Bergamo Sviluppo
Azienda Speciale della Camera di Commercio

Piano generale per la sicurezza dei documenti

Sommario

1 Aspetti generali

Il presente documento è redatto al fine di descrivere e pianificare le misure di sicurezza fisiche, logiche ed organizzative adottate da Bergamo Sviluppo per la tutela della sicurezza e dell'integrità dei dati trattati dalla stessa nell'esercizio delle sue attività in conformità al Regolamento Europeo 2016/679 in materia di protezione dei dati personali.

2 Analisi dei rischi

I rischi sono stati raggruppati in termini di:

- rischi per la riservatezza: le informazioni e i documenti devono essere accessibili ed utilizzati solo da persone autorizzate e per fini conformi agli obiettivi dell'Azienda;
- rischi per la integrità: i dati e i documenti devono essere esatti, aggiornati, corrispondenti alla realtà e protetti da qualsiasi forma di alterazione non controllata;
- rischi per la disponibilità: l'accesso ai dati e ai documenti deve poter avvenire ogni qual volta ve ne sia necessità in conformità alle esigenze dei trattamenti;
- rischi di uso improprio: l'accesso ai dati deve avvenire esclusivamente per i fini definiti dal Titolare da parte di soggetti adeguatamente autorizzati ed istruiti.

Sulla base della suddetta classificazione nella tabella seguente vengono identificati, per ciascuna risorsa critica, i rischi per i quali devono essere adottate misure di sicurezza adeguate.

Risorsa	Riservatezza	Integrità	Disponibilità	Uso improprio
Sistema informatico (server, PC, linee TD)	Diffusi Trafugati Usati per deduzioni (inferenza)	Danneggiati per: Errore utente Errore Hw Errore Sw Manomissione Virus informatici	Cancellati Mal inseriti Distrutti	Fini incongruenti Usato dopo scadenza Non accessibile da interessato Non bloccabile
Documenti cartacei	Diffusi Trafugati	Danneggiati per: Modifica Manomissione	Persi Distrutti	Fini incongruenti Usato dopo scadenza Non accessibile da interessato
Locali e strutture logistiche	Intrusione	Danneggiati per: Distruzione Manomissione	Distruzione Guasto Non disponibile	Fini incongruenti
Trattamenti esterni	Diffusi Trafugati Usati per deduzioni (inferenza)	Danneggiati per: Errore utente Errore Hw Errore Sw Manomissione	Non Disponibile	Fini incongruenti Non bloccabile

2.1 Misure di sicurezza

A fronte dell'analisi dei rischi, sono individuati specifici interventi operativi per la sicurezza così articolati:

- misure di sicurezza fisiche riguardanti la sicurezza passiva ed il controllo accessi ai locali dell'Azienda finalizzate alla salvaguardia degli strumenti informatici, i supporti di memorizzazione dei documenti informatici e di conservazione dei documenti cartacei;
- misure di sicurezza logiche riguardanti il controllo dell'accesso al sistema informatico;
- misure organizzative relative ai ruoli e alle responsabilità dei vari soggetti, interni ed esterni, che gestiscono documenti e trattano dati personali.

3 Misure Fisiche

I locali della sede operativa di Bergamo Sviluppo sono posti al secondo e terzo piano del Palazzo dei Contratti e delle Manifestazioni della C.C.I.A.A. di Bergamo.

I locali della sede operativa di Dalmine sono posti nell'Edificio 1 B presso il Polo per L'Innovazione Tecnologica di Dalmine, gestito dalla società Tecnodal Srl.

I locali sono classificati nel seguente modo:

locali aperti, ove l'accesso è libero negli orari di ufficio ed esiste una vigilanza generica da parte del personale (sale conferenze, aule, sala attesa, ecc...);

locali riservati, ove l'accesso da parte di terzi è consentito unicamente se accompagnati da personale interno;

locali di sicurezza, accessibili esclusivamente dal personale autorizzato in modo specifico.

Tale suddivisione degli ambienti si rende necessaria non solo per motivi generici di sicurezza, ma principalmente a causa del fatto che è necessario separare gli spazi in cui vengono svolti i trattamenti (a maggior ragione se con documenti cartacei) da quelli ove è consentito la presenza di soggetti terzi. E' necessario che atti, documenti, pratiche in lavorazione, dati presenti sullo schermo delle stazioni di lavoro non siano visibili alle persone non incaricate dei trattamenti.

In funzione di ciò, deve essere assicurato il controllo di tutti i soggetti che accedono ai locali.

I soggetti esterni possono circolare nei locali riservati solo se accompagnati da personale interno.

Gli archivi cartacei si distinguono tra:

archivi operativi, conservati in armadi tradizionali presso gli uffici;

archivi di riposo, conservati in locali dedicati a tale scopo. I locali destinati agli archivi di riposo sono considerate aree di sicurezza.

Gli archivi operativi non sono collocati in aree accessibili al pubblico; tali aree sono chiuse mediante serratura la cui chiave è affidata agli incaricati del Trattamento.

