera h) del Codice definisce "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- atteso che l'art. 30 del Codice, dispone che:
  - le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.
  - la designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito.

in applicazione del Codice, con la presente nomina Chiara Micoli quale Incaricato del trattamento dei dati personali relativamente a quanto di seguito indicato:

TRATTAMENTO	INFORMATIZZATO	CARTACEO
Protocollo	si	si
Atti amministrativi	si	si
Procedimenti	si	si

In qualità dipendente del CdB Laguna di Venezia incaricato del trattamento dei dati, nello svolgimento dei compiti che Le vengono assegnati dovrà:

1. adottare ogni accorgimento necessario ad assicurare l'integrità e riservatezza dei dati dei quali comunque venga a conoscenza;
2. curare che il trattamento avvenga in modo lecito e secondo correttezza, riguardi dati esatti, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati, provvedendo, se necessario, al loro aggiornamento e che la loro raccolta e registrazione avvenga per scopi determinati, espliciti e legittimi;
3. trattare i soli dati sensibili e giudiziari la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati, conservarli fino alla loro restituzione in contenitori muniti di serratura, adottare misure di sicurezza a protezione delle aree e dei locali ove i dati in oggetto vengono trattati e controllare l'accesso delle persone ai locali medesimi dopo l'orario di chiusura degli archivi, provvedendo alla loro identificazione e registrazione;

4. curare l'adozione di accorgimenti necessari alla tutela della riservatezza di dati diversi da quelli sensibili e giudiziari che presentino rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

5. svolgere le attività previste dai trattamenti di cui al punto 1 in conformità ai sistemi di autenticazione e di autorizzazione assegnati.

In ordine alla richieste di accesso agli atti e documenti contenenti dati sensibili, nell'osservanza dei principi, delle misure, modalità e accorgimenti sovra indicati, si rammenta la necessità di procedere alla previa verifica dei requisiti di cui alla L. 241/90.

Si ricordano, di seguito, alcune cautele alle quali dovrà porre particolare attenzione qualora si trovasse ad operare a contatto con il pubblico.

1) nei rapporti di front-office:

- rispetto della **distanza di sicurezza:** per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia;

- **identificazione dell'interessato**: in alcuni casi può essere necessario dover identificare il soggetto interessato per esigenze di garanzia di correttezza del dato da raccogliere, ossia può essere necessario richiedere ed ottenere un documento di identità o di riconoscimento ove si abbia un dubbio sulle modalità di scrittura del nome e cognome dell'interessato o si voglia avere garanzia dell'effettiva identità del soggetto interessato;

- **controllo dell'esattezza del dato:** fare attenzione alla digitazione ed all'inserimento dei dati identificativi dell'interessato, al fine di evitare errori di battitura, che potrebbero creare problemi nella gestione dell'anagrafica e nel prosieguo del processo;

- **obbligo di riservatezza e segretezza:** l'incaricato del trattamento deve mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni del trattamento e deve evitare qualunque diffusione delle informazioni stesse. Si ricorda che l'eventuale violazione dell'obbligo ivi considerato può comportare l'applicazione di sanzioni di natura disciplinare ed una responsabilità civile e penale, secondo quanto previsto dal codice della privacy;

2) cautele da seguire per la corretta comunicazione di dati a soggetti terzi o comunque con strumenti impersonali o che non consentono un controllo effettivo dell'identità del chiamante:

- **controllo dell'identità del richiedente:** nel caso di richieste di comunicazione di dati propri personali (presentate per telefono o per fax) occorre verificare l'identità del soggetto richiedente, attraverso la richiesta di invio, anche via fax, della fotocopia del suo documento di identità; successivamente alla verifica può essere utile comunicare all'interessato un codice personale identificativo, da comunicare al personale per ogni comunicazione impersonale (ad esempio a mezzo telefonico);

- **verifica dell'esattezza dei dati comunicati:** nell'accogliere una richiesta di comunicazione di dati personali, da parte dell'interessato ovvero di un terzo a ciò delegato, occorre fare attenzione che il dato comunicato sia esatto, pertinente, completo e non eccedente rispetto all'attività che si deve espletare, in particolare quando la richiesta viene soddisfatta telefonicamente o attraverso trascrizione da parte dell'operatore, di quanto visualizzato sul monitor; qualora si riscontri che i dati già in proprio possesso non sono aggiornati rispetto ad i dati comunicati dall'interessato, è necessario procedere all'aggiornamento dei

medesimi, previo espletamento delle formalità (richiesta, anche via fax, della fotocopia di un documento di identità) di cui al punto precedente.

3) istruzioni per l'uso degli strumenti del trattamento

- **telefono**: nel caso di richieste di informazioni da parte di organi di amministrazioni pubbliche, o di autorità giudiziarie, può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:
  - chiedere l'identità del chiamante e la motivazione della richiesta;
  - richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;
  - verificare che il numero di telefono dichiarato corrisponda effettivamente a quello del chiamante;
  - procedere immediatamente a richiamare la persona che ha richiesto le informazioni, con ciò accertandosi della identità dichiarata in precedenza;
- **fax**: nell'utilizzare questo strumento occorre prestare attenzione a:
  - digitare correttamente il numero di telefono, cui inviare la comunicazione;
  - controllare l'esattezza del numero digitato prima di inviare il documento;
  - attendere la stampa del rapporto di trasmissione, verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate;
  - qualora vengano trasmessi dati idonei a rivelare lo stato di salute, è necessario inviarli mediante raccomandata A/R al destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati, possano conoscere il contenuto della documentazione inviata;
  - in alcuni casi, può essere opportuno richiedere una telefonata che confermi da parte del destinatario la circostanza della corretta ricezione e leggibilità del contenuto del fax;
- **scanner**: i soggetti che provvedano all'acquisizione in formato digitale della documentazione cartacea (utilizzando ad esempio uno scanner) devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile; qualora vi siano errori di acquisizione ovvero si verifichino anomalie di processo, occorrerà procedere alla ripetizione delle operazioni;
- **distruzione delle copie cartacee**: coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero alla sostituzione della documentazione cartacea con registrazione ottica devono procedere alla distruzione controllata dei supporti cartacei non più occorrenti ovvero che presentino una forma non corretta. Occorre evitare di gettare la documentazione nel cestino della carta straccia senza aver previamente provveduto a rendere inintelligibile il contenuto: si potranno utilizzare apparati distruggi documenti o altri sistemi atti a ciò;
- **riutilizzo dei supporti di memorizzazione contenenti dati sensibili o giudiziari:** i supporti rimovibili (ad esempio pendrive, cd-rom, dvd) che contengano dati sensibili o giudiziari possono essere

riutilizzati solo se i dati precedentemente memorizzati non siano più visionabili da parte di terzi che procedano al riutilizzo del supporto medesimo; in caso contrario, occorrerà distruggere il supporto.

4) istruzioni in tema di sicurezza

a) password o componente riservata d'accesso alla rete:
- la password non deve contenere riferimenti agevolmente riconducibile all'incaricato e dovrebbe essere generata preferibilmente senza un significato compiuto;
- deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;
- l'incaricato è responsabile di ogni utilizzo indebito o non consentito della password di cui sia titolare;

b) back-up:
salvo che non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato, occorre procedere con cadenza almeno settimanale alla effettuazione di copie di sicurezza dei dati personali oggetto di trattamento, utilizzando gli apparati che siano messi a disposizione dell'incaricato e riporre le copie in un contenitore al quale possano accedere solamente soggetti autorizzati;

c) antivirus:
a meno che non siano adottati sistemi automatici di aggiornamento dei sistemi di protezione da programmi antivirus, gli incaricati del trattamento devono procedere all'effettuazione delle operazioni di aggiornamento dei programmi ivi considerati, almeno con cadenza settimanale o quando venga segnalata dal sistema tale esigenza, secondo le istruzioni visualizzate sullo schermo; una volta scaricato l'aggiornamento occorre procedere alla scansione dell'intero sistema per verificare la presenza sull'elaboratore in dotazione di virus;

d) stampanti:
Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento. La stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato;

e) protezione degli strumenti di lavoro:
in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (cd. screen-saver) dotato di password, ovvero, in alternativa, occorrerà porre la machina in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando.

Distinti saluti.

Direttore del CdB
Responsabile del trattamento
.....

Firma per accettazione
Incaricato del trattamento
.....

CONSIGLIO di BACINO
LAGUNA DI VENEZIA
Ambito Territoriale Ottimale per il servizio idrico integrato

Prot. n. /17 Venezia, 30/06/2017
Resp. Procedimento: Ing. Massimiliano Campanelli

Al Sig. Marco Tabacchi

Oggetto: Lettera di incarico per il trattamento dei dati personali

Il sottoscritto Massimiliano Campanelli, in qualità di Responsabile del trattamento dei dati personali ex art.29 del D.Lgs. 196/2003, per il Consiglio di Bacino Laguna di Venezia,

- visto il D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali", di seguito definito "Codice";
- premesso che il Consiglio di Bacino Laguna di Venezia è Titolare del trattamento dei dati personali, ai sensi dell'art. 28 del Codice;
- preso atto che l'art. 4, comma 1, lettera h) del Codice definisce "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- atteso che l'art. 30 del Codice, dispone che:
  - le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.
  - la designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito.

in applicazione del Codice, con la presente nomina Marco Tabacchi quale Incaricato del trattamento dei dati personali relativamente a quanto di seguito indicato:

TRATTAMENTO	INFORMATIZZATO	CARTACEO
Protocollo	si	si
Inventario beni	si	no
Contabilità finanziaria	si	no
Gestione del personale	si	no
Gestione presenze	si	no
Messi comunali	si	no
Contratti	si	si
Atti amministrativi	si	si
Procedimenti	si	si