3.1 Controllo accessi

La Camera di Commercio provvede al controllo del Palazzo dei Contratti e delle Manifestazioni mediante il servizio di ronda quotidiana notturna, festivi compresi, ad opera di Istituto per la vigilanza.
L'accesso alle aree di sicurezza e agli archivi cartacei è permesso esclusivamente al personale autorizzato.

3.1.1 Sede Operativa – Bergamo, Via S. Zilioli n. 2

- L'ingresso pedonale da Via S. Zilioli n. 2 è dotato di sistema di videosorveglianza e videoregistrazione gestito dalla Camera di Commercio di Bergamo.
- La porta d'ingresso è chiusa a chiave e le chiavi sono in dotazione ai dipendenti e agli incaricati autorizzati. Per accedere agli uffici è quindi necessario utilizzare il videocitofono. Il servizio segreteria è attivo negli orari di apertura al pubblico.
- Locali Ced (apparati di rete) e centralino telefonico posti nel seminterrato dotati di porte di ingresso con serratura la cui chiave è in possesso degli incaricati.
- Aree con archivi cartacei "operativi" mantenute chiuse mediante serratura la cui chiave è in possesso degli incaricati.
- Archivi cartacei "di riposo" in aree non aperte/accessibili al pubblico accessibili ai soli autorizzati.

3.1.2 Sede distaccata Dalmine – Via Pasubio n. 5 – Edificio 1B

- Gli ingressi di accesso al Polo Tecnologico sono presidiati da un servizio di portineria negli orari di apertura oppure sono accessibili mediante badge personale. E' attivo un sistema di videosorveglianza e videoregistrazione esterno all'edificio 1 B. Tali servizi sono gestiti da Tecnodal srl.
- Impianto di allarme collegato con istituto per la sorveglianza incaricato da Tecnodal srl (servizio incluso nel contratto d'affitto)
- Locale Ced (apparati di rete) dotato di porte di ingresso con serratura la cui chiave è in possesso degli incaricati.
- Aree con archivi cartacei "operativi" mantenute chiuse mediante serratura la cui chiave è in possesso degli incaricati.

3.2 Sistema antincendio

I locali di Bergamo Sviluppo sono protetti da mezzi antincendio mobili (estintori a polvere/anidride carbonica) azionabili manualmente dai componenti la squadra antincendio e di primo soccorso, appositamente istruiti ai sensi del D. Lgs. n. 81/2008; esistono anche idranti a muro e naspi Uni45. La manutenzione del sistema antincendio è affidata dalla Camera di Commercio a Tecnoservicecamere scarl in global service.
Gli archivi cartacei, alcuni locali tecnici, e i disimpegni/corridoi dislocati lungo le vie di fuga sono protetti da porte taglia fuoco.
La dislocazione fisica degli estintori, degli idranti e dei naspi, nonché delle porte taglia fuoco è riportata nelle piantine del Piano di evacuazione allegate al Documento di Valutazione del rischio ai sensi dell'art. 28 del D. Leg. n. 81/2008.

3.2.1 Sede operativa - Bergamo, Via S. Zilioli n. 2

Sono presenti i seguenti mezzi/sistemi antincendio:

- Estintori a polvere e ad anidride carbonica
- Idranti a muro
- Naspi Uni 45
- Attacco moto pompa
- Porte taglia fuoco
- Rilevatori fumo
- Pulsanti di allarme
- Targhe ottico/acustiche
- Sirene di allarme

La centrale del sistema antincendio secondo piano è collegata al ponte radio con trasmissione di "incendio" alla centrale operativa dell'istituto di sorveglianza, e ai numeri telefonici di cinque dipendenti individuati dalla direzione.

3.2.2 Sede distaccata Dalmine – Via Pasubio n. 5 – Edificio 1B

Sono presenti i seguenti mezzi/sistemi antincendio:

- Estintori a polvere e ad anidride carbonica
- Idranti a muro
- Naspi Uni 45
- Attacco moto pompa esterna
- Porte taglia fuoco
- Rilevatori fumo
- Pulsanti di allarme
- Targhe ottico/acustiche
- Sirene di allarme

3.3 Misure protezione dati personali

Le misure di protezione dei dati personali contenuti in archivi cartacei hanno lo scopo di evitare l'accesso non autorizzato alle informazioni personali, l'indebita modificazione dei dati, la loro comunicazione non autorizzata, l'illegittima modificazione dei trattamenti, l'appropriazione, il danneggiamento o la distruzione anche involontaria degli archivi medesimi.
Gli atti ed i documenti contenenti i dati personali vengono conservati in armadi o cassetti il cui accesso viene riservato esclusivamente al personale incaricato al trattamento.
Gli Incaricati al trattamento hanno accesso ai soli dati personali strettamente necessari per compiere il trattamento loro assegnato. Essi conservano gli atti ed i documenti contenenti i dati per il tempo occorrente - con riferimento ai termini di legge o regolamentari per la conclusione degli iter amministrativi – al trattamento e li reinseriscono negli archivi a conclusione delle operazioni affidate.
Le copie e le riproduzioni di documenti contenenti informazioni personali sono a loro volta dati personali e pertanto vanno trattate e custodite come tali.