In qualità dipendente del CdB Laguna di Venezia incaricato del trattamento dei dati, nello svolgimento dei compiti che Le vengono assegnati dovrà:

1. adottare ogni accorgimento necessario ad assicurare l'integrità e riservatezza dei dati dei quali comunque venga a conoscenza;
2. curare che il trattamento avvenga in modo lecito e secondo correttezza, riguardi dati esatti, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati, provvedendo, se necessario, al loro aggiornamento e che la loro raccolta e registrazione avvenga per scopi determinati, espliciti e legittimi;
3. trattare i soli dati sensibili e giudiziari la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati, conservarli fino alla loro restituzione in contenitori muniti di serratura, adottare misure di sicurezza a protezione delle aree e dei locali ove i dati in oggetto vengono trattati e controllare l'accesso delle persone ai locali medesimi dopo l'orario di chiusura degli archivi, provvedendo alla loro identificazione e registrazione;

4. curare l'adozione di accorgimenti necessari alla tutela della riservatezza di dati diversi da quelli sensibili e giudiziari che presentino rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

5. svolgere le attività previste dai trattamenti di cui al punto 1 in conformità ai sistemi di autenticazione e di autorizzazione assegnati.

In ordine alla richieste di accesso agli atti e documenti contenenti dati sensibili, nell'osservanza dei principi, delle misure, modalità e accorgimenti sovra indicati, si rammenta la necessità di procedere alla previa verifica dei requisiti di cui alla L. 241/90.

Si ricordano, di seguito, alcune cautele alle quali dovrà porre particolare attenzione qualora si trovasse ad operare a contatto con il pubblico.

1) nei rapporti di front-office:

- rispetto della **distanza di sicurezza:** per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia;

- **identificazione dell'interessato**: in alcuni casi può essere necessario dover identificare il soggetto interessato per esigenze di garanzia di correttezza del dato da raccogliere, ossia può essere necessario richiedere ed ottenere un documento di identità o di riconoscimento ove si abbia un dubbio sulle modalità di scrittura del nome e cognome dell'interessato o si voglia avere garanzia dell'effettiva identità del soggetto interessato;

- **controllo dell'esattezza del dato:** fare attenzione alla digitazione ed all'inserimento dei dati identificativi dell'interessato, al fine di evitare errori di battitura, che potrebbero creare problemi nella gestione dell'anagrafica e nel prosieguo del processo;

- **obbligo di riservatezza e segretezza:** l'incaricato del trattamento deve mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni del trattamento e deve evitare qualunque diffusione delle informazioni stesse. Si ricorda che l'eventuale violazione dell'obbligo ivi considerato può comportare l'applicazione di sanzioni di natura disciplinare ed una responsabilità civile e penale, secondo quanto previsto dal codice della privacy;

2) cautele da seguire per la corretta comunicazione di dati a soggetti terzi o comunque con strumenti impersonali o che non consentono un controllo effettivo dell'identità del chiamante:

- **controllo dell'identità del richiedente:** nel caso di richieste di comunicazione di dati propri personali (presentate per telefono o per fax) occorre verificare l'identità del soggetto richiedente, attraverso la richiesta di invio, anche via fax, della fotocopia del suo documento di identità; successivamente alla verifica può essere utile comunicare all'interessato un codice personale identificativo, da comunicare al personale per ogni comunicazione impersonale (ad esempio a mezzo telefonico);

- **verifica dell'esattezza dei dati comunicati:** nell'accogliere una richiesta di comunicazione di dati personali, da parte dell'interessato ovvero di un terzo a ciò delegato, occorre fare attenzione che il dato comunicato sia esatto, pertinente, completo e non eccedente rispetto all'attività che si deve espletare, in particolare quando la richiesta viene soddisfatta telefonicamente o attraverso trascrizione da parte dell'operatore, di quanto visualizzato sul monitor; qualora si riscontri che i dati già in proprio possesso non sono aggiornati rispetto ad i dati comunicati dall'interessato, è necessario procedere all'aggiornamento dei

medesimi, previo espletamento delle formalità (richiesta, anche via fax, della fotocopia di un documento di identità) di cui al punto precedente.

3) istruzioni per l'uso degli strumenti del trattamento

- **telefono**: nel caso di richieste di informazioni da parte di organi di amministrazioni pubbliche, o di autorità giudiziarie, può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:
  - chiedere l'identità del chiamante e la motivazione della richiesta;
  - richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;
  - verificare che il numero di telefono dichiarato corrisponda effettivamente a quello del chiamante;
  - procedere immediatamente a richiamare la persona che ha richiesto le informazioni, con ciò accertandosi della identità dichiarata in precedenza;
- **fax**: nell'utilizzare questo strumento occorre prestare attenzione a:
  - digitare correttamente il numero di telefono, cui inviare la comunicazione;
  - controllare l'esattezza del numero digitato prima di inviare il documento;
  - attendere la stampa del rapporto di trasmissione, verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate;
  - qualora vengano trasmessi dati idonei a rivelare lo stato di salute, è necessario inviarli mediante raccomandata A/R al destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati, possano conoscere il contenuto della documentazione inviata;
  - in alcuni casi, può essere opportuno richiedere una telefonata che confermi da parte del destinatario la circostanza della corretta ricezione e leggibilità del contenuto del fax;
- **scanner**: i soggetti che provvedano all'acquisizione in formato digitale della documentazione cartacea (utilizzando ad esempio uno scanner) devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile; qualora vi siano errori di acquisizione ovvero si verifichino anomalie di processo, occorrerà procedere alla ripetizione delle operazioni;
- **distruzione delle copie cartacee**: coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero alla sostituzione della documentazione cartacea con registrazione ottica devono procedere alla distruzione controllata dei supporti cartacei non più occorrenti ovvero che presentino una forma non corretta. Occorre evitare di gettare la documentazione nel cestino della carta straccia senza aver previamente provveduto a rendere inintelligibile il contenuto: si potranno utilizzare apparati distruggi documenti o altri sistemi atti a ciò;
- **riutilizzo dei supporti di memorizzazione contenenti dati sensibili o giudiziari:** i supporti rimovibili (ad esempio pendrive, cd-rom, dvd) che contengano dati sensibili o giudiziari possono essere

riutilizzati solo se i dati precedentemente memorizzati non siano più visionabili da parte di terzi che procedano al riutilizzo del supporto medesimo; in caso contrario, occorrerà distruggere il supporto.

4) istruzioni in tema di sicurezza

a) password o componente riservata d'accesso alla rete:
- la password non deve contenere riferimenti agevolmente riconducibile all'incaricato e dovrebbe essere generata preferibilmente senza un significato compiuto;
- deve essere custodita con la massima attenzione e segretezza e non deve essere divulgata o comunicata a terzi;
- l'incaricato è responsabile di ogni utilizzo indebito o non consentito della password di cui sia titolare;

b) back-up:
salvo che non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato, occorre procedere con cadenza almeno settimanale alla effettuazione di copie di sicurezza dei dati personali oggetto di trattamento, utilizzando gli apparati che siano messi a disposizione dell'incaricato e riporre le copie in un contenitore al quale possano accedere solamente soggetti autorizzati;

c) antivirus:
a meno che non siano adottati sistemi automatici di aggiornamento dei sistemi di protezione da programmi antivirus, gli incaricati del trattamento devono procedere all'effettuazione delle operazioni di aggiornamento dei programmi ivi considerati, almeno con cadenza settimanale o quando venga segnalata dal sistema tale esigenza, secondo le istruzioni visualizzate sullo schermo; una volta scaricato l'aggiornamento occorre procedere alla scansione dell'intero sistema per verificare la presenza sull'elaboratore in dotazione di virus;

d) stampanti:
Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento. La stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato;

e) protezione degli strumenti di lavoro:
in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure atte a escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (cd. screen-saver) dotato di password, ovvero, in alternativa, occorrerà porre la machina in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando.

Distinti saluti.

Direttore del CdB
Responsabile del trattamento
.....

Firma per accettazione
Incaricato del trattamento
.....

ALLEGATO 6

NOMINA DEL CUSTODE DELLE CREDENZIALI

CONSIGLIO di BACINO
LAGUNA DI VENEZIA
Ambito Territoriale Ottimale per il servizio idrico integrato

Prot. n. /17 Venezia, 30/06/2017
Resp. Procedimento: Ing. Massimiliano Campanelli
Resp. Istruttoria: Dott. Enrico Conchetto

Oggetto: lettera di incarico di Custode delle copie delle credenziali (D.Lgs. 196/03).

Il sottoscritto Massimiliano Campanelli, in qualità di Responsabile del trattamento dei dati personali ex art. 29 del D.Lgs. 196/2003, per il Consiglio di Bacino Laguna di Venezia,

- visto il D. Lgs. 30 giugno 2003, n. 196. "Codice in materia di protezione dei dati personali", di seguito definito "Codice";
- premesso che il Consiglio di Bacino Laguna di Venezia è Titolare del trattamento dei dati personali, ai sensi dell'art 28 del Codice;
- preso atto che il Codice prevede che ogni incaricato del trattamento dei dati sia munito di credenziali per l'autenticazione, costituite da un codice per l'identificazione (user id) associato ad una parola chiave riservata (password) per l'accesso ai dati personali presenti nei singoli elaboratori e/o nei sistemi informatici in rete.
- preso atto che l'assegnazione, la gestione e la variazione della parola chiave deve essere caratterizzata dalla riservatezza e che, pertanto, il Codice prevede l'individuazione e la nomina di un "soggetto incaricato della loro custodia";

in applicazione del Codice, con la presente nomina Enrico Conchetto quale "custode delle parole chiave riservate" attribuite ai singoli incaricati al trattamento presso il Consiglio di Bacino Laguna di Venezia.