3.4 Misure protezione dati sensibili

L'accesso agli archivi cartacei contenenti dati sensibili è controllato e selezionato sulla base delle necessità di trattamento. Gli incaricati che accedono a tali archivi devono conservare i documenti prelevati in contenitori armadi/cassetti muniti di serratura e restituirli al termine del trattamento.
E' fatto divieto di produrre copie anche parziali dei documenti contenenti dati sensibili e/o giudiziari, salvo diverse esplicite disposizioni relative a procedure per cui le copie sono indispensabili. Tutte le copie vengono trattate con le stesse misure di riservatezza e sicurezza degli originali e distrutte dopo l'uso dallo stesso incaricato al trattamento dei dati contenuti.
L'accesso agli archivi segue le norme previste per le aree di sicurezza ed è consentito esclusivamente agli incaricati specificatamente autorizzati.

4 Misure Logiche

Le misure di protezione dei dati personali trattati mediante elaboratori e contenuti in archivi informatici non gestiti da Infocamere S.c.p.A. hanno lo scopo di evitare l'accesso non autorizzato alle informazioni personali, l'indebita modificazione dei dati, la loro comunicazione non autorizzata, l'illegittima modificazione dei trattamenti, l'appropriazione, il danneggiamento o la distruzione anche involontaria degli archivi medesimi.

4.1 Titolarità degli strumenti e delle apparecchiature informatiche e controllo accesso ai sistemi di elaborazione

Bergamo Sviluppo ha la titolarità delle apparecchiature informatiche e degli strumenti assegnati ai dipendenti o collaboratori. Tali strumenti sono affidati ai medesimi a condizione che vengano custoditi con cura, evitando manomissioni, danneggiamenti o utilizzi, anche da parte di estranei, per scopi non inerenti alle funzioni istituzionali.
L'utilizzo di tali apparecchiature deve, pertanto, essere disciplinato da regole precise e certe in quanto da comportamenti - anche inconsapevolmente non leciti - possono derivare conseguenze gravi, sia sul piano tecnico (come un blocco della funzionalità o una perdita di dati) sia sul piano giuridico (mediante l'insorgere di responsabilità sia penali sia civili a carico contestualmente dell'Azienda e dello stesso lavoratore).

L'accesso diretto ai server di rete locale, virtualizzati presso Infocamere S.c.p.A. è consentito esclusivamente all'Amministratore di sistema o ai suoi delegati.
L'accesso alle risorse informatiche, locali o di rete, avviene attraverso uno specifico profilo di abilitazione. Tale profilo definisce, per ogni soggetto associato (qualsiasi utente del sistema informatico, interno o esterno), le funzionalità disponibili ed in particolare le seguenti tipologie di abilitazioni di accesso:

- accesso locale alle stazioni di lavoro

- accesso alla rete locale tramite la stazione di lavoro
- accesso ai trattamenti e/o gli archivi presenti sui server della rete locale per cui viene data abilitazione con specifici diritti (sola lettura, modifica, ecc..)
- accesso alle applicazioni presenti sul server della intranet per cui viene data abilitazione con le relative funzionalità applicative abilitate
- la possibilità di interconnessione con la rete del sistema camerale ovvero con reti esterne, in particolare Internet.

La presenza di archivi e documenti sulle singole postazioni di lavoro deve essere considerata eccezionale, a fronte di esigenze particolari per elaborazioni individuali, e di carattere temporaneo.
Qualsiasi tipo di dato/documento attinente i trattamenti svolti dal soggetto va mantenuto presso aree ad accesso controllato situate, di norma, sui file server dell'Azienda.
Il sistema di controllo accessi delle stazioni di lavoro garantisce:

- l'accesso agli archivi eventualmente presenti sulle stazioni di lavoro esclusivamente ai soggetti identificati dal titolare dell'archivio stesso;
- l'accesso alla rete esclusivamente ai soggetti autorizzati ed attraverso la o le stazioni di lavoro abilitate;
- l'accesso agli archivi ed alle applicazioni presenti sui server locali esclusivamente ai soggetti abilitati e per le funzionalità autorizzate;
- l'accesso agli archivi/servizi di InfoCamere S.c.p.A. e di interconnessione con reti esterne esclusivamente ai soggetti autorizzati.

4.1.1 Identificazione ed autenticazione degli utenti

Il sistema informatico di Bergamo Sviluppo è costituito da:

1. rete locale realizzata e sviluppata a seguito di cablaggio strutturato dei locali e gestita da un server virtuale in gestione a Infocamere S.c.p.A.;
2. collegamento con la rete nazionale Infocamere S.c.p.A. attraverso un router di proprietà della CCIAA.

Rete Locale

L'accesso del personale alla rete locale avviene mediante:
USER ID identificativo della persona
PASSWORD parola chiave personale

Il personale dipendente, come i collaboratori stabili, vengono identificati generalmente con il proprio cognome. Le password di tali accessi vengono decise direttamente dall'utilizzatore del PC, sia esso un dipendente o un collaboratore.
Le password devono avere una lunghezza di almeno otto caratteri e hanno una scadenza, imposta dal sistema, di 90 giorni. Alla scadenza gli utilizzatori hanno l'obbligo di sostituire la password.
In caso di necessità e/o di assenza dell'incaricato, l'ufficio informatico della CCIAA di Bergamo, su richiesta dell'incaricato o del suo Responsabile, provvede alla creazione di una nuova password comunicandola a chi ne fa richiesta, con obbligo di cambiarla al primo accesso da parte dell'incaricato. Sarà cura del Responsabile informare l'incaricato della predetta modalità di accesso in sua assenza.
È fatto divieto di trascrivere su carta o conservare con altra modalità la password di accesso ai sistemi informatici, nonché comunicare la password ad altri, anche per solo utilizzo temporaneo.
Ogni incaricato è abilitato in modo puntuale all'accesso alla rete e alle singole risorse di elaborazione necessarie per i trattamenti cui è autorizzato dal proprio "profilo utente". Nessun incaricato ha le abilitazioni di amministratore locale della postazione di lavoro informatica.
La password è elemento fondamentale per la sicurezza delle informazioni ed il suo corretto utilizzo è garanzia per gli incaricati del trattamento e per gli stessi utenti di Bergamo Sviluppo.
In caso di revoca dell'incarico e/o delle autorizzazioni la user-id deve essere immediatamente resa inutilizzabile, o, a seconda delle necessità, modificato il profilo di abilitazioni.

***Rete Infocamere* S.c.p.A.**

Ogni utilizzatore del sistema informatico esterno (rete Infocamere S.c.p.A.) può essere identificato mediante un codice identificativo personale (pubblico) denominato user-id ed una password (privata). La user-id non può, neppure in tempi diversi, essere assegnata a persone diverse. Ad ogni user-id è associato un profilo di abilitazioni.

L'accesso con user-id è utilizzato per la intranet camerale, la posta elettronica, l'accesso a Internet e ai servizi di Infocamere S.c.p.A.

In caso di revoca dell'incarico e/o delle autorizzazioni la user-id deve essere immediatamente resa inutilizzabile, o, a seconda delle necessità, modificato il profilo di abilitazioni.

La password è elemento fondamentale per la sicurezza delle informazioni ed il suo corretto utilizzo è garanzia per gli incaricati al trattamento e per gli stessi utenti di Bergamo Sviluppo. Al fine di armonizzare l'esigenza di sicurezza dei dati personali con il principio di efficienza dell'azione amministrativa, ciascuna password viene assegnata esclusivamente ad ogni incaricato del trattamento, rimanendo segreta per i restanti incaricati del trattamento.

Le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo da parte dell'incaricato del trattamento o comunque ogni qual volta si ritenga che la segretezza delle stesse possa essere stata violata.

La lunghezza minima della password è di 8 caratteri e deve rispettare quanto segue:

- deve contenere almeno un carattere alfabetico e uno numerico
- può contenere un carattere speciale
- non deve contenere più di due caratteri identici consecutivi
- non deve essere simile alla password precedente
- non deve contenere l'user-id come parte della password
- deve essere cambiata almeno ogni 6 mesi (tre mesi in caso di trattamento di dati sensibili)
- non deve essere comunicata agli altri utenti, nemmeno se gerarchicamente superiori
- deve essere diversa da qualsiasi combinazione con i seguenti prefissi banali (pippo, pluto, paper, game, apri, etc), combinazioni da tastiera (qwert, asdf, zxcv), nomi italiani comuni (Mario, Antonio, etc), nomi dei mesi (genn, febb, marz, etc), principali città italiane (Roma, Napoli, Venezia, etc), squadre di calcio (Juve, Milan, etc), termini informatici comuni (sys, ibm, net, demo, passw, etc)

In caso di inutilizzo per più di sei mesi o in caso di risoluzione del rapporto di lavoro, l'account sarà reso indisponibile.

E' fatto divieto di comunicare la password ad altri, anche per solo utilizzo temporaneo od in caso di emergenza.

4.1.2 Criteri e procedure di rilascio di user-id e password

Ai nuovi soggetti incaricati del trattamento vengono attribuite dall'Amministratore di sistema le abilitazioni necessarie.

Ogni situazione che comporti una variazione delle abilitazioni e/o revoca delle credenziali di accesso deve essere comunicata tempestivamente all'Amministratore di Sistema.