Quale custode delle copie delle credenziali di autenticazione informatica dovrà:

- farsi consegnare da ogni incaricato del trattamento dei dati, da ogni responsabile e comunque da chiunque altro all'interno dell'Ente sia dotato di credenziale di autenticazione, la copia della password che consenta l'accesso allo strumento informatico in uso all'incaricato;
- conservare le copie delle credenziali, consegnate dall'incaricato stesso in busta chiusa datata e sigillata mediante firma dell'incaricato su tutti i lembi, in luogo sicuro e non accessibile agli altri incaricati e ai terzi e sostituita con la prevista periodicità;
- nel caso in cui il Responsabile del trattamento abbia la necessità indifferibile di accedere ad un elaboratore in caso di prolungata assenza o impedimento dell'incaricato che lo utilizza abitualmente, consegnare al Responsabile stesso la busta contenente la parola chiave dell'elaboratore sul quale egli può intervenire unicamente per necessità di operatività e sicurezza del sistema informativo;

Consiglio di Bacino Laguna di Venezia
Via Pepe, 102 - 30172 Mestre – VENEZIA
Tel. 041 5040 793 – Fax 041 3969 123
e-mail: info@consigliodibacinolv.gov.it
pec: consigliodibacinolv@pec.it
website: www.consigliodibacinolv.gov.it
cod. fiscale: 94049070272

- informare tempestivamente l'incaricato del quale, in sua assenza, è stata consegnata la parola chiave al Responsabile del trattamento, affinché questi provveda appena possibile alla sostituzione della parola chiave, e farsela consegnare in una nuova busta chiusa.

Il Responsabile del trattamento

Il Custode delle credenziali per accettazione

Consiglio di Bacino Laguna di Venezia
Via Pepe, 102 - 30172 Mestre – VENEZIA
Tel. 041 5040 793 – Fax 041 3969 123
e-mail: info@consigliodibacinolv.gov.it
pec: consigliodibacinolv@pec.it
website: www.consigliodibacinolv.gov.it
cod. fiscale: 94049070272

ALLEGATO 7

NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI IN HOSTING

CONSIGLIO di BACINO
LAGUNA DI VENEZIA
Ambito Territoriale Ottimale per il servizio idrico integrato

Prot. n. 1062/14 Venezia, 18/11/2014

INVIATA A MEZZO: PEC

Spett.le
Accatre Srl
Via Lombardi 14/6
30020 Marcon - VE

Alla cortese attenzione del Titolare del trattamento.

Oggetto: Nomina del responsabile al trattamento dei dati personali.

Ai sensi dell'articolo 29 del D.lgs. 196/2003 (d'ora in poi Codice) con il presente atto questo Ente in qualità di Titolare del trattamento dei dati personali designa il soggetto destinatario quale Responsabile del trattamento dei dati personali limitatamente ai trattamenti funzionali all'attività di erogazione del servizio di Immedia e Immedia Plus previsti dalla convenzione in essere.

Il trattamento è strettamente collegato alle finalità stesse del contratto e limitatamente alla durata dello stesso.

La nomina a Responsabile decadrà in caso di cessazione del contratto con effetto dalla data di tale cessazione.

Modalità di trattamento e requisiti dei dati

Il Titolare dichiara che i dati da lui trasmessi ad Accatre Srl sono raccolti e trasmessi rispettando le prescrizioni di legge; sono esatti e, se necessario, aggiornati; sono pertinenti, completi e non eccedenti rispetto alle finalità per le quali vengono trasmessi.

Qualora dovesse emergere la necessità di eseguire operazioni di trattamento diverse ed eccezionali rispetto a quelle funzionalmente collegate alla prestazione, Accatre Srl informerà tempestivamente il Titolare. Inoltre in capo ad Accatre Srl incombe l'onere di comunicare al Titolare qualsiasi elemento nuovo, oggettivo o soggettivo, che possa compromettere il corretto espletamento del trattamento dei dati personali.

Obblighi

Accatre Srl deve adottare tutte le misure minime di sicurezza idonee a salvaguardare la riservatezza, l'integrità e la completezza dei dati trattati. Pertanto dovrà:

- verificare e controllare che nell'ambito della propria organizzazione il trattamento dei dati sia effettuato ai sensi e nei limiti degli artt. 11, 16, 31, 34 e 35 del Codice e coordinarne tutte le operazioni;
- individuare gli incaricati del trattamento dei dati e impartire le disposizioni organizzative e operative nonché le istruzioni richieste dall'Allegato B del Codice, necessarie per il corretto, lecito, pertinente e sicuro trattamento dei dati;
- disporre gli interventi necessari per la sicurezza del trattamento dei dati e per la correttezza dell'accesso agli stessi;
- collaborare con il Titolare all'attuazione e all'adempimento degli obblighi previsti dal Codice;

Accatre Srl non potrà comunicare né diffondere né utilizzare autonomamente per scopi diversi da quelli sopra indicati i dati personali oggetto del trattamento.