4.1.3 Screen saver

La stazione di lavoro non deve essere lasciata incustodita o comunque utilizzabile da altri colleghi o da terzi, nemmeno durante le pause brevi e la pausa pranzo. Su ogni postazione di lavoro deve essere attivata, a cura dell'utilizzatore, la funzione salva schermo (screensaver) protetto da password che si attiva dopo il tempo impostato di inattività. Con questa modalità è inibito un utilizzo improprio di dati personali in caso di abbandono, anche temporaneo, della stazione già abilitata all'accesso.

4.2 Protezione antivirus

Tutte le postazioni di lavoro sono protette contro il rischio di intrusione ad opera di programmi illeciti (inclusi quelli di cui all'art 615-quinquies del Codice Penale).
La protezione di tutte le postazioni in rete avviene in tempo reale mediante l'utilizzo di adeguati programmi antivirus e antispam, aggiornati centralmente, in grado di monitorare il rischio di infezione e gestiti centralmente da Infocamere S.c.p.A.
La protezione delle postazioni di lavoro della sede di Dalmine avviene mediante l'installazione di antivirus locali.
L'incaricato non deve disattivare il servizio "antivirus" e, in caso di malfunzionamenti o disconnessioni del servizio, deve avvisare immediatamente l'amministratore di sistema.

4.3 Backup e ripristino della disponibilità dei dati

I dati/documenti riferiti alla rete locale di Bergamo Sviluppo contenuti negli archivi informatici "virtualizzati" presso il Data center di Infocamere S.c.p.A. sono protetti contro il rischio di perdita, anche accidentale, attraverso apposite procedure di salvataggio di copie di sicurezza che garantiscano il ripristino delle informazioni. In particolare i salvataggi vengono effettuati giornalmente in orario post-produzione in modalità "incrementale"; al sabato e/o domenica vengono effettuati i backup "completi". I dati salvati vengono mantenuti disponibili per l'operazione di "restore" per 12 settimane. Infocamere S.c.p.A. garantisce il ripristino/restore dei dati con granularità fino al singolo file, qualora trattasi di sistemi operativi gestiti dalla stessa. Il ripristino/restore verrà eseguito a fronte di una richiesta e l'ufficio informatico competente potrà provvedere, mediante le funzionalità delle Shadow Copy e con tempi di lavoro limitati, al recupero dei dati in autonomia.
Il backup e il restore dei dati/documenti relativi a procedimenti affidati a responsabili esterni sono assicurati da questi ultimi.

4.4 Criteri e procedure di controllo accessi agli archivi informatici

L'accesso al sistema e alle risorse di rete è controllato da un apposito sistema di gestione che, sulla base delle abilitazioni corrispondenti ai vari profili utente, consente l'accesso ai soli archivi/dati necessari e sufficienti per il trattamento. Il Titolare e l'Amministratore di sistema hanno il compito di vigilare, ciascuno per le proprie competenze, sul corretto utilizzo delle procedure attivandosi immediatamente in caso si riscontrino variazioni dei profili di abilitazione.

4.5 Criteri e procedure per l'utilizzo della posta elettronica e di Internet

I servizi di posta elettronica e di navigazione internet sono risorse aziendali che il datore di lavoro mette a disposizione del dipendente per il perseguimento dei fini lavorativi.
L'utilizzo di tali strumenti è consentito per svolgere gli incarichi per i quali sono state assegnate le abilitazioni di accesso. L'uso improprio di tali strumenti può pregiudicare in modo rilevante la sicurezza dei dati/documenti trattati, arrecando rilevanti danni, anche sotto il profilo penale, all'attività dell'Azienda.
Per garantire gli adempimenti di sicurezza previsti dalla normativa vigente, Infocamere S.c.p.A. gestore tecnico del servizio, registra le informazioni relative all'utilizzo degli strumenti di posta elettronica e del "traffico Internet". Tali informazioni sono a disposizione esclusivamente delle autorità giudiziarie preposte e memorizzate in forma protetta per il tempo stabilito dalle normative di riferimento.
Tutti i messaggi di posta elettronica inviati dalle caselle aziendali conterranno il seguente messaggio automatico: "Le informazioni contenute in questo messaggio, dirette esclusivamente ai destinatari, non hanno natura personale e le eventuali risposte potranno essere conosciute nell'ambito dell'organizzazione. Se avete ricevuto questo messaggio per errore, Vi preghiamo di contattarci via e-mail e di cancellarlo".
Agli Incaricati sono impartite le seguenti istruzioni:

- per connettersi a Internet è necessario autenticarsi;
- gli incaricati non devono salvare password fisse nei loro browser o e-mail;

- tutte le attività in Internet devono passare da punti di accesso approvati:
- non si possono attivare connessioni di rete verso l'esterno, via Internet o altri sistemi, che non siano stati preventivamente autorizzati;
- è fatto divieto di utilizzare le caselle di posta elettronica ordinaria nominative (cognome@bg.camcom.it) o di gruppo per comunicazioni non strettamente correlate all'attività lavorativa;
- non è consentito comunicare le proprie credenziali (user-id, email) a siti e servizi internet;
- l'utilizzo di terminali personali (pc o smartphone) per la consultazione e la gestione della posta elettronica aziendale deve essere preventivamente autorizzato, compreso l'accesso alla web mail.

Nel caso di assenza programmata e al fine di non interrompere né rallentare i processi produttivi e/o lavorativi, i dipendenti sono tenuti a predisporre le funzionalità previste dal sistema di posta elettronica che permettono l'invio di un messaggio automatico di risposta che segnali altro nominativo e relativo indirizzo di posta elettronica da contattare nel caso di urgenze. Si dispone inoltre che nel messaggio automatico di risposta siano evidenziati l'inizio e la fine del periodo di assenza del dipendente, con l'indicazione di eventuale contatto alternativo.

Per coloro che a qualsiasi titolo cessino il proprio rapporto di lavoro o di collaborazione, è disposta l'immediata disattivazione dell'indirizzo di posta elettronica.
Sarà cura del Direttore dell'Azienda chiedere al responsabile del servizio di posta elettronica la disattivazione della casella di posta elettronica, a far data dalla cessazione del rapporto di lavoro.

4.6 Criteri e procedure per i supporti rimovibili e apparecchiature portatili

Relativamente ai supporti rimovibili e alle apparecchiature portatili sono impartite agli incaricati del trattamento le seguenti istruzioni:

- non utilizzare supporti rimovibili o apparecchiature portatili personali collegandole alla postazione di lavoro o alla rete (e di sistemi elettronici e telematici personali, in genere); i soli supporti rimovibili e sistemi elettronici e telematici ammessi nell'Azienda sono quelli espressamente autorizzati;
- tutti i supporti magnetici utilizzati devono essere inizializzati prima dell'uso mediante appositi software che consentano di rendere illeggibili i dati eventualmente registrati in precedenza; tale procedura si applica anche in caso di eliminazione dei supporti magnetici rimovibili;
- è fatto divieto di portare all'esterno dell'Azienda qualsiasi supporto rimovibile fornito dall'Azienda se non espressamente autorizzati

Le apparecchiature portatili sono consegnate previa esplicita richiesta per esigenze di servizio e sono soggette a regolamentazione come le normali postazioni di lavoro.

5 Misure organizzative (figure e responsabilità)

5.1 Titolare del trattamento dei dati

Titolare del trattamento è Bergamo Sviluppo – Azienda Speciale della CCIAA di Bergamo nella figura del legale rappresentante.
I principali compiti sono:

- nominare il Referente del titolare del trattamento dei dati personali e almeno un Referente interno;
- nominare i responsabili esterni del trattamento, conferendo loro istruzioni per il corretto trattamento dei dati;
- nominare gli incaricati del trattamento e conferire loro le necessarie direttive ed autorizzazioni al trattamento di dati sensibili o, in alternativa, redigere un disciplinare per gli

incaricati del trattamento dei dati;
- effettuare periodici controlli e verifiche in merito al rispetto delle prescrizioni contenute nel presente documento e delle istruzioni impartite;
- rimuovere, nel più breve tempo possibile, le accertate violazioni delle prescrizioni del documento;
- elaborare un piano di formazione ed aggiornamento costante degli incaricati del trattamento.

5.2 Referente del titolare del trattamento dei dati

Referente del Titolare del trattamento è individuato nella figura del Direttore dell'Azienda.
I principali compiti sono:
- dialogare con il Referente interno del trattamento per la definizione/aggiornamento/implementazione e per il trasferimento del modello per la protezione dei dati personali;
- analizzare, unitamente al Referente interno, le eventuali richieste pervenute, e supervisionare l'evasione delle stesse;
- indirizzare e supervisionare l'esecuzione di specifiche attività ad alto valore aggiunto previste all'interno del modello per la protezione dei dati personali (es. aggiornamento del registro dei trattamenti);
- tenere informato il Titolare circa i fatti di maggiore rilevanza, in particolare sui rischi da prevenire e misure adottate o da adottarsi, sul verificarsi di eventuali inconvenienti in merito e sulle modalità del loro superamento;
- garantire, in collaborazione con il Referente interno, la protezione dei dati personali fin dalla progettazione di un prodotto/servizio e/o sistema e protezione dei dati personali per impostazione predefinita (art. 25).