Resta inteso che Accatre Srl non avrà alcun contatto con gli interessati o comunque con terzi che possano fornire dati personali degli interessati destinati ad essere raccolti e trattati nella prestazione dei servizi ai sensi del contratto offerto, pertanto restano a carico del Titolare tutti gli obblighi stabiliti dalla normativa privacy nei confronti degli interessati stessi, compresi a titolo meramente esemplificativo gli obblighi di informazione di cui all'art. 13 del Codice, gli obblighi relativi al conferimento del consenso di cui agli artt. 23 e 26 del Codice, gli obblighi relativi all'esercizio dei diritti degli interessati di cui all'art. 7 del Codice.

Attività del Titolare

Considerato che l'affidamento all'esterno delle operazioni di trattamento non dispensa il Titolare dal rispetto degli obblighi previsti dal Codice, cioè vigilare sull'osservanza da parte di Accatre Srl delle vigenti disposizioni in materia di trattamento, il Titolare potrà attuare delle verifiche periodiche. Per facilitare tale attività Accatre Srl dovrà relazionare periodicamente sulla conformità alla norma dei trattamenti effettuati.

Il Titolare dovrà comunicare formalmente per iscritto ad Accatre Srl qualsiasi variazione si dovesse rendere necessaria rispetto al trattamento di dati affidato con la presente nomina. Le eventuali variazioni dovranno essere integrate nel presente atto.

Copia del presente atto dovrà essere restituito debitamente sottoscritto per presa visione ed accettazione.

Distinti saluti.

IL RAPPRESENTANTE LEGALE

H3 s.r.l.
Doro Luciano

IL TITOLARE

CONSIGLIO DI BACINO LAGUNA DI VENEZIA

Consiglio di Bacino Laguna di Venezia
Via Pepe, 102
30172 Mestre – VENEZIA
Tel. 041 5040793 – Fax 041 3969123
e-mail: segreteria@consiglodibacinolv.gov.
website: www.consiglodibacinolv.gov.it
cod. fiscale: 94049070272

CONSIGLIO di BACINO
LAGUNA DI VENEZIA
Ambito Territoriale Ottimale per il servizio idrico integrato

Prot. n. 1015/14 Venezia, 11/11/2014

INVIATA A MEZZO: PEC

Spett.le
Halley Veneto
Via Lombardi 14
30020 Marcon - VE

Alla cortese attenzione del Titolare del trattamento.

Oggetto: Nomina del responsabile al trattamento dei dati personali.

Ai sensi dell'articolo 29 del D.lgs. 196/2003 (d'ora in poi Codice) con il presente atto questo ente in qualità di Titolare del trattamento dei dati personali designa il soggetto destinatario quale Responsabile del trattamento dei dati personali limitatamente ai trattamenti funzionali all'attività di servizio di manutenzione del software applicativo Halley comprensivo dei Servizi al cittadino previsti dalla convenzione in essere.

Il trattamento è strettamente collegato alle finalità stesse del contratto e limitatamente alla durata dello stesso.

La nomina a Responsabile decadrà in caso di cessazione del contratto con effetto dalla data di tale cessazione.

Modalità di trattamento e requisiti dei dati

Il Titolare dichiara che i dati da lui trasmessi ad Halley Veneto Srl sono raccolti e trasmessi rispettando le prescrizioni di legge; esatti e, se necessario, aggiornati; nonché pertinenti, completi e non eccedenti rispetto alle finalità per le quali vengono trasmessi.

Qualora dovesse emergere la necessità di eseguire operazioni di trattamento diverse ed eccezionali rispetto a quelle funzionalmente collegate alla prestazione, Halley Veneto Srl informerà tempestivamente il Titolare. Inoltre in capo ad Halley Veneto Srl incombe l'onere di comunicare al Titolare qualsiasi elemento nuovo, oggettivo o soggettivo, che possa compromettere il corretto espletamento del trattamento dei dati personali.

Obblighi

Halley Veneto Srl deve adottare tutte le misure minime di sicurezza idonee a salvaguardare la riservatezza, l'integrità e la completezza dei dati trattati. Pertanto dovrà:

Consiglio di Bacino Laguna di Venezia
Via Pepe, 102
30172 Mestre – VENEZIA
Tel. 041 5040793 – Fax 041 3969123
e-mail: segreteria@consiglliodibacinolv.gov.
website: www.consiglliodibacinolv.gov.it
cod. fiscale: 94049070272

- verificare e controllare che nell'ambito della propria organizzazione il trattamento dei dati sia effettuato ai sensi e nei limiti degli artt. 11, 16, 31, 34 e 35 del Codice e coordinarne tutte le operazioni;
- individuare gli incaricati del trattamento dei dati e impartire le disposizioni organizzative e operative, nonché le istruzioni richieste dall'Allegato B del Codice, necessarie per il corretto, lecito, pertinente e sicuro trattamento dei dati;
- disporre gli interventi necessari per la sicurezza del trattamento dei dati e per la correttezza dell'accesso agli stessi;
- collaborare con il Titolare all'attuazione e all'adempimento degli obblighi previsti dal Codice;

Halley Veneto Srl non potrà comunicare né diffondere né utilizzare autonomamente per scopi diversi da quelli sopra indicati i dati personali oggetto del trattamento.