5.3 Referente interno per il trattamento dei dati

Referente interno per il trattamento è individuato nella figura del Responsabile Amministrativo.
I principali compiti sono:
- collaborare all'elaborazione e al mantenimento dell'elenco degli applicativi che trattano dati personali, con particolare riferimento a quelli che trattano categorie di dati particolari o giudiziari;
- collaborare alla tenuta e aggiornamento del Registro dei trattamenti;
- segnalare la necessità di nominare i responsabili esterni del trattamento (art. 28);
- attenersi alle indicazioni del Titolare del trattamento e del Referente del Titolare del trattamento, predisponendo tutte le misure di sicurezza necessarie alla tutela dei dati trattati, nonché fornire supporto agli stessi nel caso in cui si verifichino violazioni e conseguenti necessità di notifica agli interessati e/o all'Autorità Garante o qualora l'Autorità chieda all'Azienda di fornire informazioni in merito al trattamento;
- verificare che i le attività dell'Azienda siano svolte garantendo agli interessati un'adeguata conoscibilità dell'informativa adottata dalla stessa;
- eseguire gli opportuni controlli al fine di assicurare che il trattamento dei dati avvenga nel pieno rispetto della normativa vigente e collaborare attivamente con il DPO in occasione degli audit periodici da questi organizzati;
- gestire il rapporto con gli interessati nel rispetto della normativa privacy vigente con particolare riguardo alla dimostrazione della legittimità del consenso prestato, alla collaborazione con il DPO e con il Referente del Titolare del trattamento, nel soddisfare le richieste dell'interessato al fine di esercitare i suoi diritti, nonché all'adozione di misure appropriate per fornire all'interessato per iscritto o con altri mezzi tutte le informazioni e le comunicazioni relative al trattamento ovvero per procedere se necessario alle eventuali rettifiche o cancellazioni o limitazioni del trattamento (art. 8,12, 13, 14, 15, 16, 17, 18, 19);
- vigilare, in collaborazione con il Referente del Titolare del Trattamento, sulla protezione dei dati personali fin dalla progettazione di un prodotto/servizio e/o sistema e protezione dei

dati personali per impostazione predefinita (art. 25);

- nominare gli incaricati del trattamento - laddove l'autorizzazione non derivi già dalla organizzazione aziendale (es. stagisti) – attraverso la distribuzione del disciplinare, contenete le istruzioni relative alle operazioni di trattamento e di custodia di atti e documenti contenenti dati personali, nonché le misure minime di sicurezza;
- collaborare alla gestione di eventuali violazioni dei dati personali (artt. 33, 34);
- collaborare alla eventuale effettuazione della Data Protection Impact Assessment ed eventuale consultazione preventiva (artt. 35, 36).

.

5.4 Responsabili esterni del trattamento dei dati

Il titolare provvede alla nomina di alcuni responsabili esterni del trattamento dei dati che devono assicurare il rispetto delle seguenti istruzioni:

- curare che i dati personali oggetto del trattamento siano trattati in modo lecito e secondo correttezza. A tale scopo il Responsabile si atterrà alle disposizioni contenute nel Regolamento (UE) 2016/679 e nei provvedimenti del Garante della Privacy applicabili;
- trattare solo i dati personali strettamente necessari all'espletamento del servizio in oggetto;
- mantenere riservati i dati e le informazioni di cui venga in possesso e, comunque, a conoscenza, non divulgarli in alcun modo e in qualsiasi forma e non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione del contratto sottoscritto con il Titolare;
- adottare tutte le misure tecniche ed organizzative idonee al fine di garantire un livello di sicurezza adeguato al rischio, tenendo conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati;
- provvedere ad impartire, alle persone che il Responsabile riterrà di autorizzare al trattamento dei dati, la necessaria formazione e le istruzioni necessarie ed opportune al fine di garantire la riservatezza dei dati ed, in generale, il rispetto della normativa vigente e dei Provvedimenti del Garante applicabili;
- attuare un controllo sull'attività svolta dalle persone incaricate del trattamento al fine di verificare l'effettivo rispetto da parte di questi ultimi delle misure di sicurezza adottate e, comunque, delle istruzioni impartite;
- fornire al Titolare, a semplice richiesta e con le modalità indicate da quest'ultimo, tutti i dati e le informazioni oggetto dei trattamenti affidati al Responsabile. Le valutazioni sulla legittimità del trattamento di tali dati, dell'eventuale comunicazione a terzi o diffusione degli stessi spettano al Titolare, congiuntamente ai relativi adempimenti, ivi comprese le informative ai propri dipendenti ed agli altri interessati inerenti al trattamento dei dati;
- provvedere alla conservazione e all'integrità di tutti i documenti ricevuti necessari alle operazioni di trattamento con preclusione di qualunque diritto da parte del responsabile sui dati contenuti in tali documenti;
- assistere il Titolare, tenendo conto della natura del trattamento, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato per quanto previsto nella normativa vigente;
- in caso di violazione di dati personali, informare il Titolare del trattamento senza ritardo, comunque entro 48 ore dal momento in cui è venuta a conoscenza della violazione, e collaborare attivamente con il Titolare stesso, nella raccolta documentale e in tutte le attività connesse all'eventuale notifica al Garante Privacy e ai soggetti interessati, per quanto previsto nella normativa vigente;
- fornire al Titolare, a semplice richiesta e secondo le modalità indicate da quest'ultimo, i dati e le informazioni necessari per consentire allo stesso di svolgere una tempestiva difesa in eventuali procedure instaurate davanti al Garante o all'Autorità Giudiziaria e relative al trattamento dei dati personali;