Resta inteso che Halley Veneto Srl non avrà alcun contatto con gli interessati o comunque con terzi che possano fornire dati personali degli interessati destinati ad essere raccolti e trattati nella prestazione dei servizi ai sensi del contratto offerto, pertanto restano a carico del Titolare tutti gli obblighi stabiliti dalla normativa privacy nei confronti degli interessati stessi, compresi a titolo meramente esemplificativo gli obblighi di informazione di cui all'art. 13 del Codice, gli obblighi relativi al conferimento del consenso di cui agli artt. 23 e 26 del Codice, gli obblighi relativi all'esercizio dei diritti degli interessati di cui all'art. 7 del Codice.

Attività del Titolare

Considerato che l'affidamento all'esterno delle operazioni di trattamento non dispensa il Titolare dal rispetto degli obblighi previsti dal Codice, cioè vigilare sull'osservanza da parte del Responsabile delle vigenti disposizioni in materia di trattamento, il Titolare potrà attuare delle verifiche periodiche. Per facilitare tale attività il Responsabile dovrà relazionare periodicamente sulla conformità alla norma dei trattamenti effettuati

Il Titolare dovrà comunicare formalmente per iscritto ad Halley Veneto Srl qualsiasi variazione si dovesse rendere necessaria rispetto al trattamento di dati affidato con la presente nomina. . Le eventuali variazioni dovranno essere integrate nel presente atto.

Copia del presente atto dovrà essere restituito debitamente sottoscritto per presa visione ed accettazione.

Distinti saluti.

IL RAPPRESENTANTE LEGALE

HALLEY VENETO S.r.l.
Quinto Paolo

IL TITOLARE

CONSIGLIO DI BACINO LAGUNA DI VENEZIA

Consiglio di Bacino Laguna di Venezia
Via Pepe, 102
30172 Mestre – VENEZIA
Tel. 041 5040793 – Fax 041 3969123
e-mail: segreteria@consiglodibacinolv.gov.
website: www.consiglodibacinolv.gov.it
cod. fiscale: 94049070272

ALLEGATO 8

RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE

CONSIGLIO di BACINO
LAGUNA DI VENEZIA
Ambito Territoriale Ottimale per il servizio idrico integrato

Prot. n. **/17** Venezia, 30/06/2017
Resp. Procedimento: Ing. Massimiliano Campanelli
Resp. Istruttoria: Dott. Enrico Conchetto

Oggetto: responsabile del servizio di Conservazione.

In accordo con l'art. 6 del DPCM del 3 dicembre 2013 "*Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44 , 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*", e con la deliberazione di Comitato Istituzionale n. 23 del 12/10/2015, con cui è stato nominato il direttore del Consiglio di Bacino Laguna di Venezia quale **Responsabile della Conservazione**, con la presente si conferisce tale nomina a Massimiliano Campanelli, al quale è stata consegnata lettera di incarico al trattamento dei dati personali.

In accordo con l'art. 5 comma b) e art. 6 comma 6) del DPCM succitato, è stata nominata in data 19/10/2015 la società Infocert S.p.A. quale **Responsabile del servizio di Conservazione** che assume contestualmente il ruolo di responsabile del trattamento dei dati come previsto dal Codice in materia di protezione dei dati personali.

Il Titolare del trattamento

Consiglio di Bacino Laguna di Venezia
Via Pepe, 102 - 30172 Mestre – VENEZIA
Tel. 041 5040 793 – Fax 041 3969 123
e-mail: info@consigliodibacinolv.gov.it
pec: consigliodibacinolv@pec.it
website: www.consigliodibacinolv.gov.it
cod. fiscale: 94049070272

ALLEGATO 9

LIBERATORIA IMPRESA DI PULIZIE

CONSIGLIO di BACINO
LAGUNA DI VENEZIA
Ambito Territoriale Ottimale per il servizio idrico integrato

Prot. n. /16
Resp. Procedimento: Dott. Nicola Nardin
Resp. Istruttoria: Dott. Enrico Conchetto

Venezia, 06/10/2016

TRASMESSA A MEZZO PEC

Spett.le
A.F. Multiservice Società cooperativa
via Asseggiano, 41/L
30174 Mestre (Ve)

Oggetto: Informativa privacy e misure minime di sicurezza (D.Lgs. 196/03).