- compiere tempestivamente quanto necessario per conformarsi a richieste pervenute dal Garante o dall'Autorità Giudiziaria o, comunque, dalle Forze dell'Ordine, fornendo tempestive informazioni in caso di specifiche esigenze espresse dal titolare;
- mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente atto di nomina, consentendo e contribuendo alle attività di revisione, comprese le ispezioni realizzate dal Titolare (o da un altro soggetto da questi incaricato);
- in generale, prestare la più ampia e completa collaborazione al Titolare e al suo Responsabile per la Protezione dei Dati (Data Protection Officer), al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente;
- nominare, previa autorizzazione del Titolare del trattamento, eventuali Responsabili del Trattamento per specifiche attività, nel rispetto di quanto previsto dall'art. 28 del Regolamento (UE) 2016/679, trasferendo su di essi le disposizioni impartite dal Titolare.

5.5 Incaricati del trattamento dei dati

Tutto il personale dipendente che nello svolgimento delle proprie mansioni effettua operazioni di trattamento sui dati personali è stato incaricato del trattamento dei dati, tramite la distribuzione dell'apposito Disciplinare Comportamentale, contenente le indicazioni necessarie ad operare nel rispetto delle normative vigenti per la riservatezza dei dati e la sicurezza del trattamento e deve seguire le disposizioni particolari fissate dal Referente interno.

5.6 Amministratore di sistema

Il Garante della protezione dei dati personali nel provvedimento del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratori di sistema" ha individuato e specificato le attribuzioni alle figure preposte alla protezione dei dati trattati con sistemi informatici e alla sicurezza dei medesimi dati e sistemi.

Il Garante ha chiarito che svolgono il ruolo di Amministratore di sistema quelle "figure professionali finalizzate alla gestione e alla manutenzione di impianti di elaborazione o di sue componenti con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali".

L'Amministratore di sistema è Infocamere S.c.p.A. che potrà avvalersi per la "gestione amministrativa" dei server della collaborazione dei 3 fornitori di servizi esterni individuati da Bergamo Sviluppo e di n. 2 figure dell'ufficio informatico camerale. Gli stessi devono identificarsi con user e pw diversa dall'utente "administrator" che non può essere la stessa utilizzata per le normali attività quotidiane. Al fine di monitorare l'operato di tali figure, il Titolare o un suo delegato, con cadenza almeno annuale, può controllare le registrazioni dei log di accesso alla rete camerale, al fine di verificare eventuali incongruenze ad esempio orari di accesso non giustificati o accessi eccezionali rispetto alla norma. Il servizio di registrazione dei log di accesso è affidato a Infocamere S.c.p.A.

6 Interventi formativi

Il personale neoassunto e periodicamente tutti i dipendenti sono oggetto di specifica formazione per fornire le nozioni fondamentali e le istruzioni operative necessarie atte ad assicurare il corretto trattamento dei dati da parte di ciascun incaricato durante l'espletamento dell'attività lavorativa, sia a illustrare le novità normative in materia di privacy e sicurezza dei luoghi di lavoro.

7 Struttura di rete

7.1 Connettività alla rete geografica Sistema nazionale camerale

Bergamo Sviluppo è interconnessa alla rete geografica del Sistema nazionale camerale gestita da Infocamere S.c.p.a., società consortile del Sistema camerale, con accesso principale in fibra ottica e linea di backup HDSL.
Sede staccata: Dalmine presso il Polo Tecnologica (Dalmine, via Pasubio) è collegata ad Internet mediante una adsl fornita da Tecnodal Srl.

7.2 Virtualizzazione

Bergamo Sviluppo ha proceduto, al fine di avere un ambiente di rete locale sicuro e affidabile e rispondente alle normative sulla sicurezza e privacy, al consolidamento del proprio server mediante il processo di virtualizzazione direttamente nel Datacenter di Infocamere S.c.p.A., inserendosi nei server e nel dominio già in uso dalla Camera di commercio di Bergamo.

7.3 Sito internet

L'housing, l'assistenza tecnica e la manutenzione ordinaria dei siti (domini di proprietà dell'Azienda) è affidata a società esterna nominata "responsabile esterno del trattamento".

7.4 Collegamento Internet

Tutte le postazioni di lavoro possono navigare in Internet tramite la rete geografica di Infocamere S.c.p.A. che gestisce le politiche di sicurezza e privacy nell'utilizzo del sistema (limitazioni di navigazione, politiche di accesso, restrizioni ecc…) adottando idonee misure fisiche/logiche per ridurre al minimo rischi di "infiltrazioni pericolose" da parte di hacker.

7.5 Posta elettronica

L'Azienda Speciale utilizza il sistema di posta elettronica "centralizzato" fornito da Infocamere S.c.p.A. che ha la gestione delle politiche di sicurezza e privacy relative al servizio per ridurre al minimo i rischi di messaggi "malevoli" adottando idonee misure di "spam" e altre politiche di sicurezza.