Il Consiglio di Bacino Laguna di Venezia, titolare del trattamento dei dati, informa che per l'instaurazione e l'esecuzione dei rapporti contrattuali è in possesso di dati, relativi al Fornitore, anagrafici e fiscali acquisiti direttamente o tramite terzi, qualificati come personali dalla legge.
Con riferimento al D.Lgs. 196/2003, si informa che il Direttore del Consiglio di Bacino Laguna di Venezia, con sede in via G. Pepe, 102 Mestre (Ve), è il Responsabile del trattamento dei dati.
Con riferimento a tali dati si informa che:

- i dati vengono trattati in relazione alle esigenze contrattuali ed ai conseguenti adempimenti degli obblighi legali e contrattuali dalle stesse derivanti nonché per conseguire una efficace gestione dei rapporti commerciali ed anche ai fini della tutela del credito e della migliore gestione dei nostri diritti relativi al singolo rapporto commerciale. I dati verranno trattati in forma scritta e/o su supporto informatico o telematico;
- il conferimento dei dati stessi è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a fornirli o al successivo trattamento potrà determinare l'impossibilità della scrivente a dar corso ai rapporti contrattuali medesimi;
- il mancato conferimento, invece, di tutti i dati che non siano riconducibili ad obblighi legali o contrattuali verrà valutato di volta in volta dalla scrivente e determinerà le conseguenti decisioni rapportate all'importanza dei dati richiesti rispetto alla gestione del rapporto commerciale;
- ferme restando le comunicazioni e diffusioni effettuate in esecuzione di obblighi di legge, i dati potranno essere comunicati a professionisti e consulenti per la gestione contabile;
- i dati verranno trattati per tutta la durata dei rapporti contrattuali instaurati e anche successivamente per l'espletamento di tutti gli adempimenti di legge;

Consiglio di Bacino Laguna di Venezia
Via Pepe, 102 - 30172 Mestre – VENEZIA
Tel. 041 5040 793 – Fax 041 3969 123
e-mail: info@consigliodibacinolv.gov.it
pec: consigliodibacinolv@pec.it
website: www.consigliodibacinolv.gov.it
cod. fiscale: 94049070272

CONSIGLIO di BACINO
LAGUNA DI VENEZIA
Ambito Territoriale Ottimale per il servizio idrico integrato

- relativamente ai dati medesimi il Fornitore può esercitare i diritti previsti dall'art. 7 del D.Lgs. 196/2003 (di cui viene allegata copia) nei limiti ed alle condizioni previste dagli articolo 8, 9 e 10 del citato decreto legislativo.

Per quanto riguarda lo svolgimento delle attività previste da contratto il Fornitore dichiara di essere a conoscenza di quanto stabilito dal D.Lgs. n. 196 del 30/06/2003 e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte.
Il Fornitore ha l'obbligo di mantenere riservati i dati e le informazioni, ivi comprese quelle che transitano per le apparecchiature di elaborazione dati, di cui venga accidentalmente in possesso e, comunque, a conoscenza, di non divulgarli in alcun modo e in qualsiasi forma e di non farne oggetto di utilizzazione a qualsiasi titolo, e comunque per i cinque anni successivi alla cessazione di efficacia del rapporto contrattuale.
Per il rispetto delle misure minime di sicurezza poste a tutela dei trattamenti dei dati personali saranno considerate autorizzate all'accesso nei nostri locali solo le persone assegnate dalla Vostra Società alle pulizie dei locali e di cui siano stati preventivamente forniti i nominativi. In caso di assenza o impedimento del personale incaricato, sarà Vostra cura ed obbligo, comunicarci i nominativi dei sostituti.
Le persone autorizzate dovranno limitarsi alle sole attività di pulizia.

Il Fornitore dichiara di aver ricevuto completa informativa ai sensi dell'art. 13 D.Lgs. 196/2003 unitamente a copia dell'art. 7 del decreto medesimo, ed esprime il consenso al trattamento ed alla comunicazione dei propri dati qualificati come personali dalla citata legge nei limiti, per le finalità e per la durata precisati nell'informativa.

Responsabile del trattamento
del Consiglio di Bacino

Il rappresentante legale
di A.F. Multiservice Società cooperativa

Consiglio di Bacino Laguna di Venezia
Via Pepe, 102 - 30172 Mestre – VENEZIA
Tel. 041 5040 793 – Fax 041 3969 123
e-mail: info@consigliodibacinolv.gov.it
pec: consigliodibacinolv@pec.it
website: www.consigliodibacinolv.gov.it
cod. fiscale: 94049070272

CONSIGLIO di BACINO
LAGUNA DI VENEZIA
Ambito Territoriale Ottimale per il servizio idrico integrato

D.Lgs. 30 giugno 2003, n. 196

Art. 7 (Diritto di accesso ai dati personali ed altri diritti)

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione:

a) dell'origine dei dati personali;

b) delle finalità e modalità del trattamento;

c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;

d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;

e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:

a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Consiglio di Bacino Laguna di Venezia
Via Pepe, 102 - 30172 Mestre – VENEZIA
Tel. 041 5040 793 – Fax 041 3969 123
e-mail: info@consigliodibacinolv.gov.it
pec: consigliodibacinolv@pec.it
website: www.consigliodibacinolv.gov.it
cod. fiscale: 94049070272